
CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

THE CYBER THREATS ARE REAL: WHAT YOU NEED TO KNOW

Clyde Roark
Gulf Coast Cybersecurity Advisor, Region 4
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

Major Cyber Threats To Water/Wastewater

Ransomware:

- Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable
  - Medusa (ransomware as a service)
  - Clop



Volt Typhoon

- People's Republic of China State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Nation State Cyber Actors:

- CISA and FBI are actively triaging a growing number of incidents involving publicly internet-facing PLCs operating in remote mode. Several dozen entities nationwide have been affected—primarily small and rural systems, though mid-size utilities are beginning to report similar issues

Commonly Used Terms

Information Technology (IT)

The systems that collect, store, and process data.

Operational Technology (OT)

Hardware or software that detects or cause a change, through direct monitoring of industrial equipment.

Port

A virtual point where network connections start and end

Firewall

A device that restricts data communication traffic between two connected networks

Software

Programs and data stored in hardware and used by a computer

Hardware

The physical components of a system (computer, etc.)

Operating System

A software that controls the operation of a computer and directs the processing of programs

Cyber Threats to Water Systems

- The good news: each community is divided into their own command and control systems. The bad news: each community is divided into their own command and control systems.
- “When we think about cybersecurity and cyber threats in the water sector, this is not a hypothetical. This is happening right now. We have seen these types of attacks from California to Florida, Kansas, Maine, and Nevada.” - EPA Assistant Administrator for Water Radhika Fox
- A community, for the most part, can survive without electricity for a week or more. We cannot survive a few days without water.
- https://www.latimes.com/california/story/2023-05-08/is-californias-water-infrastructure-at-risk-of-attack

Why and Who would attack Water/Wastewater Systems

- **Why? WWS Is An Easy Target and Demands Attention**
  - IT/OT convergence increases threat attack surface
  - Typically, low cybersecurity resources.
  - Poor cyber hygiene and network segmentation
- **Who? Anyone, Anybody**
  - Strong organized state actors attempting to disrupt our way of life
  - Mid to low level criminals looking for a quick buck or make a political statement
  - You! Insider threats from accidental everyday operations to disgruntle employees



Nation State Cyber Actors Vs You



Clyde Roark
July 27, 2023

IRAN VS US WATER SECTOR Explained

- **Iran wishes to destroy or disrupt water/wastewater operations**
- **Foreign cyber actors are breaking into internet-connected control equipment** (PLCs) used in water and wastewater systems, especially when those devices are directly reachable from the internet. This includes SCADA systems connected via cellular mobile service exposed to the internet. [cisa.gov]
- **Attackers can change what operators see** on SCADA/HMI screens, hiding real problems and causing systems to run in unsafe ways (for example, disabling alarms or altering chemical/pressure settings).
- **Current tactics include targeting PLCs without passwords**, applying actor-controlled passwords, and changing IP addresses, resulting in lockouts and stoppages



Iranian Capabilities

- Iran does NOT have the same military might as the US, ex: NAVY
  - United States: ~234 ships, including 18 aircraft carriers and 65 submarines.
  - Iran: ~70 vessels, no carriers, 2 submarines, mostly for regional operations in the gulf. No capable blue water navy

  [globalmilitary.net]
- The United States far surpasses Iran in traditional military power—troops, planes, ships, technology, global reach, and nuclear weapons
- Despite lacking U.S.-level conventional capability, Iran invests heavily in missiles, drones, proxy forces, and cyber operations to offset disadvantages. [geopolitika.it].



Clyde Roark
July 27, 2023

RANSOMWARE







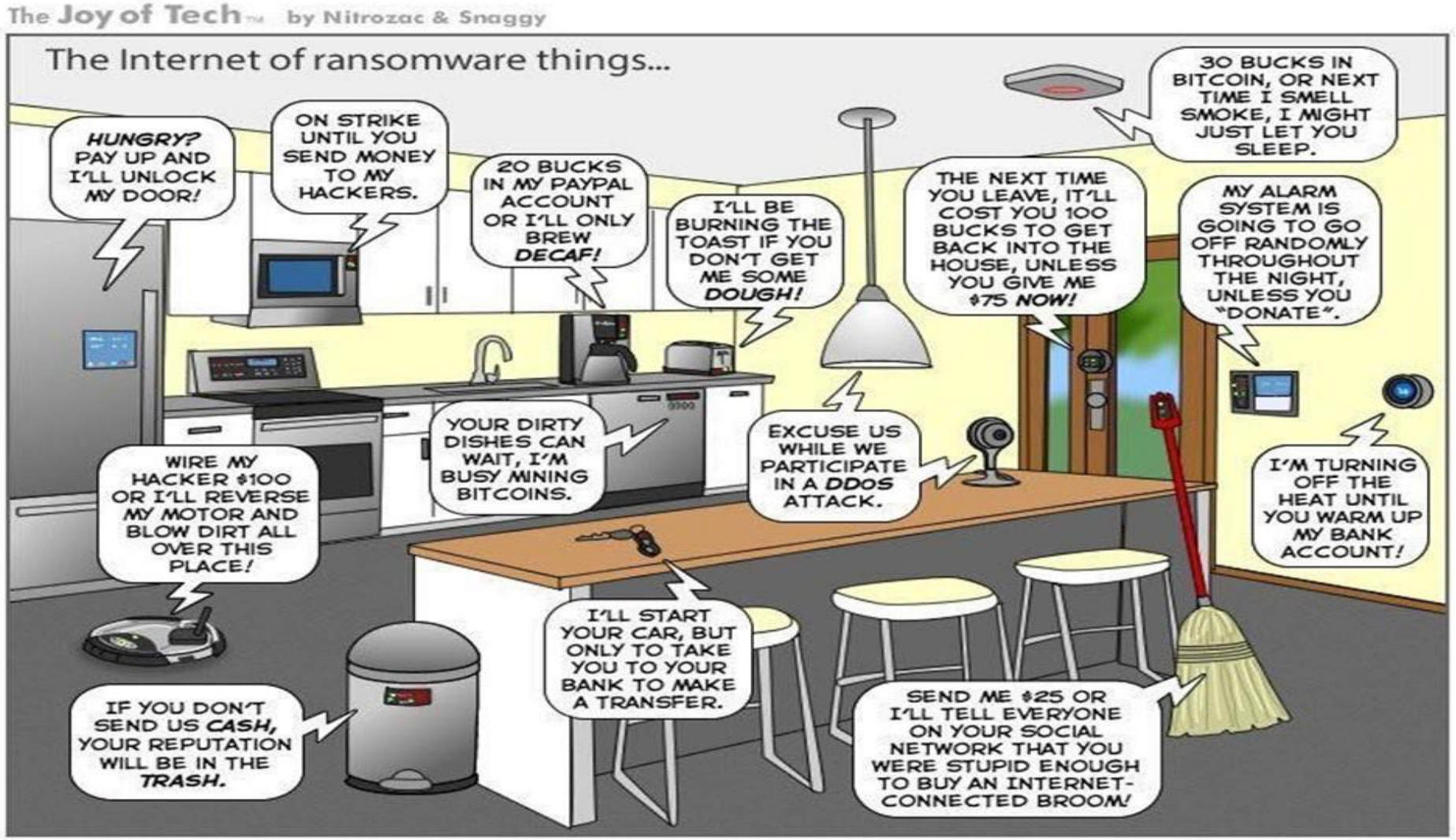
Clyde Roark
July 27, 2023

Ransomware: Medusa Vs Italian Water Supplier Alto Calore Servizi SpA

- The Medusa ransomware group took credit for the attack and said they were giving the water company seven days to pay a ransom. Medusa provided samples of the data it stole and, like with other victims, offered them several options: pay $10,000 to extend the ransom deadline one day or $100,000 to delete all of the data taken.
- The group said it took customer data, contracts, minutes from board meetings, reports, pipe distribution information, expansion documents and more.
- The company manages 58 million cubic meters of water a year.
- They are a Ransomware-as-a-service (RaaS)



Ransomware: Infects…Encrypts…Extorts



IT/OT Convergence



Clyde Roark
July 27, 2023

IT/OT Convergence Explained

- IT includes any use of computers, storage, networking devices and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.
- OT, traditionally associated with manufacturing and industrial environments, includes industrial control systems such as supervisory control and data acquisition.
- The gray area that connects IT and OT is the development and deployment of Internet of Things (IoT) devices. IoT devices include a wide assortment of sensors for gathering real-world conditions, such as temperature, pressure and chemical compositions. IoT devices also include an array of actuators that translate digital commands and instructions into physical actions, such as controlling valves and moving mechanisms. Each IoT device is designed to communicate over standard networks, allowing them to exchange OT data with IT resources -- servers and storage -- sometimes over considerable distances. Makes “dumb” things “smart”.
- IoT devices are historically vulnerable to attacks, which means that the OT attack surface expands when it is integrated with IT. Cybersecurity should therefore be a major concern to the business, as OT is responsible for smooth facility operations.

Hackers Vs Springfield Illinois Water Utility

- Hackers gained remote access into the control system of the city water utility in Springfield, Illinois, and destroyed a pump last week, according to a report released by a state fusion center and obtained by a security expert.
- The hackers were discovered when a water district employee noticed problems in the city's Supervisory Control and Data Acquisition System (SCADA). The system kept turning on and off, resulting in the burnout of a water pump.



Clyde Roark
July 27, 2023



Network Complexity 1

System Maintenance 2

Network Segmentation 3

Data 4

Ransomware 5

OT SYSTEMS

System owners should ensure that OT systems that help water systems control valves and pumps and monitoring are properly protected through patching and proper network mapping. Human machine interfaces, through which operators typically control OT systems, should be a priority for securing.

IT/OT CONVERGENCE

Properly segmenting IT/OT systems, and ensuring that no part of OT systems connect directly to the internet, can greatly reduce the possibility of a successful attack upon Industrial Control Systems (ICS)/SCADA systems that support the supply water function.

IT SYSTEMS

Implementing cyber hygiene and best practices within IT networks can protect water systems from cyber attacks such as ransomware and data theft, and reduce the risk of lateral movement within water systems or networks.

RESOURCES

AVAILABLE RESOURCES INCLUDE: CISA's **Cyber Resource Hub** provides a range of free, immediately available cybersecurity resources. CISA's **Cyber Essentials Toolkit** for non technical leadership. **Securing Networking Devices** provides guidance on Segmenting and Segregating Networks. **Stopransomware.gov** contains best practices for preventing or responding to ransomware. The **Industrial Control Systems Joint Working Group (ICS JWG)** has links to trainings and resources related to the securing and safe operation of ICS systems. CISA also provides no cost **cybersecurity assessments.** The **WaterISAC** produces physical and cyber threat alerts and best practices specifically for the water and wastewater sector. The **AWWA's Security Guidance and Tool** supports the sector in implementing the NIST Cybersecurity Framework and use of Cybersecurity Guidance and Assessment Tool.

