



Reduce Your Risk for Preventable Cyber Attacks

NEWWA/NEWEA IT & Asset Management Fair


November 2, 2021

About WaterISAC

- Non-profit established by the water sector
- 3,000 members across several hundred utilities and other organizations
- WaterISAC provides members:
 - Physical and cyber security threat information
 - Resilience and mitigation resources
 - Pandemic resources
 - Education and training through webinars
 - Reports on physical and cyber incidents
 - Twice-weekly newsletter
- **Free 2-month Trial Membership:** waterisac.org/membership

Active Threat Environment

JOINT CYBERSECURITY ADVISORY

Co-Authored by:  **TLP: WHITE** Product ID: AA21-287A
October 14, 2021

Ongoing Cyber Threats to U.S. Water and Wastewater Systems

SUMMARY

Note: This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the [ATT&CK for Enterprise](#).

This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of [U.S. Water and Wastewater Systems \(WWS\) Sector facilities](#). This activity—which includes attempts to compromise system integrity via unauthorized access—threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities. **Note:** although cyber threats across [critical infrastructure sectors](#) are increasing, this advisory does not intend to indicate greater targeting of the WWS Sector versus others.

To secure WWS facilities—including Department of Defense (DoD) water treatment facilities in the United States and abroad—against the TTPs listed below, CISA, FBI, EPA, and NSA strongly urge organizations to implement the measures described in the Recommended Mitigations section of this advisory.

Immediate Actions WWS Facilities Can Take Now to Protect Against Malicious Cyber Activity


- Do not click on [suspicious links](#).
- If you use [RDP](#), secure and monitor it.
- [Update](#) your OS and software.
- Use [strong passwords](#).
- Use [multi-factor authentication](#).

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at [www.fbi.gov/contact-us/field-offices](#), or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at [CyWatch@fbi.gov](#). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at [CISAServiceDesk@cisa.dhs.gov](#).

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see [http://www.us-cert.gov/ftp/](#).

TLP: WHITE

TLP: AMBER



Quarterly Water Incident Summary


Incidents and Suspicious Activities

Q1-21

January – March 2021
Published June 15, 2021

TLP: AMBER

TLP: AMBER



Quarterly Water Sector Incident Summary


Incidents and Suspicious Activities

Q2-21

April – June 2021
Published October 14, 2021

TLP: AMBER

TLP: AMBER



Quarterly Water Incident Summary

Incidents and Suspicious Activities

Q4-20

October – December 2020
Published March 29, 2021

TLP: AMBER

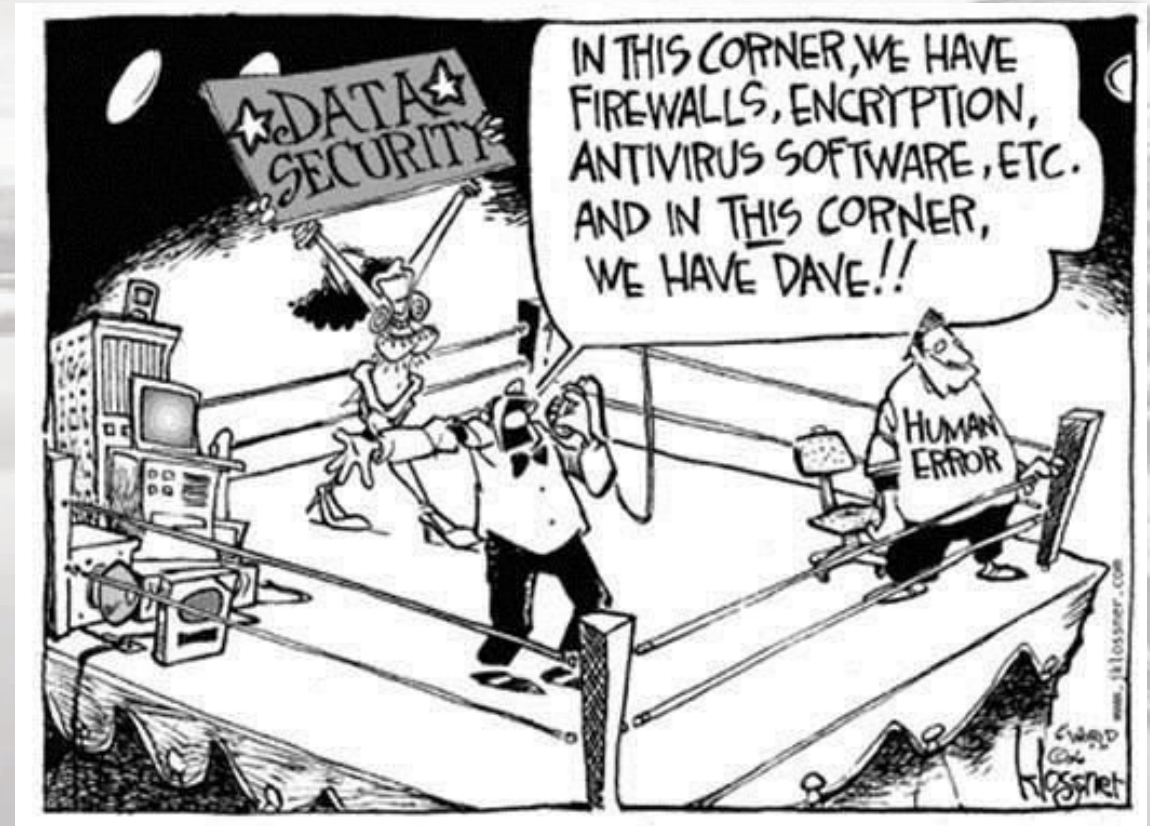
<https://us-cert.cisa.gov/ncas/alerts/aa21-287a>

