BAYWORK Water Industry Summit

Session One: Building Cyber Resilience

Andrew Ohrt, West Yost, Moderator

Panelists:

- Don Hester (US Dept. of Homeland Security/CISA)
- Bill Johnson (East Bay Municipal Utility District)
- Cecil Lawson (Valley Water)
- Raphael Okubo (Contra Costa Water District)


Cybersecurity
Orientation

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

Iran-affiliated and pro-Russia cyber actors gained access to and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise, as they are commonly connected to corporate IT networks and increasingly to the Internet. Many operators face numerous competing priorities, such as physical facilities operations and maintenance, which further constrains the time and resources that operators can dedicate to cybersecurity practices. Furthermore, the limited number of ICS vendors, wide availability of product configurations, and operational commonalities across the water sector make it easier for cyber actors to compromise vulnerable systems.

IRGC-affiliated "Cyber Av3ngers" compromise Unitronics programmable logic controllers (PLCs)

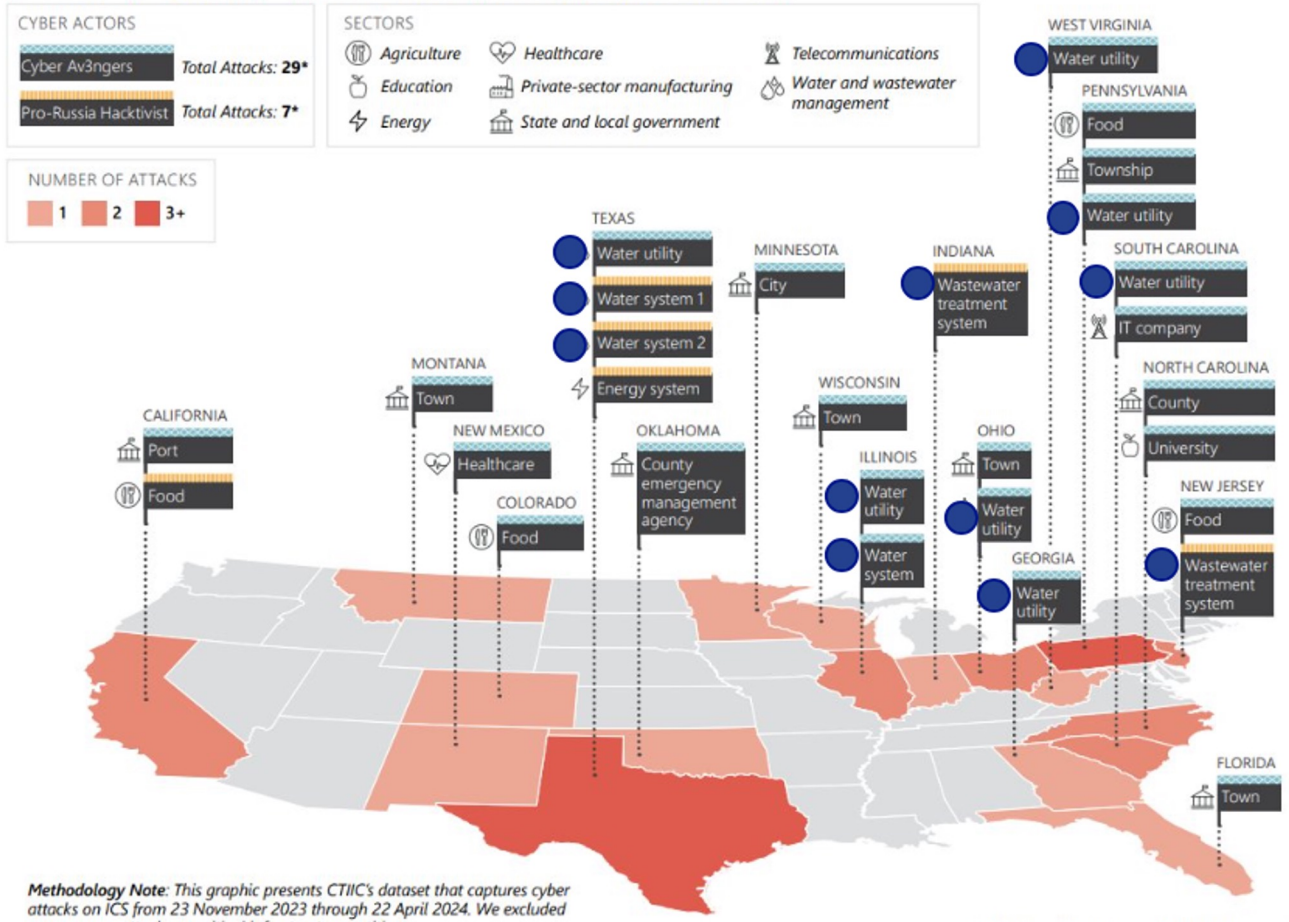
In November 2023, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained access to the Israeli-made Unitronics Series ICS PLCs in multiple US entities, mostly water and wastewater systems, and defaced the PLCs' touch screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations.

