

5TH ANNUAL AFCEA LAS VEGAS CYBER & TECH DAYS AT
NNSS

Protecting the Mission

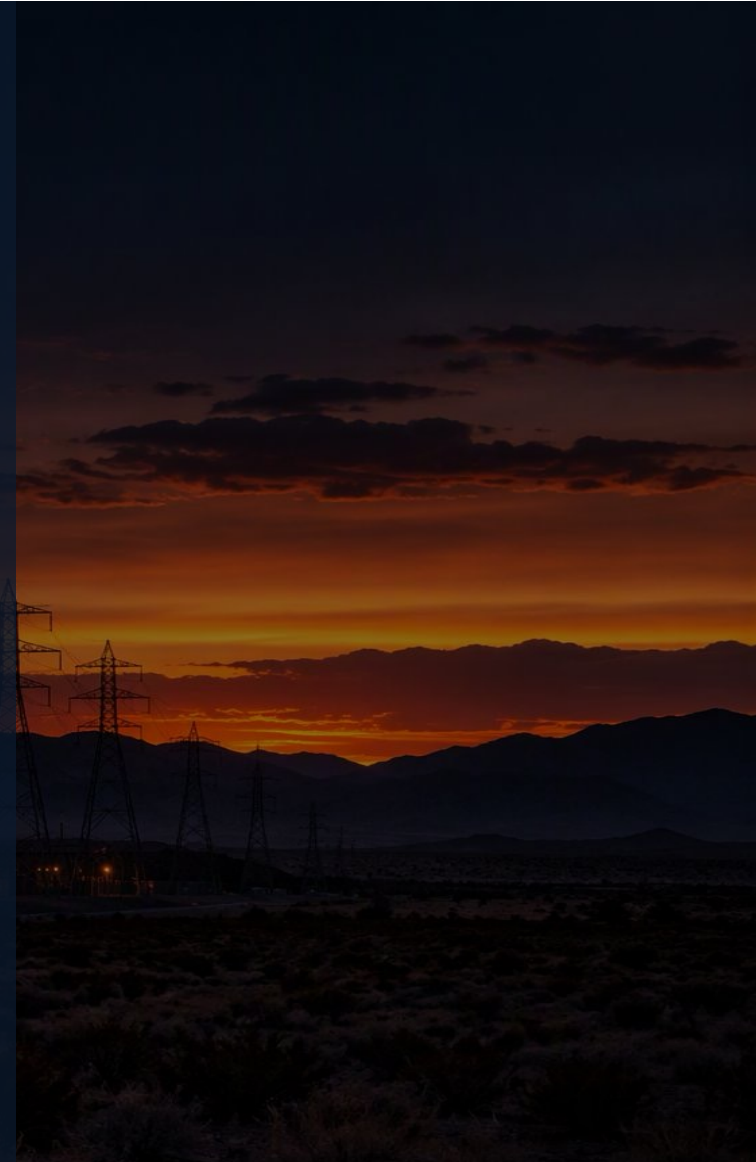
Operational Technology Security for Critical
Infrastructure

Christopher A. Warner, MBA, GCIP

Principal Security Architect | CDW

Adjunct Professor | UNLV | Critical Infrastructure

October 2026 · Nevada National Security Sites



ABOUT THE SPEAKER

Why I Care About This Mission



30+ years

Securing OT/ICS and associated IT across critical infrastructure sectors



8 years USAF

Electronic & Cyber Warfare, Sensors, Nellis AFB, NV
Terminal Threat Specialist – DoD/OGA Contractor



14 years InfraGard

CISO Cross-Sector Council Member



Engineering GRC / ERM

Governance, Risk, Compliance; Enterprise and Integrated Risk Management helping form frameworks for E&U; O&G; Critical Manufacturing, etc.



Education

MBA; MA Organizational Risk Mgmt; GCIP; IEC 62443; NIST SME; Purdue CIMT; USAF Electronic Warfare Fighter Pipeline graduate.



UNLV

Adjunct Professor, Critical Infrastructure Technology

IT VS. OT

OT Is Not IT – The Priorities Flip

	IT	OT
Purpose	Business data & services	Physical process, safety, mission
Lifecycle	3–5 years	20+ years
Protocols	Standard, COTS	Proprietary, legacy
Maintenance	Regular windows	Limited / no downtime
Failure impact	Productivity, data loss	Safety hazard, physical damage

Security priority order

IT	OT
1. Confidentiality	1. Availability
2. Integrity	2. Integrity
3. Availability	3. Confidentiality

*In OT, availability and safety come first.
Downtime is a mission failure.*

INTERDEPENDENCE

OT Runs All 16 CI Sectors



Energy



Water & Wastewater



Nuclear



Chemical



Critical Manufacturing



Defense Industrial Base



Government Facilities



Healthcare & Public Health



Emergency Services



Communications



Information Technology



Financial Services



Transportation



Dams



Food & Agriculture



Commercial Facilities

Lose one, the others feel it.