Tactics, Techniques, and Procedures

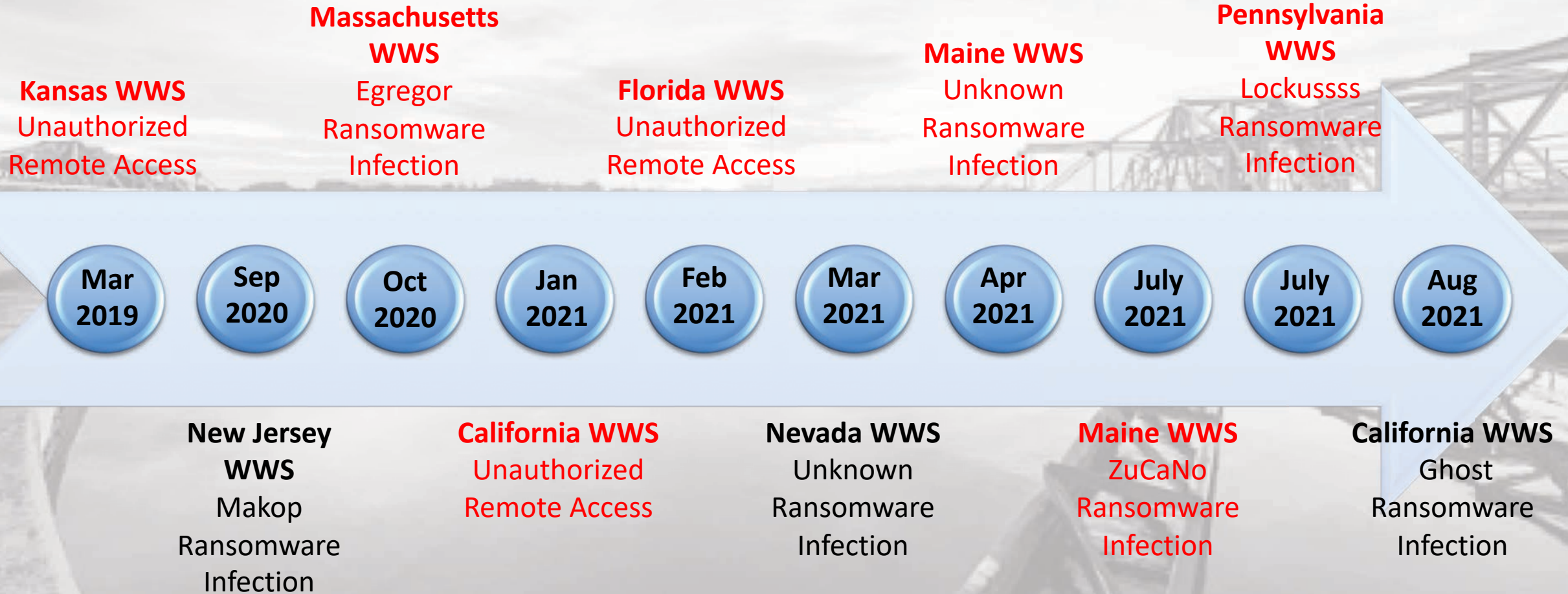
- Phishing and spear phishing
- Exploitation of unsupported or outdated operating systems and software
- Exploitation of control system devices with vulnerable firmware versions
- Exploitation of unsecured remote access

Vulnerabilities

- Insider Threats
- COVID-19 Environment
- Unpatched Vulnerabilities
- Supply Chain



Timeline



Attack Vectors and Other

Vulnerabilities

	Phishing	Unsupported / Outdated OS and Software	Unsecured Remote Access	Malicious Insider
<u>March 2019</u> KS – Unauthorized Remote Access			X	X
<u>October 2020</u> MA - Egregor Ransomware Infection	X			
<u>January and February 2021</u> CA and FL – Unauthorized Remote Access		X	X	X
<u>April and July 2021</u> ME – Ransomware Infections		X	X	
<u>July 2021</u> PA – Lockussss Ransomware Infection			X	

Phishing

- Three Modes

- Attachments
- Links
- Credential harvesting

- Common targets

- Customer Service
- Human Resources
- IT Administrators
- Finance
- Legal
- Executives
- Everyone!