Pro-Russia hacktivist compromised several water plants and claimed to compromise two dairies

A pro-Russia hacktivist remotely manipulated control systems within five water and wastewater systems and two dairies. The actors have typically accessed the ICS components via control interfaces with public-facing IP addresses.

- On 20 and 24 April 2024, the group posted videos showing an attacker remotely manipulating settings on human-machine interfaces (HMIs) within two US wastewater systems and one purported US energy company.
- On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks.
- On 23 and 27 November 2023, the group also claimed on its public Telegram channel that it had attacked two US dairy systems.

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024

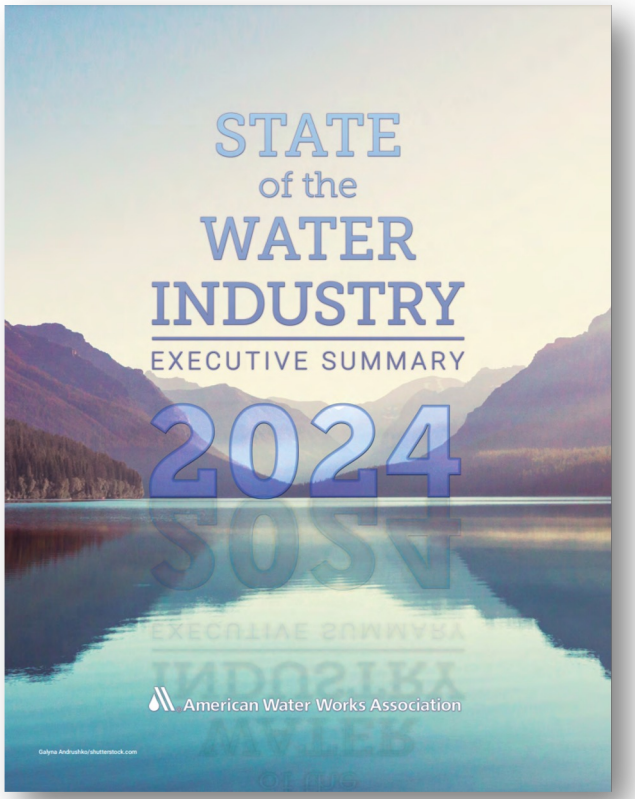


***Methodology Note**: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.*

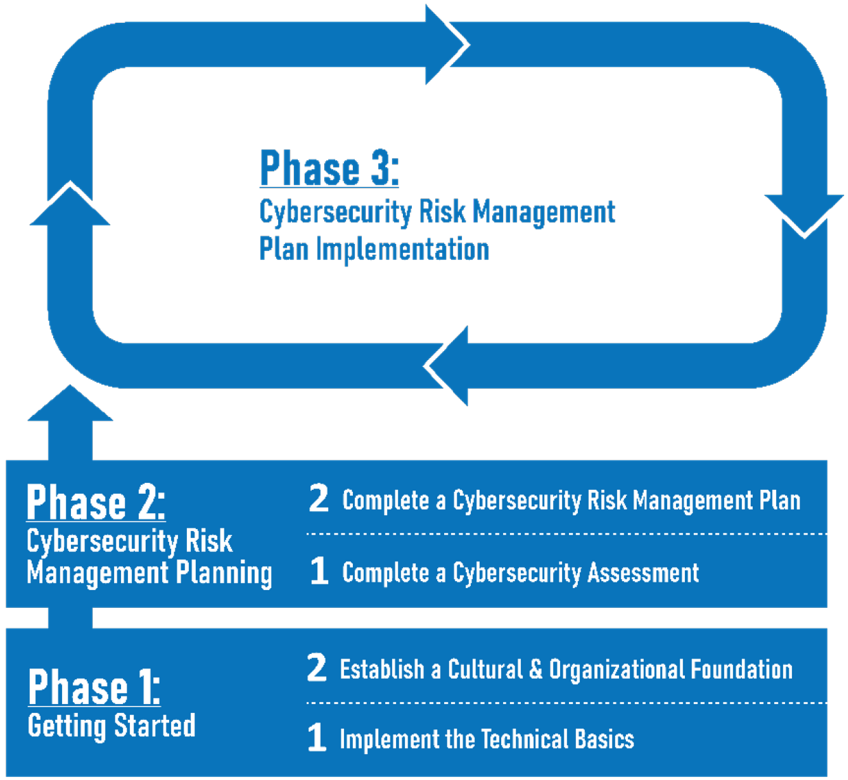
*Including seven attacks at additional US locations.

Point of Reference – #1

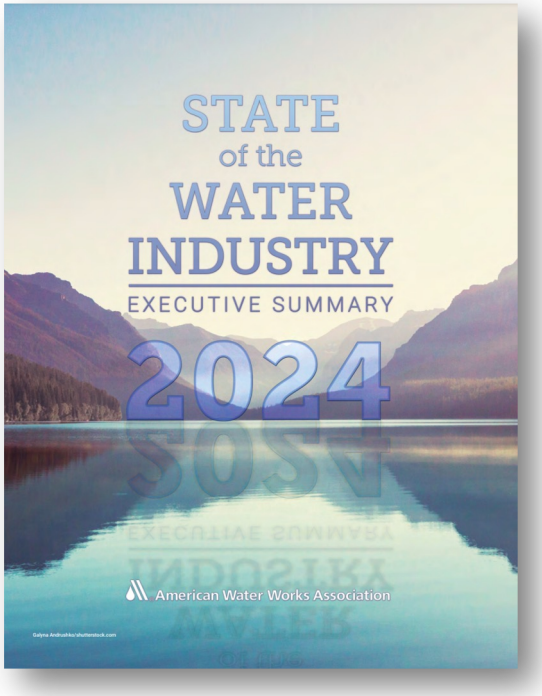
Point of Reference – #2



AWWA's Evolution of Resources



Point of Reference – #3



Andrew's Advice to Chad

1. Work with CISA
2. Create a cybersecurity line item in your budget
3. Determine your ability to operate in the absence of automation

But Don’t Take it From Me

Valley Water