The grid needs water. Water needs power. Every sector needs communications.

Over 75% of U.S. critical infrastructure is privately owned and operated.

THE COMMON DENOMINATOR

One Playbook, Many Industries



PLCs & RTUs



HMIs & SCADA



Engineering workstations



Cellular-connected field devices



Vendor remote-access tools



If a technique works on an exposed PLC at a water plant, it works anywhere that controller is exposed. The industry changes. The malware doesn't.

THREAT LANDSCAPE

Threats Have Moved to Physics

1,693

ransomware attacks on industrial orgs in
2024

Dragos

+87%

year-over-year increase

Dragos

12+

states with reported activity in the recent
U.S. water-sector campaign

Public reporting



Most successful OT attacks exploit preventable weaknesses, not zero-days.

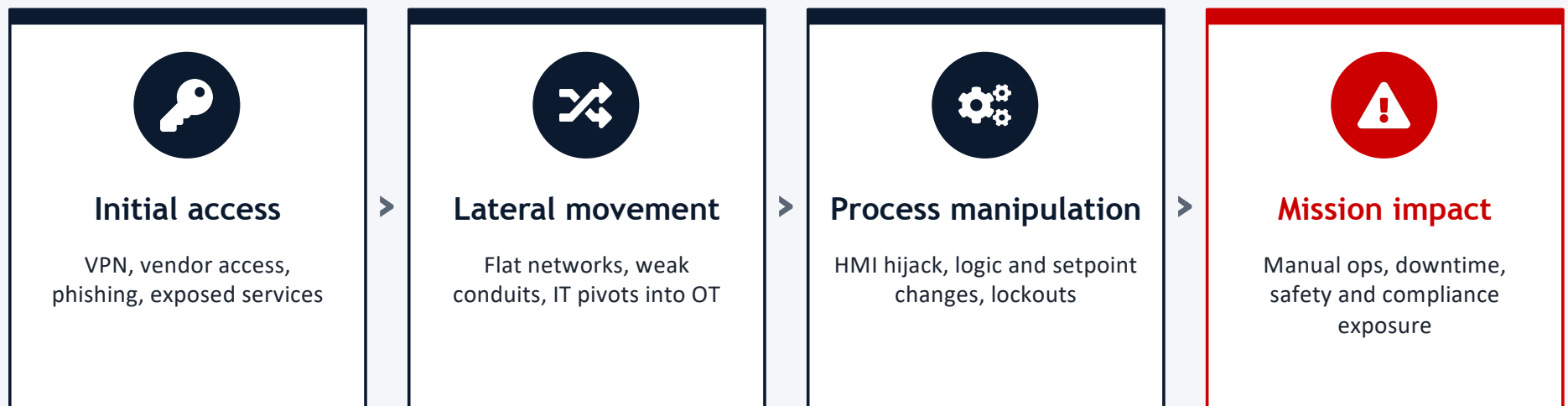
Who Is Targeting OT

Actor	Group	Targets	OT risk
China	Volt Typhoon / VOLTZITE	Comms, energy, transportation, water	Pre-positioning for disruption
Russia	Sandworm / ELECTRUM	Power grid, substations, SCADA	Operational disruption
Iran	IRGC-linked / CyberAv3ngers	Internet-exposed PLCs; water, energy	Loss of control, public impact
North Korea	Lazarus / Andariel	Defense industrial base, energy, manufacturing	IT-to-OT compromise path

Nation-state OT campaigns rarely start at the PLC. They start with remote access, exposed edge devices, weak identity, vendor pathways, and flat IT/OT conduits.

