Cybersecurity for the Water Industry

Let Our Comprehensive Knowledge Help You Navigate the Complexities of Cybersecurity.

BLACK & VEATCH

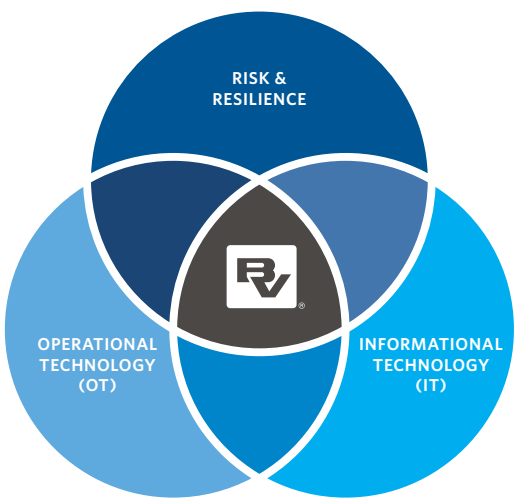
Cybersecurity and System Resilience

Water Systems Are Critical Infrastructure. Let's Keep Them Safe.

Technology is all around us, connecting us in a myriad of ways. While it's opened new ways for connectivity and added new lanes to the information superhighway, the Internet of Things has also created a different risk for our nation's critical infrastructure, including water and wastewater systems.

Cybersecurity breaches can lead to:

- Defacement of the utility's website or compromise the email system.
- Theft of customers' personal information from billing systems.
- Redirection of financial payments to malevolent individuals or groups.
- Release of ransomware that can disable maintenance, customer service and billing.



Even worse, cyber-attacks on water, wastewater or stormwater utilities' industrial control systems, called SCADA systems or operational technology (OT), can cause significant harm through alterations in the treatment or conveyance processes. These can include:

- Releasing ransomware that mandates manual control.
- Changing chemical dosing that could injure people or mandate boil water alerts.
- Opening and closing valves or stopping pumps that could prevent firefighting.

Black & Veatch combines in-depth knowledge of utility operations, SCADA and resilience with a comprehensive understanding of cybersecurity. We partner with utilities to help navigate the complex world of cybersecurity to identify custom, cost-effective solutions. We're at the nexus of OT, information technology (IT) and risk & resilience – all for water, wastewater and stormwater utilities.

Best Practices for Cybersecurity

The intersection of IT and OT creates operational efficiencies but also presents added security vulnerabilities. Control systems are most secure when isolated with dedicated firewalls and internet connectivity removed. However, operational data needs to be shared with internal stakeholders for water quality compliance reports.

The water for your community must be on 24/7/365 but updating the OT systems means significant unplanned downtimes. The need for significant testing and the downtime requirements have led to an "if-it's-not-broken, don't-fix-it-mentality," leaving the OT systems on unsupported versions of Windows. Like other software, OT software evolves and is updated to new versions compatible with more current operating systems. It needs testing and training for operators to understand and navigate the new interfaces to operate the water equipment.

Black & Veatch Water Cybersecurity Services

Black & Veatch has nationwide SCADA and IT capabilities that can help your SCADA or distributed control system to be more secure. We identify, categorize and characterize critical assets and OT computer systems that require security controls. Our areas of assistance can be recommending, installing and correctly configuring:

- **Multi-factor authentication for remote access.**
- **Anti-virus that will not impact SCADA system performance.**
- **Network configurations to improve segmentation and isolate computer systems that cannot be updated.**
- **SCADA firewall.**
- **Centralized log server that captures events for all remote connection protocols.**
- **SCADA operating systems functional with up-to-date versions of Windows.**
- **Supported versions of SCADA software.**
- **Staff skills assessments.**
- **Policies and procedures.**
- **Incorporation of cybersecurity into SCADA master plans.**
- **Legacy programmable logic controllers with efficient downtime.**
- **Baseline of the SCADA system and change control program.**
- **Disaster recovery of the SCADA system.**

In addition to the above, Black & Veatch is at the leading edge of resilience. The company is guiding Water Research Foundation Project No. 5014, which is developing a comprehensive framework for risk and resilience planning. Black & Veatch has also done more than 20 risk & resilience assessments (including cybersecurity) and more than 130 vulnerability studies in recent years for clients of all sizes across the U.S.

Can You Afford Not to Have It?

In the end, network security threats are a very real challenge for water utilities. Cybersecurity comes at a cost around valuing and investing in smart technology but also safety and security. When they occur, cyber-attacks not only erode customer confidence and cost money, they compromise your ability to provide clean, safe drinking water or effective wastewater management to your communities.

A breach of your systems is a breach on your community's resilience and customer confidence in the utility to provide the services promised. That changes the age-old question of "Can I really afford it?" to "Can I really afford not to have it?"

Physical Security

Black & Veatch also supports physical security at your sites. Our services include assessments for vulnerability, conditions and fencing; camera coverage and security monitoring; and defense zones (public areas, employee areas and high-security areas).

Where to Begin?

Just getting started can be tough! The proliferation of even more standards and regulations in recent times has made simply navigating the relevant cybersecurity standards and guidance a daunting task.

With a solid background and understanding of these regulations, we can help you navigate the labyrinth. And, by leveraging the American Water Works Association's Cybersecurity Risk Assessment Tool, for which Black & Veatch provided technical guidance, our company can audit the SCADA system to determine the areas of highest vulnerability – helping you understand where best to start.

Contacts

Jacques Brados – Water Cybersecurity National Practice Lead
P +1 602 381-4456 | E BradosJ@bv.com

Will Williams – Associate Vice President, Asset Management
P +1 404 432-3860 | E WilliamsWD@bv.com