Clean Water • Healthy Environment • Flood Protection

CCWD


Panel Discussion

Cybersecurity Threats

Cecil Lawson, Deputy Administrative Officer
Valley Water

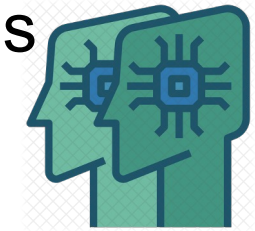
Risk: Targeted threats, water…

- **Nation-states:** well-resourced groups with political or economic motivations.
- **Benefactors:** China, Russia, North Korea*
- **Targets:** disrupt Critical Infrastructure
- **Operational Threat:** Stagnation

*Technology pirates: England (Sir Francis Drake) and Spain, 1694

AI and OT: Is the juice worth the squeeze?

- Information Technology mission
  - Operational efficacy
- The next frontier – AI and OT (SCADA)
  - Air Gapped (no connection)
  - Data Diode (unidirectional network)
  - Digital Twins



BAYWORK Water Industry Summit

Breakout Discussion One:
Building Cyber Resilience

- ❑ Introductions – 5 min.
- ❑ Assign roles (i.e. note-taker/presenter) – 5 min.
- ❑ Work through exercise modules – 35 min.
- ❑ Present key points to the larger group – 15 min.

Instructions for the Discussion

- Listen to situational update provided by the facilitators.
- Once the situational update is complete, openly discuss as a group responses to the scenario and the questions provided.
- Ask questions through the facilitators; facilitators will direct responses.
- Evaluators will record major actions, decisions, and discussion contents.

