EPA Drinking Water Security, Preparedness and Resilience

Patti Kay Wisniewski
EPA Drinking Water Security, Preparedness and Resilience Coordinator
cell: 215-514-7893
Wisniewski.patti-kay@epa.gov

Be Proactive about Cybersecurity – You will sleep better at night

Many things will keep water suppliers up at night -- supply chain issues, COVID illnesses of staff, family and friends, approaching severe weather and cybersecurity breaches. There are numerous resources to assist water suppliers with unraveling the complicated web of how someone can attack the IT of a water system. But the key is to begin to take steps now to protect our infrastructure and to continue to provide safe drinking water.

WHY: Water systems have been attacked and this will very likely happen again. It is important to minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to: interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment; theft of customers' personal data such as credit card information or Social Security numbers stored in on-line billing systems; loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes, encrypted data files and more. Any of these impacts can erode public confidence in water supply safety.

WHAT: According to IBM, cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. In 2020, the average cost of a data breach was $3.86 million globally, and $8.64 million in the United States.

WHO: All water utilities need to understand the problem and be proactive in addressing it. State primacy agencies need to address the status of cybersecurity programs during site visits such as sanitary surveys and share resources for improvements with water suppliers. EPA will develop guidance and conduct training for sanitary survey inspectors and water suppliers. It is anticipated that the Department of Homeland Security DHS, will issue cybersecurity performance goals for critical infrastructure control systems.

WHEN: *NOW!* Don't be overwhelmed by the myriad of ways you could be attacked or the tremendous amount of resources that exist to assist you. "Just do it," as Nike says. Think of Spring as the time to spring into action to protect your IT system.

If you have completed your risk and resilience assessment (RRA) and have updated your emergency response plan (ERP) as required under the America's Water Infrastructure Act, but failed to include addressing cybersecurity events, do this now. The RRA should cover electronic, computer, or other automated systems and the security of such systems. An ERP should include strategies and resources to improve the resilience of the system, including physical security and cybersecurity of the water system. In addition, the ERP should include plans to address malevolent acts, which is what a cyber-attack is considered.

HOW: Here are some ideas to get you started but this is not an exhaustive list.

Follow the recommendations in EPA's Cyber Incident Action Checklist to prepare, respond and recovery from an attack. https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf

Develop a cybersecurity culture by training staff and establishing and enforcing policies.

Be suspicious of emails. Curb your curiosity to open all emails and click on links. Don't trust anyone unless you know them and yet, you still need to be cautious and leery of anything that does not look or feel right.

Require changing of passwords every 90 days and do not allow sharing of passwords.

Use multi-factor authentication: what you have and what you know (similar to how most banks require you to log into your account by sending you a text with a code to your cell phone or email).

Revoke/inactivate credentials of former employees.

Keep software up to date and install patches when available.

Limit remote access and allow only for those with a verified operational need.

Practice shifting to manual operations to be more familiar if or when the need arises.

Back up data and store off-line, allowing for easier restoration if data is lost, stolen or encrypted.

Keep servers in a secure room, lock the door and limit access.

Keep billing IT separate from SCADA IT.

Consider cybersecurity when undertaking other projects so it isn't an add-on or an after-thought.

Sign up for a FREE, confidential, cybersecurity assessment and technical assistance offered by EPA's contractors at https://horsleywitten.com/cybersecurityutilities/

WHERE: Numerous resources exist and advisories are shared by CISA, EPA, AWWA, WaterISAC to name a few. Many are free and without membership subscriptions. Sign up for these and stay on top of updating software.

EPA: https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector

CISA Advisories: https://www.cisa.gov/uscert/ncas/alerts; subscribe at the link at the bottom of their page.

WaterISAC: https://www.waterisac.org/fundamentals

AWWA: https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

WHO (again): Consider reporting events to the WaterISAC which compiles water sector incident information to share with the sector. This assists other water suppliers with knowing what events are occurring across the sector. Information shared is done anonymously. https://www.waterisac.org/report-incident

Capture response assistance contacts, such as the Critical Infrastructure Security Agency (CISA) per the Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government (https://www.dhs.gov/publication/cyber-incident-reporting-unified-message-reporting-federal-government) which explains when, what, and how to report a cyber incident to the federal government. Key contact information is:

Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov/
To report incidents, phishing, malware, or vulnerabilities:
Online forms: https://www.cisa.gov/uscert/report
Email CISA Service Desk: cisaservicedesk@cisa.dhs.gov
Phone: 888-282-0870

Federal Bureau of Investigation (FBI)
https://www.fbi.gov

Finally, remember to capture your planned response and recovery actions in emergency response plans and Continuity of Operation Plans and exercise these plans at least annually. If an event has occurred be sure to conduct an after-action review, capture ideas for improvements in your plans and provide additional staff training.

Taking steps now to further protect your water system will help you sleep at night. At least until the next storm is heading your way.

Patti Kay Wisniewski
EPA Drinking Water Security, Preparedness and Resilience Coordinator
cell: 215-514-7893
Wisniewski.patti-kay@epa.gov