WATER SECTOR CYBERSECURITY BRIEF FOR STATES

Introduction

Implementing cybersecurity best practices is critical for water and wastewater utilities. Cyber-attacks are a growing threat to critical infrastructure sectors, including water and wastewater systems. Many critical infrastructure facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation.

Cyber Threats to Water and Wastewater Systems

Cyber-attacks on water or wastewater utility business enterprise or process control systems can cause significant harm, such as:

- Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment;
- Deface the utility's website or compromise the email system;
- Steal customers' personal data or credit card information from the utility's billing system; and
- Install malicious programs like ransomware, which can disable business enterprise or process control operations.

These attacks can: compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liabilities.

Benefits of a Cybersecurity Program

The good news is that cybersecurity best practices can be very effective in eliminating the vulnerabilities that cyber-attacks exploit. Implementing a basic cybersecurity program can:

- Ensure the integrity of process control systems;
- Protect sensitive utility and customer information;
- Reduce legal liabilities if customer or employee personal information is stolen; and
- Maintain customer confidence.

Challenges for Utilities in Starting a Cybersecurity Program

Many water and wastewater utilities, particularly small systems, lack the resources for information technology (IT) and security specialists to assist them with starting a cybersecurity program. Utility personnel may believe that cyber-attacks do not present a risk to their systems or feel that they lack the technical capability to improve their cybersecurity.

Be assured, however, that basic cybersecurity best practices can be carried out by utility personnel without specialized training, and user-friendly resources are available to help. You just have to know how to start and where to look!

WATER SECTOR CYBERSECURITY BRIEF FOR STATES

How to Use This Brief

EPA developed this brief in cooperation with the Association of State Drinking Water Administrators' Security Committee to help state staff (or their designated assistance providers) start a conversation with utilities about cybersecurity. Information gathered from the questions on this page can help you to understand a utility's current cybersecurity practices and point them toward resources to enhance their program. You may also leave the next two pages with the utility as a reminder of your discussions. Those pages provide recommendations for building a cybersecurity program and responding to cyber-attacks.

10 Questions for a Cybersecurity Dialogue with a Utility*

Does your utility …

1. **Keep an inventory of control system devices and ensure this equipment is not exposed to networks outside the utility?**
   - Never allow any machine on the control network to "talk" directly to a machine on the business network or on the Internet.
2. **Segregate networks and apply firewalls?**
   - Classify IT assets, data, and personnel into specific groups, and restrict access to these groups.
3. **Use secure remote access methods?**
   - A secure method, like a virtual private network, should be used if remote access is required.
4. **Establish roles to control access to different networks and log system users?**
   - Role-based controls will grant or deny access to network resources based on job functions.
5. **Require strong passwords and password management practices?**
   - Use strong passwords and have different passwords for different accounts.
6. **Stay aware of vulnerabilities and implement patches and updates when needed?**
   - Monitor for and apply IT system patches and updates.
7. **Enforce policies for the security of mobile devices?**
   - Limit the use of mobile devices on your networks and ensure devices are password protected.
8. **Have an employee cybersecurity training program?**
   - All employees should receive regular cybersecurity training.
9. **Involve utility executives in cybersecurity?**
   - Organizational leaders are often unaware of cybersecurity threats and needs.
10. **Monitor for network intrusions and have a plan in place to respond?**
    - Be capable of detecting a compromise quickly and executing an incident response plan.
11. For more information about each of these questions, see WaterISAC *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* at https://www.waterisac.org/fundamentals.

Taking the Next Step with a Utility

If utility staff can knock each of these questions/answers out of the park, then the utility has a good cybersecurity program in place. However, if the response to these questions is "No," "Not sure," or "How about this weather?" then encourage the utility to use the next page to start building a cybersecurity program.

IMPLEMENTING A CYBERSECURITY PROGRAM AT YOUR WATER OR WASTEWATER UTILITY

Cybersecurity Worksheet

Use this worksheet as recommendations for an effective cybersecurity program. Talk to your IT service providers and others who manage your IT systems about how to carry out these actions at your utility.

Action	Notes	Date Completed
Audit IT systems and identify vulnerabilities		
Keep a list of the highest cybersecurity risks and how they will be addressed		
Ensure all IT systems have up-to-date antivirus and anti-malware software		
Install security patches on all IT systems on a monthly basis		
Implement secure remote access practices		
Segregate networks and control access to networks based on job function		
Monitor networks for suspicious activity and be prepared to respond if detected		
Establish strong password policies		
Consider "application whitelisting" on critical systems (allow execution of approved files only)		
Improve physical security for IT equipment		
Segregate business enterprise and process control systems, and require separate credentials for access		
Establish secure policies for mobile devices		
Develop a contingency and disaster recovery plan for critical IT systems		
Develop and exercise SOPs for manual operation of utility processes if control systems are compromised		
Implement redundancies in your system to limit service outages		
Conduct cybersecurity training for utility staff and contractors		

IMPLEMENTING A CYBERSECURITY PROGRAM AT YOUR WATER OR WASTEWATER UTILITY

Steps for Responding to a Suspected Cyber Incident at a Water or Wastewater Utility

Response

1. Disconnect compromised computers from the network. Do *not* turn off or reboot systems.
2. Assess the scope of the compromise, and isolate all affected IT systems.
3. Open a ticket with your antivirus software or security service vendor.
4. Assess any potential damage, including impacts to treatment processes or service disruptions.
5. Initiate manual operation of equipment if control systems have been compromised.
6. Distribute any advisories or alerts to customers as needed, including customers whose records may have been compromised.
7. Identify methods to scan all IT assets to eradicate malicious code. Assess and implement recovery procedures.

Reporting

1. Report the incident to local law enforcement and the primary oversight agency (typically, the state).
2. Contact the DHS Cybersecurity and Infrastructure Security Agency (CISA) at https://www.cisa.gov/reporting-cyber-incidents. CISA can assist your utility with identifying and restoring affected systems, coordinating federal assistance, and improving security.
3. Submit an incident report through WaterISAC (analyst@waterisac.org; 866-H2O-ISAC).

Important Contact Information

Role	Point of Contact	Phone Number	Email
IT service vendor			
Local law enforcement			
State agency			
Cybersecurity and Infrastructure Security Agency (CISA)			https://www.cisa.gov/reporting-cyber-incidents
WaterISAC		866-H2O-ISAC	analyst@waterisac.org

For More Information

For more information on available cybersecurity guidance and resources:

- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- DHS Cybersecurity and Infrastructure Security Agency
- American Water Works Association (AWWA) Resources on Cybersecurity
- EPA Cybersecurity Incident Action Checklist