WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: *Medium Drinking Water System #2*

Cybersecurity: Take Charge and Take Advantage

OVERVIEW

This medium-sized drinking water utility provides safe drinking water to 85,000 customers. With cybersecurity threats growing every day, and news that other local entities had experienced ransomware disruptions, this utility decided to reduce its cyber risks while increasing staff cybersecurity awareness and culture.

CYBERSECURITY APPROACH

With no one person in charge of cybersecurity, past efforts at the utility lacked momentum and cohesion. To energize and focus these efforts, the utility hired a full-time IT Manager to oversee both its information technology (IT) and operational technology (OT) systems. The new manager leveraged several free cybersecurity resources and technical assistance programs:

- EPA's cybersecurity assessment and technical assistance program
- Tabletop exercises conducted by regional DHS Cybersecurity and Infrastructure Security Agency (CISA) representatives
- Nationwide Cybersecurity Review (NCSR) self-assessment based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Guidance, tools, and free services (e.g., alerts) from the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- American Water Works Association (AWWA) water sector cybersecurity resources
- Local water sector associations/organizations
- A cyber audit performed by the state auditor's office

These resources enabled the IT manager to better understand the water sector's cyber risks and what could be done to mitigate them. Several cyber improvents were instituted at the utility:

DEVICE SECURITY

- Completed a thorough asset inventory to identify and replace legacy equipment
- Implemented server upgrades

DATA SECURITY

- Deployed a Managed Detection and Response (MDR) service

VULNERABILITY MANAGEMENT

- Employed active vulnerability detection to apply software updates and patches

RESPONSE AND RECOVERY

- Established offsite back-ups of critical data

OTHER

- Instituted virtual local area networks (VLANs) to segment the OT and IT networks

The IT Manager is also working on creating the utility's IT and OT standards to cover topics such as hardware retirement/replacement, acceptable use of utility devices, incident response procedures, data disposal criteria, password control, malware detection, and media protection.

LESSONS LEARNED

- Research and take advantage of all the free resources available to help implement cybersecurity practices.
- A stepwise, methodical approach with the understanding that you will not be able to do everything you want to do at once can help limit frustration.
- Invest time and resources on staff cybersecurity awareness training. Bottom line: you want to build both cybersecurity awareness and a cybersecurity culture at your utility.

READY TO BUILD YOUR CYBERSECURITY PROGRAM?

Ready to make your utility more cyber secure? EPA can help. Visit the *Cybersecurity for the Water Sector* website and learn more about resources that can bring your utility one step closer to cybersecurity resilience.