OPERATIONAL TECHNOLOGY ESSENTIAL TRAINING

Bridging the Gap Between IT and OT for Water and Wastewater

State of Kansas: Office of IT Services

Category: Cybersecurity

Initiated: February 2020

Completed: September 2023

Allie Denning

Director, Public Affairs

Allie.Denning@ks.gov

(O) 785-296-4112

Executive Summary

Critical infrastructure is increasingly vulnerable to cyber-attacks, and among the most vulnerable are water and wastewater facilities. In July 2023, the Kansas Department of Health and Environment (KDHE), the Kansas Information Security Office (KISO), and the Cybersecurity and Infrastructure Security Agency (CISA) joined forces to launch an Operational Technology Training program for Water/Wastewater operators across Kansas. This comprehensive training initiative serves a dual purpose:

1. Equip operators with the knowledge to identify cyber technology within their facilities.
2. Assist them in conducting self-assessments to bolster readiness for future external security audits.

By enhancing the cybersecurity posture of our water/wastewater infrastructure through education and training, the initiative aims to safeguard critical assets and ensure the continuity of essential services.

Idea

The security of our water and wastewater critical infrastructure is paramount to ensuring safe drinking water and safeguarding public health in Kansas.

The Environmental Protection Agency (EPA) memorandum of 2021 highlighted the vulnerabilities inherent in public water systems (PWSs) and the challenges they face in addressing cybersecurity concerns. These challenges include limited financial resources, disparate expertise and knowledge, the need for assessments to adapt to evolving cyber threats, and a shortage of staff.

The memorandum proposed the use of self-assessments in sanitary surveys, offering states the option to develop their own programs for water cybersecurity. This prompted the partnership between the KISO, KDHE, and CISA beginning in July 2023.

Kansas has a diverse array of water and wastewater systems, each with its own unique hurdles due to variations in size, age, infrastructure, and resource constraints. Moreover, the pervasive lack of financial resources and staff exacerbated the cybersecurity void across the state.

Recognizing the absence of a one-size-fits-all solution, our agencies concluded that the most effective approach to bolstering cybersecurity in Kansas was to leverage their collective expertise and resources through educational awareness and training over the course of four phases:

- Phase 1: January 2024 - Outreach and training for water operators
- Phase 2: Survey and OT Identification
- Phase 3: Self-Assessment
- Phase 4: Follow-Up and Next Steps

Implementation

PHASE 1: January 2024 - Outreach and Training for Water Operators

Despite the absence of a budget, we adopted a resourceful approach.

Commencing in January 2024, the KISO, KDHE and CISA embarked on a series of educational campaigns and training sessions in six communities across the State of Kansas. Given Kansas's predominantly rural landscape, we utilized our network of local partners to identify suitable training locations in Hays, Garden City, Salina, Wichita, Pittsburg, and Topeka. These sessions empowered water and wastewater operators with knowledge on operational technology (OT) and its identification.

We collaborated with Sam Alva from CISA to develop a tailored curriculum aimed at bridging the IT-OT gap. Additionally, we maximized available resources by providing free training materials through platforms like Texas A&M extension and the federal virtual training environment (Fed VTE) courses.

One of the trainings can be viewed online at https://www.youtube.com/watch?v=Lwl6xuVOpIw.

PHASE 2: Survey and OT Identification

Subsequent to the training, PWS operators will complete a brief survey comprising 3-4 questions to ascertain the presence of operational technology (OT) in their systems and/or environments.

PHASE 3: Self-Assessment

PWS systems identified as having OT will complete an electronic assessment aligned with CISA's cybersecurity performance goals (CPGs).

PHASE 4: Follow-Up and Next Steps

The KISO and/or CISA will offer follow-up support and technical assistance to PWS systems that identify vulnerabilities during their assessments. The KISO will also provide assistance to operators with annual testing of their plans through tabletop or functional exercises.

Continued support will be available to PWS systems as workshops are scheduled throughout the state. These workshops, hosted by the KISO, KDHE, and CISA, will assist water operators in formulating incident response plans tailored to their specific environments. This initiative, currently under development by CISA, is slated for deployment across Kansas in Q4 2024 or Q1 2025.

Additionally, PWSs encountering critical needs but lacking immediate financial resources can explore funding avenues through the Department of Homeland Security and the State and Local Cybersecurity Grant Programs.

Impact

Impacts and Measuring Success

While the project is still in its nascent stages, early indications already demonstrate its significant impact on enhancing cybersecurity resilience in water and wastewater systems. One key metric of success is the noticeable improvement in operator awareness and knowledge, leading to enhanced cyber hygiene practices and an increased ability to mitigate potential threats from malicious actors.

The project also serves as a blueprint for future endeavors in critical infrastructure protection. By pioneering a replicable model, we have unlocked a scalable solution that transcends geographical boundaries. Any jurisdiction across the country can leverage our framework to enhance cybersecurity in their water and wastewater systems. Thus, our project not only addresses the immediate needs of Kansas's water and wastewater operators but also lays the groundwork for nationwide cybersecurity resilience in critical infrastructure.

Since the launch of the project, its innovative approach has garnered widespread recognition, elevating the profile of water and wastewater cybersecurity on a national scale. This heightened visibility is evidenced by notable achievements such as the invitation extended to the KDHE to provide testimony before the United States Congress on January 31, 2024. Additionally, Government Technology featured the project in a story published in February, highlighting its pioneering efforts in the field of critical infrastructure protection. The KISO and CISA also hosted an operational technology training for public entities as a precursor to our annual cybersecurity summit in April 2024.

Looking Ahead

These early successes pave the way for continued progress and resilience in the cybersecurity landscape of Kansas. Looking to the end of this year, we are poised to host further workshops, empowering operators to craft incident response plans tailored to their systems' needs.

As the project evolves, we anticipate a tangible reduction in successful cyber-attacks targeting the water and wastewater sector across the State of Kansas. This anticipated decrease in cyber incidents underscores the project's efficacy in fortifying critical infrastructure and safeguarding public health and safety.

TESTIMONIALS

Kansas Department of Health and Environment

"Kansas is leading the nation in its approach to help secure water and wastewater infrastructure from cyber attacks. At a recent meeting in Washington, D.C., I served on a panel with cybersecurity professionals who expressed a keen interest in our work, with some individuals commenting that we can be a model for the rest of the country."

– Cathy Tucker-Vogel, Section Chief, Public Water Supply Section, Kansas Department of Health and Environment

"The collaboration between CISA, KDHE, and KISO grew out of a need to protect our nation's most critical asset, water/wastewater. CISA, along with KISO and KDHE, decided to develop an Operational Technology (OT) training plan that would provide resilience and reduce the attack surface for water/wastewater. The OT training plan consists of a four-phase approach. Phase one provides OT essential training, giving operators who are the first line of defense the ability to understand their OT environment. Phase two provides operators and asset owners the ability to develop and execute an incident response plan, which will reduce the impact of operations and increase the recovery time objective if affected by a ransomware attack. Phase three continues to develop water/wastewater operators' knowledge in the OT environment, enhancing their abilities to manage the OT environment. Phase 4 will include ongoing support and technical assistance. With the assistance of KDHE and the Kansas Municipal Utilities (KMU), our training has reached many of Kansas' 105 counties, increasing the awareness of threats to OT."

– Samuel Alva, Sector Specific CPG Advisor, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency