

USCM Mayors Water Council
Meeting

Cybersecurity for Water Infrastructure

**Norman Anderson, PE,
CISSP GICSP**



What are Your Concerns?

Top Concerns

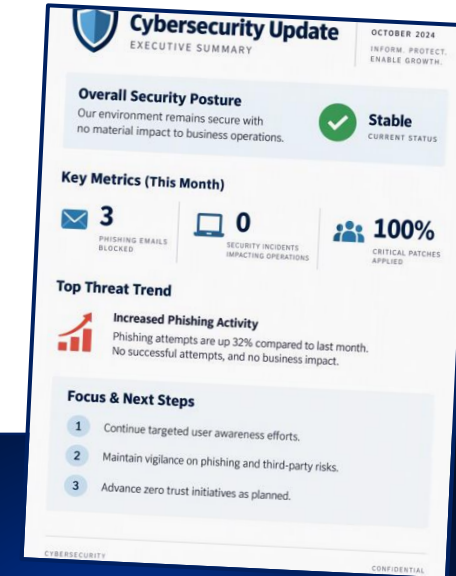
- 1 Unsafe water or wastewater discharge.
- 2 Loss of public trust.
- 3 Loss of service or operational control.
- 4 Ransomware or financial loss.
- 5 Regulatory or legal exposure.



Engagement

How can you stay informed?

Do you know what your utilities are doing about cybersecurity? Being informed allows for decision making and holds staff accountable.



Why water systems are a target?

Essential and highly visible

Water and wastewater are essential public-health services. Targets have high visibility and media coverage.

Geopolitical targets

Nation-state actors target these systems as part of international conflicts.

Operational exposure

Internet-exposed operational technology can allow remote tampering. Impacts can include loss of visibility, control, pressure or continuity.

Critical safeguards

Manual operations and tested recovery remain critical safeguards.



What is the problem?



People Problem?

People can cause cybersecurity issues when they:

- Are not properly trained.
- Do not understand their role in cybersecurity.
- Make mistakes (e.g., clicking on phishing emails).
- Do not follow policies and procedures.

AWARENESS TURNS RISK INTO RESILIENCE.



Technology Problem?

Technology can be an issue when it is not:

- Properly configured.
- Used as intended.
- Regularly updated and maintained.
- Integrated effectively with other security tools.
- Aligned to meet business needs.

THE RIGHT TECHNOLOGY ONLY WORKS
WHEN APPLIED CORRECTLY.



Governance Problem?

The real problem is governance because it:

- Defines accountability and responsibility for people.
- Ensures the proper application and configuration of technology.
- Establishes policies, standards, and oversight to manage risk.
- Aligns people and technology to achieve a defined set of outcomes.
- Addresses known risks and adapts to changing threats.

STRONG GOVERNANCE CONNECTS PEOPLE,
TECHNOLOGY, AND RISK TO DELIVER RESULTS.



It's a Governance Problem.

People and technology matter, but **governance** ensures their effective use to meet defined outcomes and address known risks.

CLEAR ROLES.
RIGHT TOOLS.
REAL SECURITY.

Cybersecurity is a utility program

Manage it like safety, O&M, meter programs, compliance, and capital planning

Govern

Ownership, policy,
risk acceptance,
reporting,
documentation

Know

Asset management,
dependencies,
vulnerabilities,
critical functions

Protect

Access control,
segmentation,
backups, secure
configuration

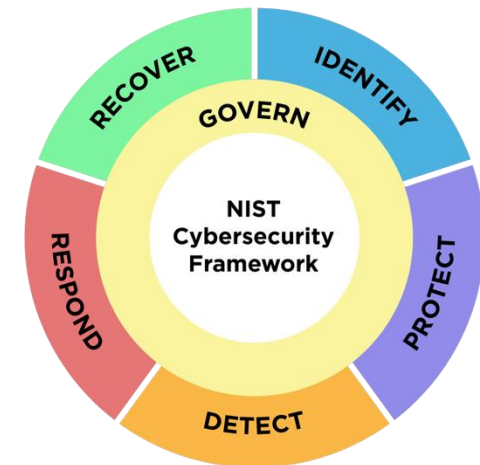
Respond

Roles,
communications,
manual operations,
incident actions

Recover

Restore priorities,
tested backups,
lessons learned

Align with cybersecurity frameworks such as NIST Cybersecurity Framework (CSF) 2.0



IT and OT responsibilities must be documented. Governance connects and sustains them.

