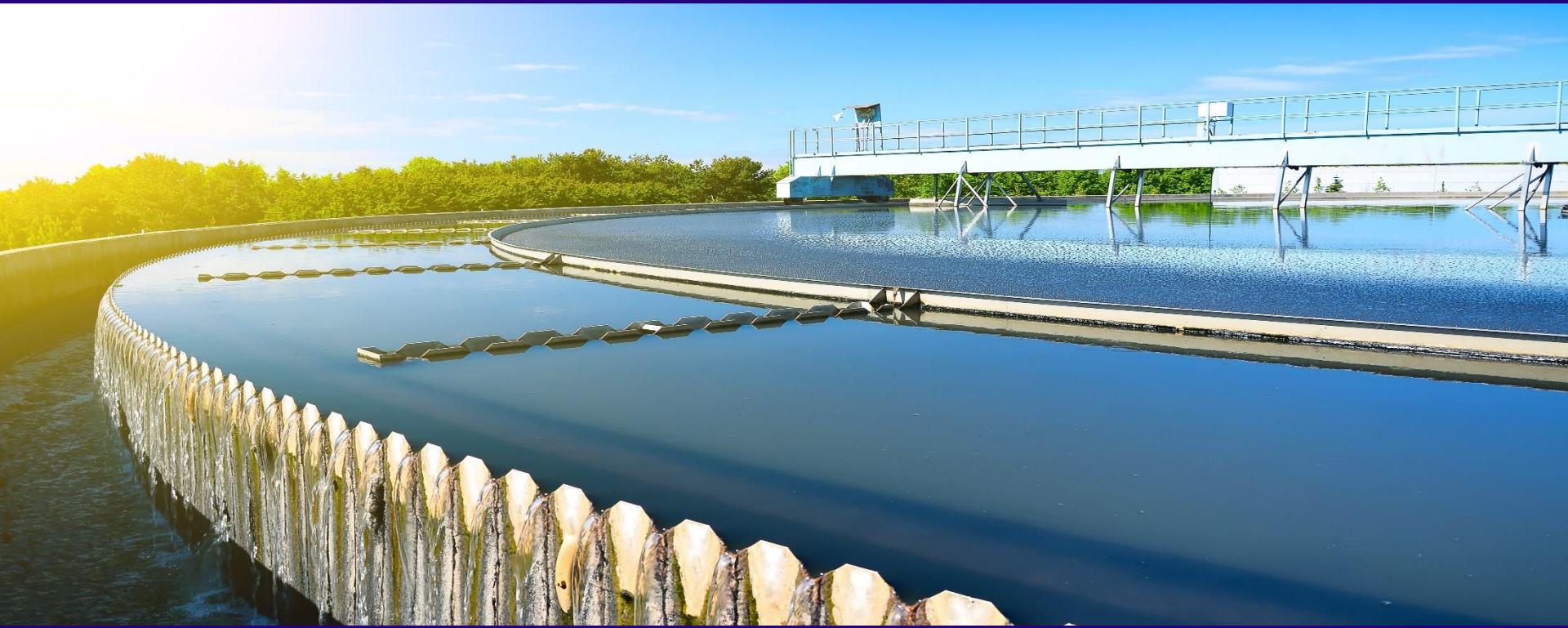
A Practical Approach to Cybersecurity



Presented By: Anthony Ciavardelli & Martin Auman
Keystone Engineering Group, Inc.

Who Is Keystone Engineering Group, Inc.?