Clyde Roark
July 27, 2023

EPA Cybersecurity for the Water Sector

EPA FACT SHEET

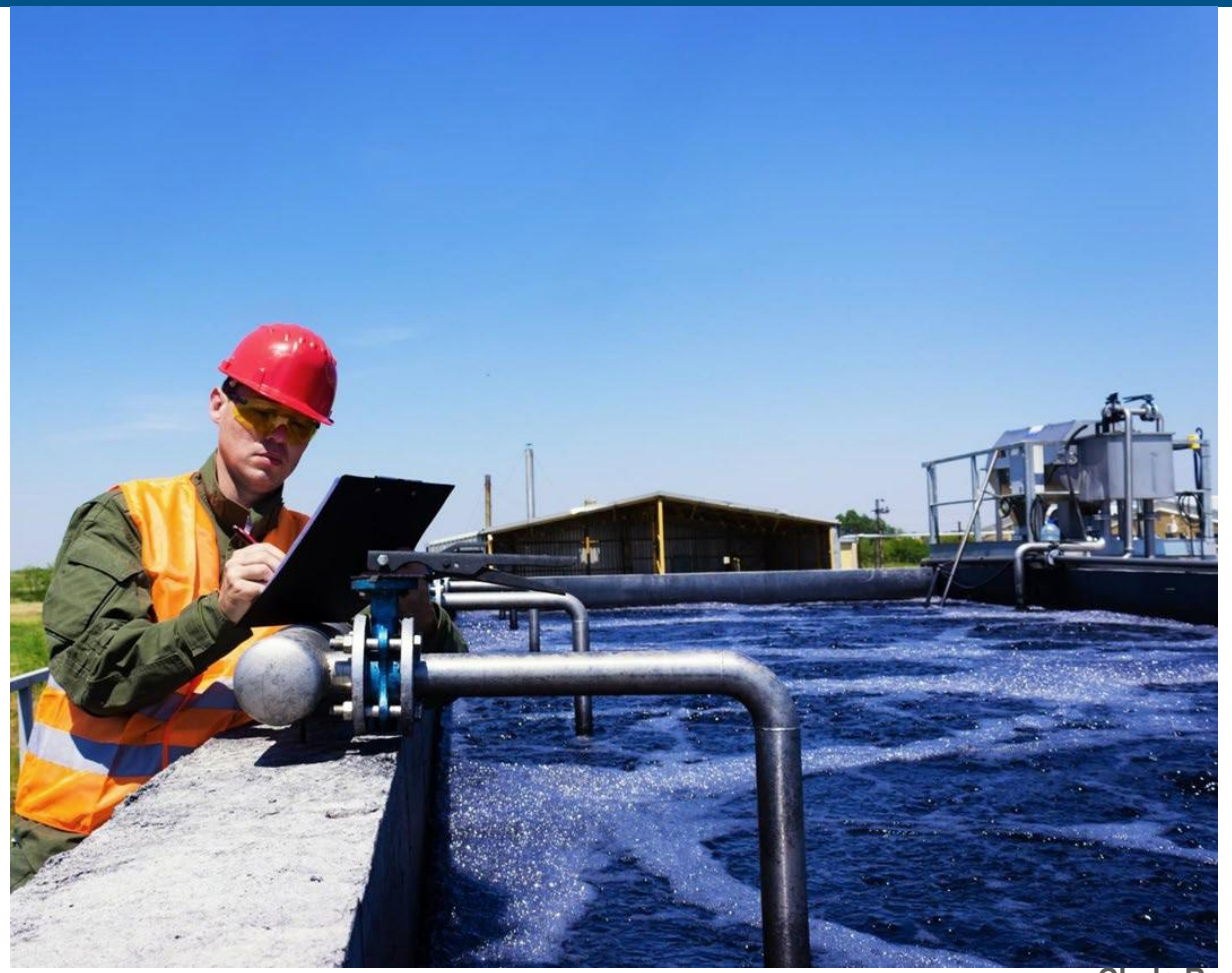
Increasing Cybersecurity Resilience at Public Water Systems

Cyber-attacks against public water utilities are increasing. These attacks have the potential to disable or contaminate the delivery of drinking water to consumers and other essential facilities like hospitals. While some public water systems (PWSs) have taken important steps to improve their cybersecurity, many PWSs have failed to adopt basic cybersecurity best practices and consequently are at risk of a cyber-attack.

Clyde Roark
July 27, 2023

Why is Cybersecurity Important to the Water Sector?

- Cyber attacks could impact public health
- Cyber attacks could cause service disruptions
- Cyber criminals could gain access to protected employee and customer information



Clyde Roark
July 27, 2023

You Vs The World. Establish A Cybersecurity Program



Clyde Roark
July 27, 2023

Never Use Default Passwords

A default password is a standard preconfigured password for a device or software. They are the default configuration for many devices and, if unchanged, present a serious security risk.

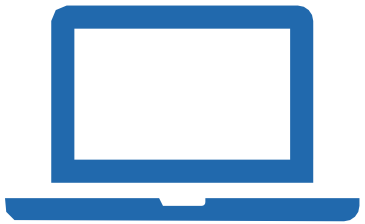
- ALWAYS change default passwords for all IT and OT systems
- In cases where default OT passwords can’t be changed, isolate the equipment and schedule to check logs for sign-ins

Remove PLCs from direct internet access

- Install them behind a secure firewall, gateway, or VPN;
- Never allow remote access without multi-factor authentication
- Enforce Password Length & Complexity- require all employees to create long and complex passwords and contain **one uppercase letter**, **one lowercase letter**, **one number**, **one symbol.**
  EXAMPLES: P@$$w0rD, iL^vE_C@t$, W@ter_$*CuR!ty

Require Separate IT and OT Credentials

Usernames and Passwords, also known as “credentials," should be different for users who access both IT and OT networks.



