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

Cybersecurity: Do What Works for You

OVERVIEW

In 2019, the office manager at a small, combined utility was the victim of an email phishing attack. Cyber criminals were able to take control of the office manager's email account and send thousands of emails to everyone in their contact list, including employees and customers, attempting to spread their attack. The utility's phones began ringing off the hook with questions about the emails that were being received. After speaking with its liability insurance provider, the utility knew it was time to improve its cybersecurity.

CYBERSECURITY APPROACH

The utility knew they needed a cybersecurity lead to oversee the improvements; however, utility management was concerned about the resources required to hire a full-time staff member for this role. After careful consideration and research, the utility contracted a small cybersecurity firm to oversee its cybersecurity program. The cybersecurity firm worked with the utility to create a cybersecurity policy, which outlined all the technical and administrative controls in place to protect the utility's assets. The cybersecurity controls implemented include:

ACCOUNT SECURITY

- Multi-Factor Authentication
- Strong and Separate Passwords
- Standard Operating Procedure for Changing Default Passwords
- Separate User and Privileged Accounts

DEVICE SECURITY

- Endpoint Detection
- Updated Inventory of all Assets
- Current Documentation and Configurations for all Assets

DATA SECURITY

- Security Logs

GOVERNANCE AND TRAINING

- Quarterly Cybersecurity Training
- Cybersecurity Posters and Signage

VULNERABILITY MANAGEMENT

- Maintaining up-to-date Operating Systems and Software
- Continuous Scanning for Vulnerabilities
- Cybersecurity Alerts
- Regular Penetration Testing

RESPONSE AND RECOVERY

- Cybersecurity Incident Response (IR) Plan
- Nightly Data Backups
- Cybersecurity Insurance

WEBSITE AND EMAIL SECURITY

- Website Filters
- Email Security Controls with Phishing Detection Enabled

The utility understands cybersecurity is a continuous process and is always looking to make improvements. While most of the utility's cybersecurity improvements have involved its Information Technology (IT) assets, it has now shifted its focus to its Operational Technology (OT) assets. Virtual Private Networks (VPNs) are currently being installed at the Raw Water Intake and Water Treatment Plant. Plans are also underway to establish regular meetings between the cybersecurity firm and the OT lead to ensure the utility has a comprehensive cybersecurity program.

LESSONS LEARNED

- Investing in cybersecurity is better than dealing with the consequences, including irate customers and potential operational disruptions, of a cyberattack. The office manager felt a tremendous amount of guilt following the 2019 cyber incident and wants to avoid a future situation like this. The utility stressed that "investing" does not always mean large sums of money. There are many free cybersecurity resources available that you should consider taking advantage of to get started.
- Cybersecurity awareness training is important. The office manager shared that an employee recently approached them with a suspicious email and was curious if it was legitimate. It was determined the email was a phishing attempt and the employee was able to detect it using the information learned from quarterly cybersecurity training.
- Be creative with your resources and think outside the box. Although approaches may vary depending on your resources, this utility elected to contract a cybersecurity firm instead of hiring a full-time staff member. The utility understood their resource constraints and was still able to develop a cybersecurity program. Cybersecurity does not always have to be a one-size-fits-all approach. Consider all your options and determine what works best for your unique situation.

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.