

Navigating the CPS Blind Spot

OT Cyber Threats & Securing Our Critical Infrastructure



Isaac Johnson

Isaac.j@claroty.com

- ✓ State & Local Principal
- ✓ Former Systems Engineer, Manager InfoSec
- ✓ Marketing for Public Sector (SLTT)



Ryan Welch

Ryan.w@claroty.com

- ✓ Claroty Director Department of War
- ✓ Former Air Force Officer & Nuclear Engineer
- ✓ Soccer Coach, Mountain Climber, Backcountry Fisherman



Sean Tufts

Sean.t@claroty.com

- ✓ Field CTO
- ✓ Former GE, Optiv and NFL employee
- ✓ Leads Energy vertical for Claroty

“

*There are risks and costs to action. But they are far less than the long-range risks of **comfortable inaction**.*

~John F. Kennedy



Vital statistics...

Public Sector

Municipalities

- ❑ There are ~**19,500 cities** in the U.S.
- ❑ There are ~**16,000 towns** in the U.S.
- ❑ Approximately ~**3,500- ~4,000 villages** in the U.S.

Counties

- ❑ There are **3,143 counties** in the U.S.

Tribes

- ❑ There are **547 recognized tribes** in the U.S.

Education (K12)

- ❑ There are nearly **99,000 public schools** in the U.S.

Special Districts

- ❑ There are roughly **39,500 special districts** in the U.S.

Public Health (Hospitals & Clinics)

- ❑ There are ~**3,489 local health departments** in the U.S.

Territories

- ❑ There are **11 inhabited territories** in the U.S.

Businesses

- ❑ There are ~**3,200,000 water-reliant businesses** in the U.S.



Water Systems



*Bedrocks of Society: There are **148,000 regulated public water systems** in the U.S. (~49,500 of which are community systems)*

“Does your utility's Emergency Response Plan (ERP) have a specific playbook for a major OT cyber incident?”

- ☐ **Yes, we have a detailed, tested** playbook for OT-specific incidents.
- ☐ **Yes, we have a general** cyber incident plan, but it's not specific to OT.
- ☐ No, our ERP is primarily focused on **physical threats and natural disasters**.
- ☐ We are **currently developing** this section of our ERP.



Global State of CPS Security, 2024:

Public Sector

Business Impact of Disruptions

- ✓ **Counter High-Priority Threats:** Prioritize defense against state-sponsored actors, a top-ranked threat that has actively targeted water systems. Threat intelligence is key to defending these critical assets.
- ✓ **Prioritize Based on Financial Risk:** 45% of organizations suffered financial impacts of \$500,000+ from CPS attacks. A formal risk assessment was the most cited missing capability that could have reduced the impact of these costly incidents.
- ✓ **Justify Spending with Downtime Costs:** Nearly half (49%) of organizations experienced over 12 hours of operational downtime due to cyberattacks. This directly contributes to top financial impacts of concern to state & local government functions, like lost recovery costs (35%).
- ✓ **Secure the Supply Chain Blind Spot:** A staggering 82% of organizations were attacked via third-party access. Address this risk with cross-functional teams, as 63% of respondents lacked a clear understanding of these external connections



Download: Survey Results – The Global State of CPS Security, 2024 ~
<https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions>

The background features a complex, abstract design. It includes a circular radar-like pattern with concentric arcs and radial lines, overlaid with binary code (0s and 1s) in various colors (yellow, orange, red, blue). The overall aesthetic is high-tech and digital.

THE CPS BLINDSPOT

The Riskiest Cyber-Physical Systems
Being Overlooked By Traditional
Vulnerability Management Approaches

WHAT ARE HIGH-RISK DEVICES?

Traditional Methods fail to take into consideration high-risk characteristics we identify, which include but are not limited to:

- ! Weak or default system passwords
- ! Outdated firmware
- ! Communication over insecure protocols
- ! Failing to assess configurations that could allow attackers an initial network foothold
- ! Continued reliance on end-of-life devices that no longer receive feature or security updates

Note:

Our research focused on assets that meet our definition of high-risk devices, are connected directly to the Internet rather than through a secure access solution, and contain a known exploitable vulnerability (KEV). The risk of exploitation of these devices is high, and successful attacks could **significantly impact public safety**.

Nation State and Hacktivist Attacks with Physical Consequences (2010 - 2024)

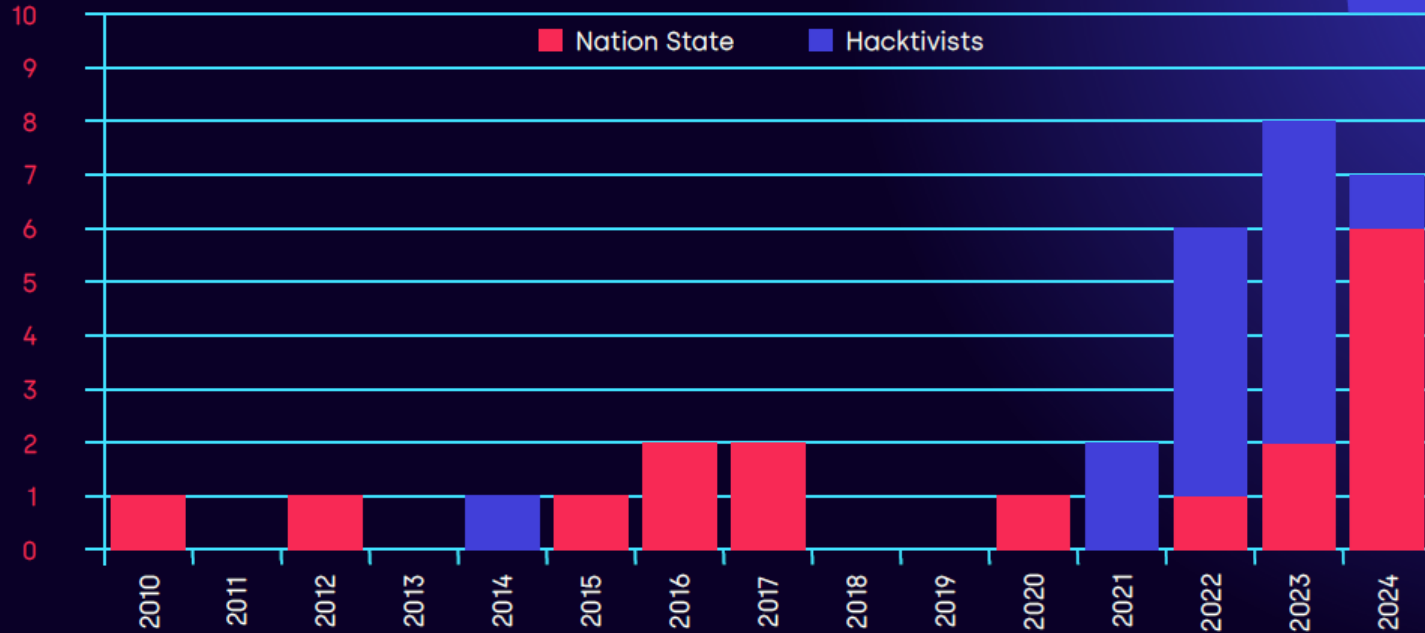


Figure 2: Nation state and hacktivist attacks with physical consequences (2010 – 2024)

“To what extent were OT cybersecurity risks incorporated into your most recent AWIA RRA?”

- ☐ **Fully integrated:** We modeled specific cyber-attack scenarios (e.g., ransomware on SCADA).
- ☐ **Generally addressed:** We identified cybersecurity as a threat but did not model specific OT impacts.
- ☐ **Minimally included:** It was mentioned as a risk but not analyzed in depth.
- ☐ It was a **major challenge** and a known gap in our assessment.
- ☐ **Not applicable** to us



*The greatest long-term threat facing our country, in my view, is represented by the People's Republic of China...which I consider to be the defining threat of our generation. The Chinese government is **pre-positioning on American civilian critical infrastructure**. To lie in wait on those networks, to be in a position to wreak havoc, can inflict real-world harm at a time and place of their choosing.*

~Christopher Wray, FBI Director

Source: CBS News

ICS Capable Malware

2010: Stuxnet

2013: Havex – OPC scanning capabilities

2016: CrashOverride- turned off the power to Kiev for an hour.

