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

Cybersecurity: Become Your Own Best Resource

OVERVIEW

A drinking water utility felt safe and secure, but knew they needed to stay ahead on cybersecurity. In 2021, U.S. Environmental Protection Agency (EPA) cybersecurity outreach efforts to the water sector coincided with the utility's planned upgrades to their assets. The manager therefore contacted EPA to perform a cybersecurity assessment to ensure the utility had done everything possible to protect their assets, for both operational technology (OT) and information technology (IT).

CYBERSECURITY APPROACH

After the cybersecurity assessment, the manager met with the utility's Board. The manager was able to pursue training although the Board did not authorize contractor support for implementing further best practices. The manager earned industry-standard IT and cybersecurity certifications. Cybersecurity practices self-implemented at the utility since 2021 include:

ACCOUNT SECURITY

- Use of a password manager

DEVICE SECURITY

- Inventory of OT and IT assets
- Network topology mapping and monitoring (e.g., new device notifications)

GOVERNANCE AND TRAINING

- Utility cultural changes that enhance the importance of cybersecurity
- Monthly cyber awareness training
- Quarterly phishing assessments

VULNERABILITY MANAGEMENT

- Anti-virus and anti-malware installation
- Monthly security patch updates

OTHER

- Network segmentation
- Site-specific Virtual private networks (VPNs)
- Phones and printers moved to Virtual Local Area Networks (VLANs)
- Email scanning
- Cyber insurance

The utility is not done with its cybersecurity improvements. In the future, the manager intends to:

- Budget for Wi-Fi upgrades to add more VLANs so that Internet of Things (IoT) devices for physical security (e.g., video cameras) can be installed on their own secure network.

- Create a server rack with high availability clusters for backup and failover purposes, which will lead to less downtime of utility processes and operations in the event of one server's failure.
- Perform offsite backups for data redundancy.
- Remove legacy systems by replacing them with devices running a new operating system (OS) that does not use a graphical user interface (GUI). The new OS will be more resilient to attack.
- Create the utility's OT and IT protocols 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.
- Potentially develop an in-house cybersecurity laboratory or "sand box" where the utility can safely test new devices and processes before introducing them into utility networks.

LESSONS LEARNED

- Utilities should plan and budget for continuous software and hardware upgrades. To make this possible, take time to educate your Board or Commission on the value of cybersecurity so that they will be willing to support these efforts in the future.
- Educate staff as well; some cybersecurity practices may involve changes (e.g., better passwords or logon procedures), but education about the importance of such practices to the public health mission of the utility helps make such adjustments easier for staff.
- Take time to document all the improvements you are implementing. In many smaller utilities, one person may oversee making all the changes and if nothing is written down, no one will know what was done.
- Obtain cybersecurity insurance. If there is an incident, cybersecurity insurance can help to fund response and recovery actions.

READY TO BUILD YOUR CYBERSECURITY PROGRAM?

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.