- Introduction of Keystone Team Members
- A Brief Review of Keystone
  - Professional Engineering Firm
  - Systems Integrator
  - 70+ Employees
  - 5 Offices
    - Frazer, PA
    - Clarks Summit, PA
    - Hamilton, NJ
    - Lewes, DE
    - Seaford, DE
  - Water/Wastewater

AGENDA

Operation Technology (OT) Cyber Attacks

Preventing Cyber Attacks

Cybersecurity Tools & Resources

OT Cyber Attacks

Iranian Nuclear Facility - Stuxnet (2010)

Colonial Pipeline (2021)

California Bay Area WTP (2021)

Aliquippa Water Authority (2023)

Preventing Cyber Attacks

- Disable Removable Media Access
- Multi-Factor Authentication
- Disable Stale Accounts
- DO NOT reuse passwords
- Implement Jump Host
- Change Default Passwords

Preventing Cyber Attacks Cont'd

- Principle of Least Privilege
- Network Segmentation
- Conduct Cybersecurity Assessments
- Limit Exposure to Internet
- End User Awareness Training
- Trust but Verify!

Cybersecurity Tools & Resources

System Backups

Cybersecurity Assessments & Resources

Vulnerability Scans

System Backups

- This is the Recovery Portion of Security Plan
- Why Back up?
- What to Back Up?
  - Software and Code
    - PLC, HMI, Reporting, Remote Notification
  - Produced Data
    - Automated Reports, SCADA Trended Data
  - Or: Full System Backup
    - Backs up entire Operating System.

CISA – Region 3

Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia

AT-A-GLANCE

Regional Office: Philadelphia, Pa.

Area: 5 States & District of Columbia; 244 Counties; 7 Tribal Nations

Size: 127,324 square miles

Estimated Population: 30,724,788

Key Facts:

- Region 3 includes Pa., Del., Md, W.Va., Va., and D.C.
- Region 3 is home to multiple major metropolitan areas.
- One of the most densely populated regions per square mile.

This region contains varied infrastructure, hosts a plethora of special events, and includes coastal areas.

CISA – Cybersecurity Assessment

ASSESSMENTS

CSAs offer three types of assessments: Cyber Infrastructure Survey, Cyber Resilience Review, and External Dependency Management, to provide a strategic, all-encompassing assessment of an organization's cyber posture.

PSAs conduct Assist Visits to provide critical infrastructure facilities with an overview of available DHS services and/or provide a facility walk-through. PSAs may conduct more detailed security assessments, upon request.

PSAs conduct assessments using the **Infrastructure Survey Tool (IST)** or **Rapid Survey Tool (RST)**. Both tools help PSAs examine the most critical aspects of a facility's security and resilience posture, and an IST will compare a facility against the national average for similar facilities. as well as a facility-specific report.

PSAs administer the **Regional Resiliency Assessment Program (RRAP)**, a voluntary cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. RRAPs address a range of infrastructure resilience issues that could have significant consequences.

Contact Region 3

Contact Regional Staff via Email

CISARegion3@hq.dhs.gov

To report anomalous cyber activity and/or cyber incidents 24/7, email report@cisa.gov, or call (888) 282-0870.

EPA – Cybersecurity Resources

EPA FACT SHEET

EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems

Improving cybersecurity across the water sector remains one of EPA's highest priorities. EPA continues to underscore that adopting cybersecurity best practices at drinking water and wastewater utilities is essential to protect communities from the increasing number and severity of cyber-threats facing our nation's water systems. The Agency will continue to explore opportunities to lower cybersecurity risk for public water systems.

EPA will continue to support states, technical assistance providers, drinking water and wastewater systems by providing ongoing technical assistance in the form of cybersecurity assessments, subject-matter expert consultations, training, and funding.

EPA Fact Sheet – Cybersecurity Resources

Training
Planning
Assessments
Technical Assistance
Funding Opportunities

https://www.epa.gov/system/files/documents/2023-10/epa-cybersecurity-fact-sheet_508.pdf