2017: Triton – triggered safety shutdowns at two petrochemical sites

2022: Pipedream - ICS hacking tools that was detected before physical consequences

2023: CosmicEnergy – used only as an educational tool for Russian penetration testers

2023: Unitronics PLC – Targeting and exploitation of water & waste-water systems

2024: FrostyGoop – disrupted heating to 600 apartment buildings in Ukraine

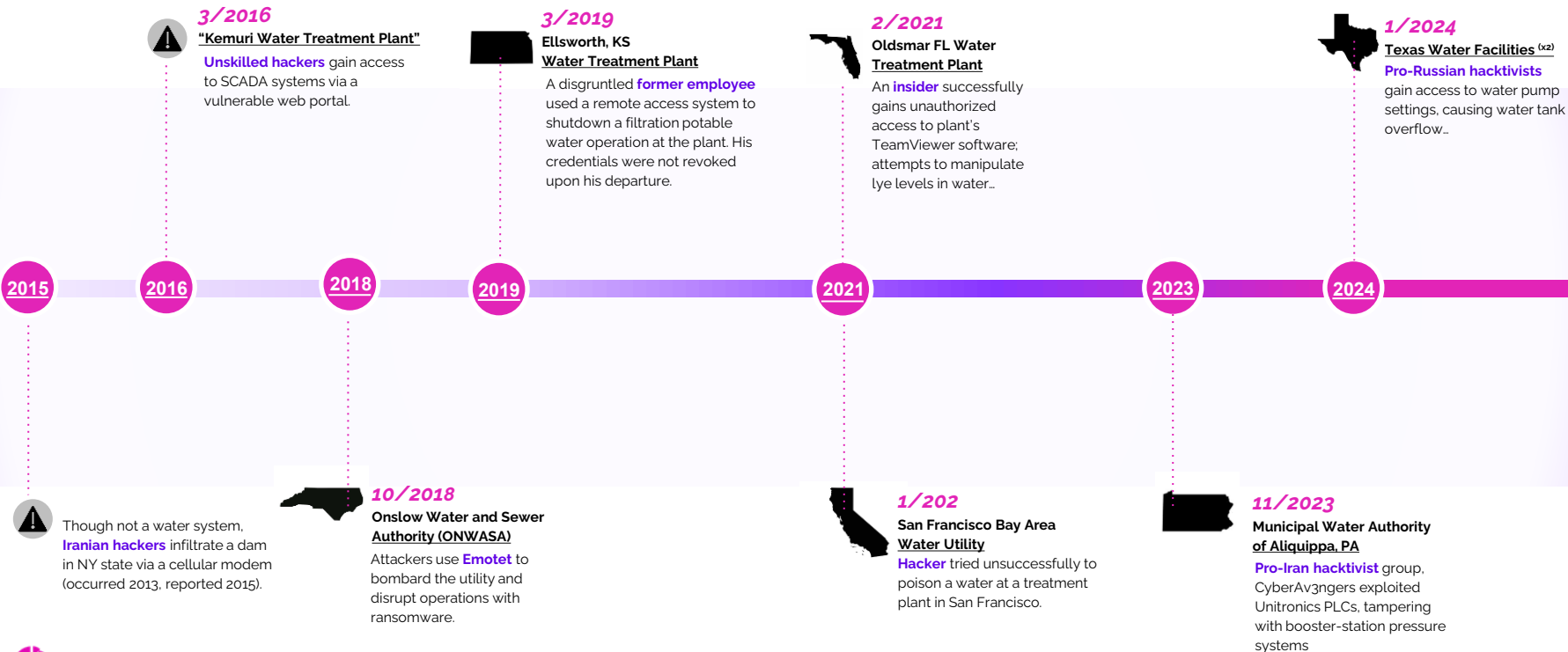
2024: IOControl – disrupted fuel pumps in thousands of Iranian gas stations

2024: Fuxnet – caused a DDOS attack via Meter-Bus (MBus) RS485 communications and bricked over 500 sensor gateways



Timeline of Events & Incidents: 2015 - 2025

Across U.S. Water/Wastewater Systems, Critical Infrastructure



Unitronics PLC

Public Sector

US sanctions Iranian officials over cyber-attacks on water plants

7 February 2024

By Azadeh Moshiri, BBC News

Share

Iranian-Linked Hacks Expose Failure to Safeguard US Water System

- The EPA, lawmakers, water associations can't agree on rules
- Nation's water systems are poorly protected from cyber threats



TECHNOLOGY

Iran-linked cyberattacks threaten equipment used in U.S. water systems and factories

UPDATED DECEMBER 2, 2023 · 1:51 PM ET · 0

Juliana Kim

SECURITY / TECH / POLICY

Cyberattacks are targeting US water systems, warns EPA and White House

The US has imposed sanctions on six officials of the Islamic Revolutionary Guard Corps (IRGC) which it says conducted cyberattacks on American water plants late last year.

