PNWS-AWWA Water Information Technology Committee

Synergizing the Water Industry with Technology

March 2024

Purpose: The goal is to equip water purveyors with current available technologies in order to improve their day-to-day operations and to disseminate information on risks and vulnerabilities with technologies.

Mission: One way to do it is to educate, by providing technical training for water operators responsible in managing their infrastructure. The topics that seem to be relevant at the time are:

- GIS and all of its components and advantages to the industry
- Finance and administrative components that utilizes technology
- Cybersecurity and managing employees to deal with the unknowns in the tech world
- The disconnect between IT departments and operations
- Cloud computing (Azure, etc.)

Proposed Date & Time and Venue:

May 23rd, 2024
Pierce County Environmental Services Building

Proposed Agenda:

Each session is geared for 50 minutes, plus 10 minutes Q&A

Session 1: What It Takes To Utilize GIS To Improve Operations

Speaker & Co-Speaker: Shawn Buck, Covington Water District. Xiuxia Liu, Northshore Utility District, and Kevin Wyckoff, Lakewood Water District

Course Abstract: Presenters will describe how their agencies use Commercial Off the Shelf (COTS) software solutions to improve utility field operations. Implemented solutions that will be demonstrated and discussed include public facing applications for notifying customers of outages, connecting applications through the use of hyperlinks, Water Meter and System Valve Inspection Solutions, Collecting and Sharing GPS Data in Web Maps. The intent is to provide non-Information Technology Staff with an idea of the kinds of tools that can easily be built and deployed at their organizations.

Session 2: Water In The Cloud - The Good & Bad

Speaker & Co-Speaker: Ian Moore, CISSP DHS CISA

Course Abstract: Ian Moore will present on the cybersecurity challenges and best-practices related to a water organization moving to the cloud. He identifies the critical pieces and parts of cloud development and deployment that must be considered and secured in the design and planning phases. Ian will shine some light on the current cyber risks and threats related to cloud environments and the activities that should be taken to ensure a more secure deployment. Lastly, Ian will connect the audience with the various resources that CISA can provide that can help secure a cloud deployment.

Session 3: What The Future Brings For AI To The Water Industry

Speaker & Co-Speaker: Alex Salazar, CISSP DHS CISA & Tim Loosier, Baseform

Course Abstract: Artificial Intelligence has become the buzzword of 2023-24. The concept of Artificial Intelligence has been around for decades, but recent breakthroughs led to the widespread access of its capabilities via GPT's. Join Alex Salazar as he talks about what is AI, it's current capabilities, and what it means for cybersecurity. You will also hear about the Cybersecurity and Infrastructure Security Agencies (CISA) guidance on AI and protecting Critical Infrastructure.

Session 4: The Needed Change Of Habit - Addressing Cybersecurity

Speaker: Chris Callahan, CISSP DHS CISA

Course Abstract: Chris Callahan will present the use case of CyberAvengers and recent attacks on US Water Utilities, he will describe best OT practices and ways to protect against similar cyber-attacks. The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona "CyberAv3ngers" are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies. In addition to the recent CISA Alert, the authoring agencies are releasing this joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with IRGC cyber operations.