# WATER SECTOR CYBERSECURITY PROGRAM CASE STUDY: *Medium Combined System*

## *Cybersecurity Improvements: A Phased Approach is a Sensible Approach*

## OVERVIEW

Ten years ago, a vendor walked into the administrative building of the utility to present on the products and services they offer. The vendor connected a laptop into the building's network and commented on the brand of programmable logic controllers (PLCs) in use at the utility. It was at that moment the Operations Director realized that something had to change.

## CYBERSECURITY APPROACH

In addition to the incident described above, cyber incidents were in the news and utility staff wanted to separate operational technology (OT) and information technology (IT) assets to improve security and monitoring. With support from the utility's leadership, a budget was set aside each year to make improvements in a phased approach. To date, the utility has implemented:

### ACCOUNT SECURITY

- Multifactor authentication (MFA) for all accounts, including email

### DEVICE SECURITY

- Updated and reconfigured domain controllers
- Application download restrictions

### DATA SECURITY

- Endpoint detection and response for ransomware
- Managed detection and incident response solution
- Security Information and Event Management (SIEM)

### GOVERNANCE AND TRAINING

- Monthly cybersecurity training for all staff

### VULNERABILITY MANAGEMENT

- Access-limited USB ports on OT network devices

### RESPONSE AND RECOVERY

- Routine backup testing
- A Business Continuity Plan

### OTHER

- Redundant firewalls
- Virtual local area networks (VLANs) at every plant separated by demilitarized zones (DMZs)
- Domain Name System (DNS) filtering (third party)
- Virtual private network (VPN) protected communications
- Separate fiber cabling for OT and IT
- Email threat protection (third party)

Like many others, the utility views cybersecurity as a constantly evolving and ongoing effort. Future options being considered include Privileged Access Management (PAM) to protect against credential theft and privilege misuse, blue team/red team training (designed to improve the utility's cybersecurity), and annual penetration testing to better evaluate the security of the utility's OT and IT systems.

## LESSONS LEARNED

After ten years of ongoing cybersecurity improvements, utility operational, OT, and IT staff have many insights to share.

- First, do not try to do everything at once. Take time to learn about your utility's cybersecurity needs and phase the implementation process to make it manageable.
- Outside vendor help and consultants can be critical to success but be sure you are engaging with qualified third parties who know industrial control systems as well as IT systems (and that may not be the same firm).
- Try not to take shortcuts or cut corners to save a few dollars; one ancillary benefit the utility discovered during the process was that both their OT and IT systems' overall reliability increased as they separated those networks and invested in better and more secure assets and procedures.
- Keep your Board or Commissioners and other key stakeholders informed of both the cybersecurity needs and the progress being made. This was important to securing funding from the budget each year.
- Find out what other utilities have done too. Attending water sector association events such as conferences is a good way to network with several utilities at one time and learn what they did.
- Finally, don't forget your end user. Utility staff may be resistant to change (e.g., new login procedures) at first, so upfront explanations, discussions, and training will help to overcome these initial hesitations. Be available to answer questions; staff who feel supported are more likely to accept change as well.

## 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.