Username: ITUser2
Password: Pa$$w0rD



Username: OTUser2
Password: Il0v3w@t3r

Clyde Roark
July 27, 2023

Enable Multifactor Authentication (MFA)

MFA (also called "Two-Step Verification") is a security feature that allows the user to present two pieces of evidence to confirm their identity:

- Something you know (password, PIN #, etc.)
- Something you have (smart card, smartphone)
- Something you are (fingerprint, facial recognition)

MFA is more secure because it eliminates the risk of hackers using stolen passwords and users reusing and sharing passwords.

Many IT and OT software platforms come with an option that will allow the IT/OT support staff to enable and configure MFA.

Clyde Roark
July 27, 2023

Check system logs for warning signs

- Look for unusual traffic on common control-system ports (44818, 2222, 102, 502)
- Review for any unexpected changes to controller logic or project files
- Be aware! Notice any unusual operations like loss of connection to out stations, uncommon low pressure pump readings and changes to operator profiles

Strengthen basic cyber hygiene

- Change default passwords,
- Validate PLC logic before switching to “run” mode,
- Ensure IT/OT teams or integrators review systems for exposed devices and apply vendor and CISA hardening guidance.



CISA CYBER SERVICES

Clyde Roark
July 27, 2023

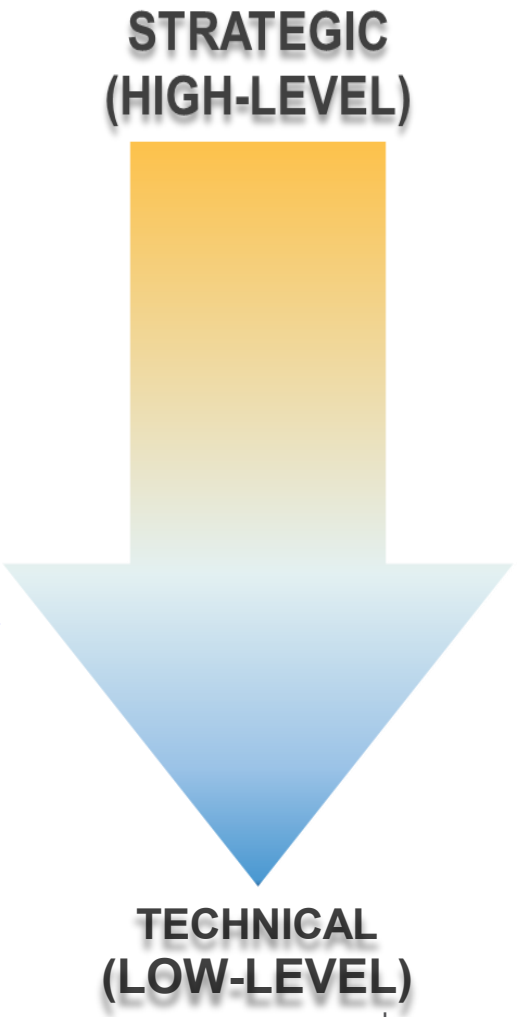
CISA No-Cost Cybersecurity Services

High-level Resources:

- Cybersecurity Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)
- Cyber Tabletop Exercises
- Workshops

Tactical Resources:

- **Cyber Hygiene Services | CISA**
- Ransomware Vulnerability Warning Pilot (RVWP) | CISA
- Known Exploited Vulnerability Catalog| CISA
- Remote Penetration Test (RPT) | CISA
- Risk and Vulnerability Assessments (RVA) |CISA



Questions & Contact Info



Contact Information

Ryan Lewis
Region 4 Cybersecurity State Advisor – KY/TN
Ryan.Lewis@cisa.dhs.gov
(202) 975-9453 (Cell)

Clyde Roark
Region 4 Cybersecurity Advisor – Gulf Coast
Clyde.Roark@cisa.dhs.gov
(850)776-2894 (Cell)