GENERAL SYLLABUS

Cyber-Resilience Through Manual Operations: Engineering and Operations Lessons Learned

Presented by: West Yost Associates

When the SCADA system at a water or wastewater utility is compromised by malware or shut down by a cyber-attack, the essential services that the utility provides the community can be suspended. The negative impacts that service interruptions can have on community health, utility financial standing and reputation can persist well beyond the duration of the attack.

Cybersecurity organizations like CISA (Cybersecurity & Infrastructure Security Agency) have recently warned that cyber-attacks may increase in the near term due to heightened international tension. CISA has issued several recommendations on how utilities can improve the resilience of their systems including ensuring that manual system operations can be maintained while control systems or communications networks within the utility are inoperable.

Since many SCADA systems were developed to replace manual operations, West Yost has developed this training course to help utility leaders, engineers, operations staff, and IT/SCADA cybersecurity staff better understand how manual operations can be implemented to maintain essential services under a sustained cyber-attack. West Yost is partnered with leading cybersecurity experts at the Idaho National Laboratory and American Water Works (AWWA) to bring Cyber-Informed, Consequence-Driven Engineering to the water and wastewater sector. CCE emphasizes the need for cyber-physical resilience which includes maintaining operations in the absence of automation.

This course has been developed through West Yost's extensive experience to raise awareness and provide insights on how to limit the consequences of a range of cyber risks that have emerged over the last 20 years and those yet to emerge.

Course Outline and Objectives

This workshop will provide utility leaders, engineers, operations staff, and IT/SCADA cybersecurity staff with immediate steps that they can take to improve the resilience of their SCADA systems and their organizations to cyber-attack.

Case studies will be presented detailing how automation systems need to be deconstructed to identify engineering and operational issues and implement specific changes to enable manual operations during a cyber-attack.

A tabletop exercise is explained to help participants assess their ability to perform manual operations in a stepwise fashion to improve their organizations' capabilities, document manual operating procedures, inform ongoing training, and create a culture of resilience that will improve all-hazards resilience.

Learning Objectives:

- Describe the contents of recent CISA/U.S. Environmental Protection Agency/Water Information Sharing and Analysis Center (WaterISAC).
- Describe current climate of geopolitics and potential impact on cyber security for water and wastewater utilities.
- List types of cyber threats facing the water sector.
- Describe how better engineering practices will improve cyber resilience and how to maintain essential services while also ensuring regulatory compliance.
- Describe methods to confirm the ability to run systems manually in the absence of automation.