/ States are being asked to assess vulnerabilities at water utilities following attacks linked to the Chinese and Iranian governments.



By Jess Weatherhead, a news writer focused on creative industries, computing, and internet culture. Jess started her career at TechRadar, covering news and hardware reviews.

Mar 20, 2024, 5:12 PM GMT+2

3 Comments (3 New)

The Municipal Water Authority of Alliquippa, PA (pictured) was targeted by a cyber attack last year. Image: AP Photo / Gene J. Puskar



This photo provided by the Municipal Water Authority of Alliquippa shows the screen of a Unitronics device that was hacked in Alliquippa, Pa., on Nov. 25. Municipal Water Authority of Alliquippa via AP

Analysis Reveals...

Active Exploits
Persist

Ransomware Still
Reigns

Real Operational
Impacts

940,000+

OT Devices Analyzed

270

Organizations



Food & Beverage



Pharma



Automotive



Oil & Gas



Mining



Chemical



Aviation



Rail



Maritime/Ports



Key Global Findings Overview

Public Sector

12%

of researched organizations have OT assets communicating with malicious domains.



12%
contain KEVs



40%
of the organizations analyzed have these assets insecurely connected to the internet



7%
of the devices are exposed with KEVs that have been linked to known ransomware samples and actors



31%
of the organizations analyzed have these assets insecurely connected to the internet



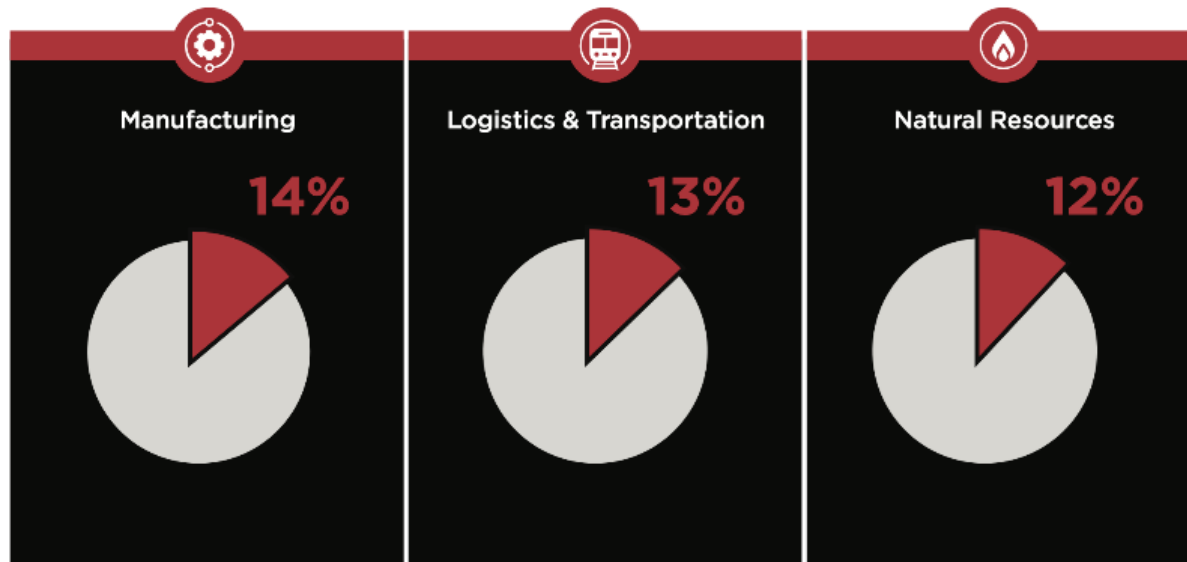
Key Global Finding:

Significant Malicious Traffic

Public Sector

The **potential for damaging attacks** that disrupt services or are destructive to critical infrastructure **is real.**

OT Devices Communicating with Malicious Domains

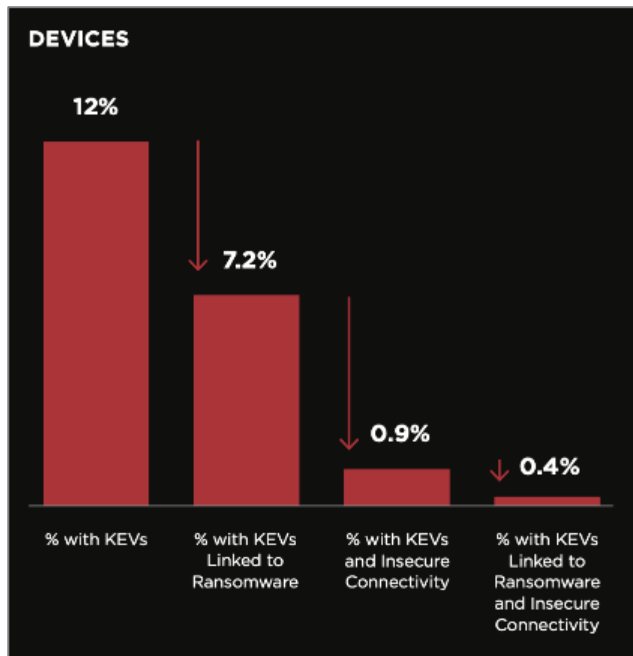




Key Global Finding:

KEVs in Insecure Assets

Public Sector



Prioritize Remediation:

1. KEVs, first
2. With a ransomware link
3. And insecure connectivity

“What was the biggest challenge in completing your AWIA-mandated cybersecurity assessment?”

- ☐ **Lack of visibility** into all OT assets.
- ☐ **Shortage of staff** with OT-specific security expertise.
- ☐ **Budgetary constraints** for tools or external consultants.
- ☐ **Difficulty quantifying** the risk of cyber threats
- ☐ **Not applicable** to us



*The inherent nature of operational technology creates obstacles to securing these mission critical technologies...There is a clear imperative for security and engineering leaders to shift from a traditional vulnerability management program to an exposure management philosophy to ensure they can **make remediation efforts as impactful as possible.***

~Grant Geyer, Chief Strategy Officer



Operationalize Standards & Guidance

For sustained cyber-operational resilience.

Laws & Regulations

- ✓ Executive orders
 - ✓ Laws, regulations
- EX:** SDWA, AWIA 2018



Funding & Capital

- ✓ Continually proving stewardship
 - ✓ Pathways to eligibility
- EX:** "Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program" (app period closed 10/6/2025)



Guidelines & Frameworks

- ✓ How things must be done, maintained
 - ✓ Prioritize low-hanging fruit
- EX:** CISA's "Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators"



Standards & Manuals

- ✓ What must be done
 - ✓ Why it must be done
- EX:** NERC CIP-015



G430-24

J100-21

Your Utility

M5

G440-22

market forces

market forces



Awareness is not just about “clicks”...

It's also about knowing...

Public Sector



What you have...

- Raw asset data
- Unknown risk profile



What matters most...

- Understand context
- Keep critical services list
- Keep critical assets list
- Know your risk profile



What to do about it...

- Develop playbooks
- Follow guidelines
- Foster partnerships (interdepartmental, public-private, etc.)



How to do it...

- Design protections
- Deploy controls
- Develop automation
- Design orchestration
- Conduct regular training
- Optimize



Recommendations

Public Sector



Threat Detection

Prioritize threat remediation **based on KEVs** that are insecurely exposed to the internet and at risk of ransomware.



Exposure Management

Focus on the most consequential impacts to production by remediating risks that are **exploitable today**.



Network Protection

Restrict lateral movement using network segmentation to prevent attackers from reaching isolated network segments that are critical to process integrity, for example.



Secure Access

Remove an attackers opportunity for entry by closing risky exposure points with a **purpose-built CPS access solution**.

CPS Zone Management

Comprehensive Asset Inventory



Thank you