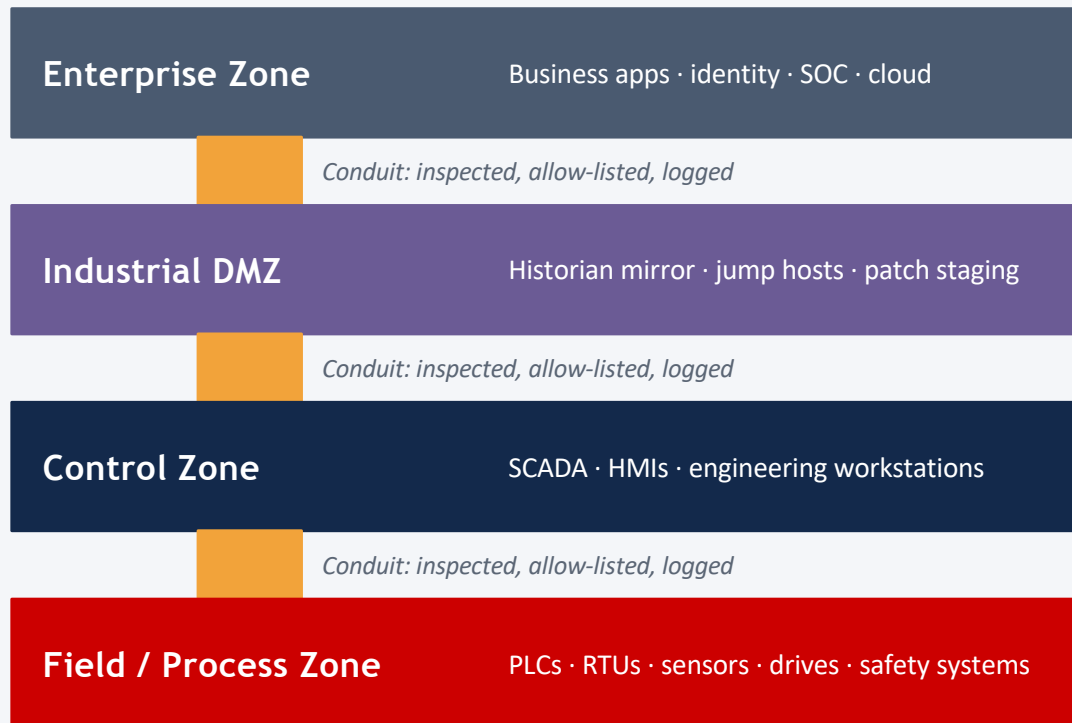
ATTACK PATH

When a Cyber Event Becomes Physical



Case in point, Kemuri Water (2016): attackers entered through a payment web server, reached a 1988-era SCADA platform bridging IT and OT, and manipulated valves and chemical flow.

Zones & Conduits (IEC 62443)



1

Define zones

Group assets by function and criticality

2

Secure conduits

Only required flows cross a boundary

3

Broker access

No direct path from IT or the internet to controllers

4

Monitor

Passive, protocol-aware visibility on every conduit

Read the Process Before You Control It

Start with replicated historian and read-only SCADA data. No write path. No control authority.

1 OBSERVE

Historian replica / one-way feed

Anomaly detection • Predictive maintenance • Alarm and event correlation

2 UNDERSTAND

Operational context matters

Custom logic and workarounds • Aging assets and changed processes • Rare states the model has never seen

3 GOVERN

AI advises. Deterministic controls decide.

Human-in-the-loop • Physics-based limits and interlocks • Independent safety protections

FOR NOW: READ-ONLY AI. CONTROL REMAINS ENGINEERED, VALIDATED AND HUMAN-AUTHORIZED.

AUTONOMOUS VEHICLES

Yes, this is converged IT + OT + AI:

Sensors, compute, communications and actuators make decisions in the physical world.

TRUE ICS RAISES THE STAKES

A model can learn abnormal operation as “normal.”

Bespoke processes, undocumented changes and complex physics can defeat pattern recognition. In a power plant, refinery or water system, a wrong action can cascade beyond one machine.



THE CONTROL-SIDE REALITY

You Don't Secure a PLC by Changing Its Password

- Keep controllers in RUN, not REMOTE or PROGRAM
- Monitor key position; alarm on mode change
- Alarm on unexpected logic downloads or checksum changes
- Remove controllers and workstations from internet and cellular exposure
- Broker all vendor and engineering access
- Keep validated, restore-tested backups of logic and configs

A physical key switch is a control neither IT nor an attacker can override remotely.

PRIORITY CONTROLS

Five Controls That Matter Most



Asset Discovery & Monitoring

You can't protect what you can't see.
Inventory, map vulnerabilities, watch traffic.



Segmentation

Zones and conduits stop lateral movement from IT into OT.



Threat & Vulnerability Mgmt

Risk-based. Mitigate where you can't patch.



Incident Response

OT-specific plans, backups, and recovery.
Often the fastest win.



Secure Access

MFA, identity-based, time-bound, recorded vendor sessions.

RESILIENCE

Operating in a Degraded State

Assume the path exists

Plan as if similar attack paths already exist in your environment.

Rehearse manual ops

Operators must be able to run the process safely without the HMI.

Restore with confidence

Offline, validated backups of PLC logic, configs, and golden images.

Exercise together

OT tabletop exercises with operations, engineering, IT, and leadership.



You can't patch physics, but you can build resilience.

WHERE TO START

Roadmap to Stronger OT Security

01

Baseline program maturity

02

Choose the right framework

03

Enumerate assets & metadata

04

Map value streams & functions

05

Build a unified risk view

06

Design risk-based controls

07

Implement control sets

08

Test, train, monitor, improve

Frameworks: NIST CSF 2.0 · NIST SP 800-82 · ISA/IEC 62443 · NERC CIP · CISA CPGs

ONE MISSION, ONE TEAM

Cyber Risk Is Now Operational Risk

Assume

the attack paths already exist

Win

with fundamentals, not more tools

Unite

IT, OT, engineering, operations, and leadership

Fifth-generation warfare isn't fought only in the kinetic space. It's fought against the systems that run daily life. That makes this everyone's fight.

Thank you • Questions

Christopher A. Warner | CDW OT/ICS Security | christopher.warner@cdw.com | [Christopher Warner MBA](#) | [LinkedIn](#)