WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: *Small Wastewater System*

Asset Inventory: A Good First Step to Balancing Risks

OVERVIEW

All mechanical operations at this system became automated when a new wastewater treatment plant came online in 2017. The plant operator had to balance the welcomed convenience of automation and productivity with the new cybersecurity risks introduced.

CYBERSECURITY APPROACH

The utility developed a cybersecurity policy document to ensure that vulnerabilities were considered, and cybersecurity risks mitigated. Topics covered include:

ACCOUNT SECURITY

- Separate standard user and privileged accounts
- Password length requirements
- Secure remote access policy

DEVICE SECURITY

- OT and IT network asset inventory

DATA SECURITY

- Log collection and monitoring frequency for intrusion detection

VULNERABILITY MANAGEMENT

- OT asset connection to the public Internet

RESPONSE AND RECOVERY

- Cybersecurity incident reporting
- Cybersecurity Incident Response Plan for critical threat scenarios, including disabled or manipulated process control systems
- System backups for post-incident recovery efforts

OTHER

- Segmentation of OT and IT networks

The policy document detailed the expectations, standards, and safeguards to reduce cybersecurity risks at the utility. For example, staff have unique user accounts with separate logins and passwords, and not all staff have programming privileges once logged into the SCADA system. The document clearly defined who to call for help once a cyber incident is discovered and provided contact information. In addition to the cyber policy, the Incident Response Plan was updated to describe how to run the plant in full “manual mode” without the benefit of the SCADA system in case of a cyber incident.

The utility has planned to make more cyber improvements such as enhancing internet capabilities. Enhancing Internet capabilities will allow operators to remotely access the SCADA system via a virtual private network (VPN). However, the utility will be introducing this new capability with multi-factor authentication procedures for logging in. The utility is committed to their goal of boosting convenience and productivity while balancing the new cybersecurity risks that these features bring.

LESSONS LEARNED

- Take advantage of free cybersecurity assessments. The utility took advantage of the U.S. Environmental Protection Agency's free cybersecurity vulnerability assessment which laid the groundwork for their cybersecurity improvements.
- Take action on all of the no-cost implementation measures. The cybersecurity measures implemented by the utility were essentially free, other than requiring some technical input from existing vendors and the operator's time (e.g., drafting the policy document, overseeing implementation of the identified actions) over an eight-month period.
- Maintain a cybersecurity asset inventory. In retrospect, one item the utility realized as fundamental to their success was the cyber asset inventory. This inventory served as the springboard for all other cyber improvements, as it gave them a clear snapshot of what they owned and how it was connected. In the operator's words, "It's really hard to know how to protect what you don't know you have." The inventory has also assisted in ongoing maintenance for cyber assets, as it listed all the assets in one place and contained information such as model and serial number, age, how the asset is used within the network, and vendor contact information for the asset.

READY TO BUILD YOUR CYBERSECURITY PROGRAM?

Visit the *Cybersecurity for the Water Sector* website and learn more about resources that can bring your utility one step closer to cybersecurity resilience.