Additional Resources

Water Information Sharing and Analysis Center (WaterISAC)

waterisac.org

American Water Works Association (AWWA)

awwa.org/cybersecurity

Vulnerability Scanners

CISA Vulnerability Scan Example

2023-07-23

CYBER HYGIENE

REPORT CARD

0
Hosts with unsupported software

1
Potentially Risky Open Services

33%
Increase in Vulnerable Hosts

CISA
CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

July 1, 2023 — July 23, 2023
Host Scans on All Addresses

July 21, 2023 — July 23, 2023
Vulnerability Scans on All Hosts

ADDRESSES OWNED

6
No Change

ADDRESSES SCANNED

6
No Change
100% of addresses scanned

HOSTS

4
Increase of 1

SERVICES

14
Increase of 7

VULNERABLE HOSTS

4
Increase of 1
100% of hosts vulnerable

VULNERABILITIES

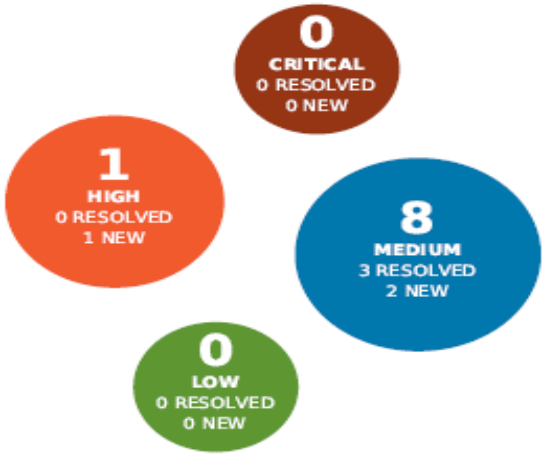
9
No Change

American Water Works Association

Keystone ENGINEERING GROUP

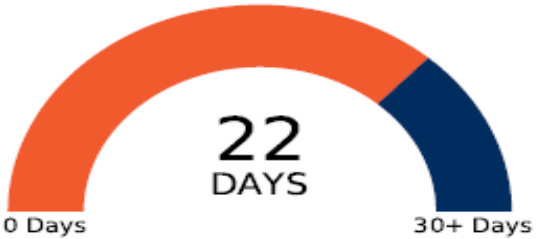
VULNERABILITIES

SEVERITY BY PROMINENCE



VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 0	FTP 0
Telnet 0	RPC 1
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

None Open | Open, No New | Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

Detections

New Potentially Risky Services Detected

Cyber Hygiene scans of your host(s) conducted in the past day have detected new potentially risky services.

These services warrant your attention. All services are potentially at risk of attack, but some can be more risky when open to the public (e.g. RDP, Telnet, etc.), especially if they are open as Networked Management Interfaces. CISA recommends validating that each service below is intended to be available to the public and, where applicable, the service is up-to-date on the latest version, correctly configured, and uses strong authentication. A red asterisk (*) denotes the possibility of a networked management interface.

Host	Port	Service	Category	Initial Detection (UTC)
[redacted]	445	microsoft-ds	SMB*	2024-03-06 00:43

New Potentially Risky Services Detected

Cyber Hygiene scans of your host(s) conducted in the past day have detected new potentially risky services.

These services warrant your attention. All services are potentially at risk of attack, but some can be more risky when open to the public (e.g. RDP, Telnet, etc.) CISA recommends validating that each service below is intended to be available to the public and, where applicable, the service is up-to-date on the latest version, correctly configured, and uses strong authentication.

Host	Port	Service	Category	Initial Detection (UTC)
[redacted]	49669	msrpc	RPC	2023-07-01 11:03
	6183	msrpc	RPC	2023-07-01 11:03

CISA's Cyber Hygiene Vulnerability Scanning

1. Register for this service by emailing vulnerability@cisa.dhs.gov

2. After CISA receives the required paperwork, scanning will start within 72 hours, and organizations will begin receiving reports within two weeks.

3. Once initiated, this service is mostly automated and requires little direct interaction.

4. CISA performs the vulnerability scans and delivers a weekly report.

Final Thoughts

Recovery from a cyber-attack is costly and time consuming, but recovery is possible (and less painful) if you have taken preventative steps.

Critical Infrastructure Owners, Operators, and Cyber Defenders must be equipped with the technologies and tools required to dramatically raise adversary time, costs, and technical barriers.

Thank You!