IT and OT Cybersecurity protect different outcomes

One enterprise program, two distinct operating environments

Information technology (IT)

Primary focus: information and business services

Examples: email, finance, billing, records, cloud services

Security priorities: confidentiality, integrity, availability

Typical response: isolate, patch, rebuild, restore

Operational technology (OT)

Primary focus: safe, reliable physical operations

Examples: SCADA, PLCs, HMIs, radios, pumps, valves, chemical feed

Security priorities: safety, availability, process integrity

Typical response: preserve control, coordinate with operators, use manual procedures

Shared governance

Common risk framework and executive accountability

Clearly assigned IT and OT control ownership

Coordinated identity, remote access, monitoring, incident response, recovery, procurement, and reporting

Changes tested against operational consequences

Governance turns activity into accountability



Leadership and responsibility

Executive sponsor with authority and budget visibility.
Define internal, vendor and third-party responsibilities.

Governance committee

Define responsibility. Include utility management, OT, IT, operations, engineering, legal, finance, and emergency management or law enforcement.

Policies and planning

Develop policies, procedures and an overall cybersecurity plan.

Reporting and review

Report status quarterly and review the program annually.
Use quantifiable metrics and track implementation progress.

Asset management is the foundation

You cannot prioritize what you cannot see

Inventory

Hardware, software,
firmware,
communications, owners

Criticality

Single points of failure,
necessary for operation,
required for compliance

Lifecycle

Support status,
replacement plans,
conditional assessment,
outdated or unsupported,
configuration baselines

Change

Authorized changes,
backups, testing,
documentation



VISIBILITY
IS KEY TO
CYBERSECURITY



**PENETRATION
TESTING**
IDENTIFIES
WEAKNESSES



**NETWORK
MONITORING**
DETECTS THREATS
IN REAL TIME



**PROPER
ASSET
MANAGEMENT**
KEEPS YOUR
ORGANIZATION STRONG

Start with critical functions and external connections, then improve completeness over time.

Documentation leads to repeatable results

BUILD THE POLICIES TOGETHER

Separated but integrated OT/IT policies and solutions.



TRAIN STAFF

Train staff on the policies and procedures for consistent results. Documentation aids in change management.



TURN FEEDBACK INTO THE STANDARD

Implement lessons learned and issues into policies and project plans for immediate results.

Federal Programs



No-Cost Cyber Vulnerability Scanning for Water Utilities



EPA Water Resilience Cybersecurity Help Desk



EPA No-Cost Cybersecurity Assessment Service



H.R.2594 - To establish a Water Risk and Resilience Organization to develop risk and resilience requirements for the water sector.
119th Congress (2025-2026) | [Get alerts](#)

BILL Hide Overview ✕

Sponsor: [Rep. Crawford, Eric A. "Rick" \[R-AR-1\]](#) (Introduced 04/02/2025)

Committees: House - Transportation and Infrastructure; Energy and Commerce

More on This Bill
[Constitutional Authority Statements](#)
[CBO Cost Estimates \[0\]](#)

State Programs and Legislation



[Services](#) [Policy](#) [Project Delivery](#) [Training](#) [Security](#)

Cal-Secure 2.0

California's Cybersecurity Roadmap



OFFICIAL SITE OF THE STATE OF NEW JERSEY

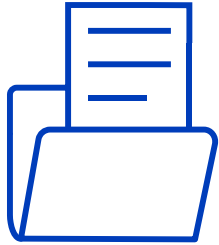


NEW JERSEY

CYBERSECURITY & COMMUNICATIONS
INTEGRATION CELL



Success depends on these key elements.



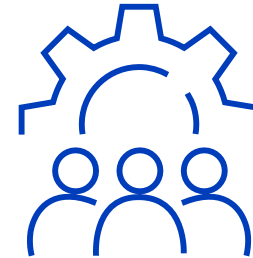
Document

Implementation plan, policies, and procedures for repeatable results and actionable guidance.



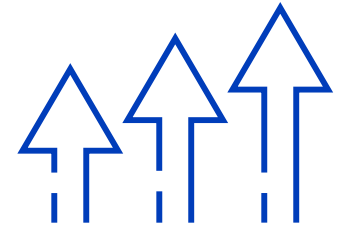
Govern

Program and plan empowered by executive leadership to drive progress.



Inform

Manage assets, people, and technology to track progress and make informed decisions.



Improve

Review of lessons learned applied to future project implementation.

Program success is measured by whether all levels of an organization are informed and engaged.



Norman Anderson, PE, CISSP, GICSP
nanderson@carollo.com