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

Air Gapping: Secure but not Foolproof

OVERVIEW

A forward-thinking Chief Executive Officer (CEO) at this utility realized years ago that cybersecurity was an emerging threat to their operations. With Board support, they hired a full-time information technology and operations Director to take on the challenge of upgrading and securing all Operational and Information Technology (OT and IT) systems at the utility.

CYBERSECURITY APPROACH

With top-down support from both the CEO and the Board, the first step the Director took included inventorying the networks owned by the utility and noting every device and its configuration. The goal was to identify all OT assets and cybersecurity gaps. Enhancements since then include:

ACCOUNT SECURITY

- Reassigned account privileges based on need

DEVICE SECURITY

- Application download restrictions with enforced procedure for download requests
- USB drives are scanned for malware prior to use in the networks

DATA SECURITY

- Traffic monitoring and logging with quarterly reports

GOVERNANCE AND TRAINING

- Regular cybersecurity training for all staff

VULNERABILITY MANAGEMENT

- Installed anti-virus software on all personal computers

RESPONSE AND RECOVERY

- Created a Cyber Incident Response Plan annex to their Emergency Response Plan

OTHER

- Air gapped SCADA systems on a dedicated intranet system and permanent VPN tunnel to main office
- Installed Virtual Local Area Networks with device traffic filtering
- Segmented OT and IT networks
- Emails links are scanned for malware
- Filter on firewall by IP address (e.g., country of origin)
- Simulated phishing tests with a third-party vendor that attempts to spoof staff every six to eight weeks
- Installed cyber locks on all remote facilities to replace key access
- Installed video cameras to observe facility activity

The utility is planning the following: SCADA upgrade to a hosted version with multi-factor authentication (MFA) at a water treatment plant, tracking staff door swipes at all facilities, and installing more physical security to protect cyber assets from both outsider and insider threats. In addition, the utility will implement more *Zero Trust* strategies as its cybersecurity program matures.

LESSONS LEARNED

- Understand account access privileges. This utility shared that at the start of their cybersecurity risk mitigation project they knew very little about their OT and IT systems and what login privileges were available to staff. To their surprise, over 65 staff had full Administrator privileges even though not everyone's position required this level of access. One of their first steps was to rollback privileges to match job roles.

- Air-gapping is preventive, but not absolute. This utility also uses air gapping to prevent hackers from gaining access to their SCADA systems, but they know air gapping a SCADA system is not 100% secure. You still need to control staff and vendor access to SCADA, perform software updates and patches, scan outside devices plugging directly into SCADA, and install anti-virus and malware protection on all work terminals. Based on staff demand, this utility is considering allowing remote SCADA access for some users but is investigating the safeguards that can be put into place to make remote access as secure as possible.

- Key leadership support is important. Finally, if you can, convincing utility leadership and your Board to support cybersecurity is critical. With this support, you can implement improved cybersecurity measures through time, do your research, and know that a budget will be set aside each year for upgrades. And, like many things, cybersecurity is not "one and done." It is a continual process so plan on making changes and updates every year.

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.