Module Format

There are two slides per module…

1st slide – Situational update

2nd slide – Questions for open discussion

The Scenario

- The Baywork W/WW Utility provides potable water treatment and sanitation for a community of 25,000.
- The OT utility staff (operations & distribution) and the IT staff have a good working relationship.
- OT relies on IT for any connection to the internet.

Module 1: Remote Pump Station HMI Not Responsive

- Day 1 – CISA releases an Industrial Control System (ICS) alert regarding a widely exploited security vulnerability in a remote radio network-capable device of which your organization has multiple.
- Day 2 – A distribution operator notices communication errors generated at a remote Pump Station. The operator travels to the site and finds the local controls are working as expected.
- Day 3 – An operator in the treatment plant control room notices that values and statuses from the remote Pump Station (PS) section on the SCADA HMI are not updating. The operator finds that the pumps do not seem to be responding to start/stop commands sent from the main control center.

Module 1 *Discussion Questions*

1. Would your organization receive the alert described in this scenario? If so, what action would you take?

2. What actions, if any, would your organization take based on this information?

3. Who within the Operations group is responsible for correlating events and sharing information on automation and communications loss across your organization?

4. Should the operators contact any other insider or outside support for help to resolve the issue?

Module 2: Remote Pump Station and Treatment HMI non-responsive

- Day 4 – Operators notify their supervisors that SCADA HMI values and some portions of the treatment process are not responding to set points or start/stop requests through the SCADA HMI. Later in the day, the remote Pump Station section of the SCADA HMI stops updating again.
- Day 5 – Operators receive alarms and find that SCADA HMI values for influent flow to Treatment and the remote Pump Stations pressure and associated storage tank level have stopped updating.
- Day 9 – Leadership authorizes external support from a contracted SCADA automation consultant. The consultant accesses the OT network remotely to begin troubleshooting the issues.

Module 2 *Discussion Questions*

1. What security training/certifications/experience is required for internal personnel and/or vendors/consultants to obtain remote network access?

2. What security-related training does each department, or your organization provide to, or require of IT/OT personnel with access to your OT-ICS-SCADA systems?

3. Does your organization have established security policies that provide standards and guidance for auditing, logging, and monitoring OT-ICS-SCADA systems? What actions should Operations and Distribution personnel be taking with these new events occurring?

4. Should Operations provide updates to anyone outside of the OT-ICS-SCADA groups (e.g. other operators, management, third-parties, etc.)?

5. Any thoughts on whether or not to isolate the OT-ICS-SCADA network from other networks?

Module 3: System-Wide Data Loss

- Day 9 – IT/OT personnel are finishing their shifts or have already left to go home. An operator notices that HMI screens are not displaying any trend data. A lab technician reports that Excel spreadsheets containing lab information and regulatory reporting data are no longer accessible.
- Day 9 – The utility's SCADA consultant is called to come on site to investigate. The consultant finds that the SCADA Servers storing the lab's Excel spreadsheets and the Data Historians databases have all been encrypted.
- Day 9 – The GM receives an email noting that the utility's SCADA files have been encrypted, and they can be recovered by making a payment.

Module 3 Discussion Questions

1. Is your organization capable of 100% manual operations for OT-ICS-SCADA processes? For how long?

2. What additional internal and external resources would you engage?

3. How are response activities coordinated between different departments and levels of personnel within your organization?

4. How long until Operations can trust the OT system again?

5. Should the organization report the cyber-attack to any external entities?

Conclusion: Forensic Analysis Completed

The utility's CIRP is activated. The systems are restored from immutable backups and safe return to normal operations is achieved.

Conclusion:

The investigation reveals that the attackers were able to establish a persistent connection, conduct reconnaissance on the network, and inject malicious code to select devices.

Through the persistent connection, the attacker was able to execute the Ransomware payload and encrypt the data servers on the OT-ICS-SCADA network.

Based on the forensic evidence, it appears the attackers mission objective was to cause disruption and financial gain.


baywork
Bay area water/wastewater workforce reliability
WATER INDUSTRY SUMMIT
THANK YOU!!