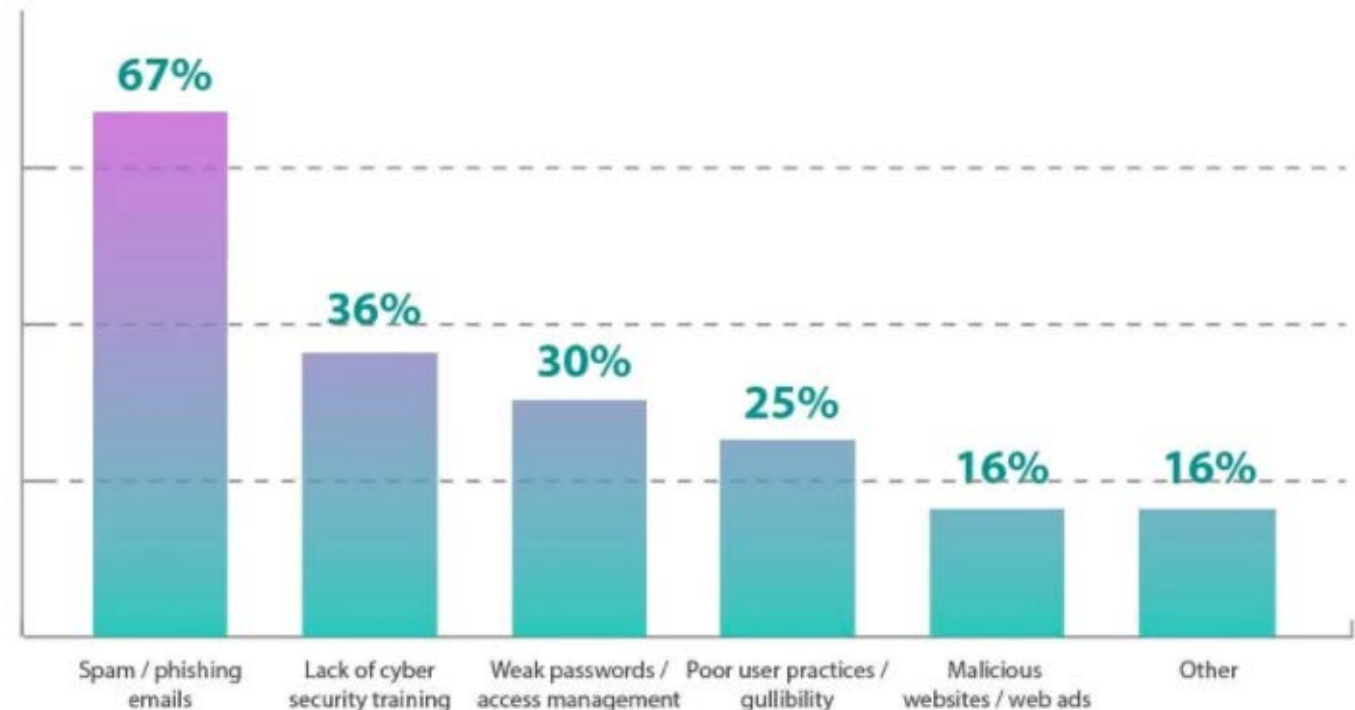


Ransomware

- National Council of ISACs
 - Fall 2020 Report
 - Sep 2021 Statement
- Evolution
 - Double extortion
 - Automation?

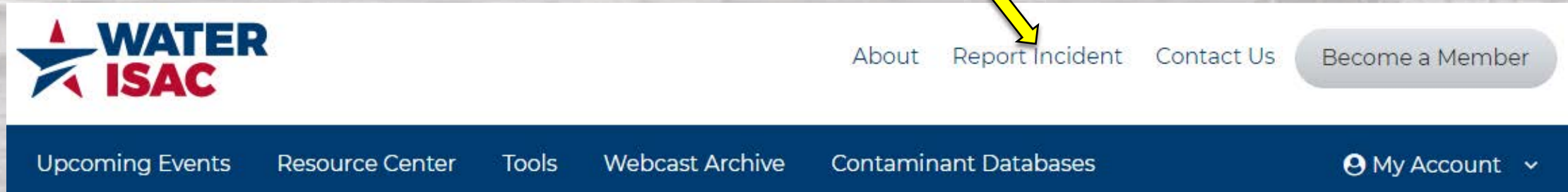
MOST COMMON METHODS OF RANSOMWARE INFECTIONS IN NORTH AMERICA

Based on MSPs reporting attacks on organizations. (Some were targeted by more than one method.)



Reporting

- Online Incident Reporting Form:
 - <https://www.waterisac.org/report-incident>



- Email: analyst@waterisac.org
- Phone: (866)H2O-ISAC
- Q3 2021 Incident Survey: Deadline Nov 5

Mitigations

■ Recommended Immediate Actions

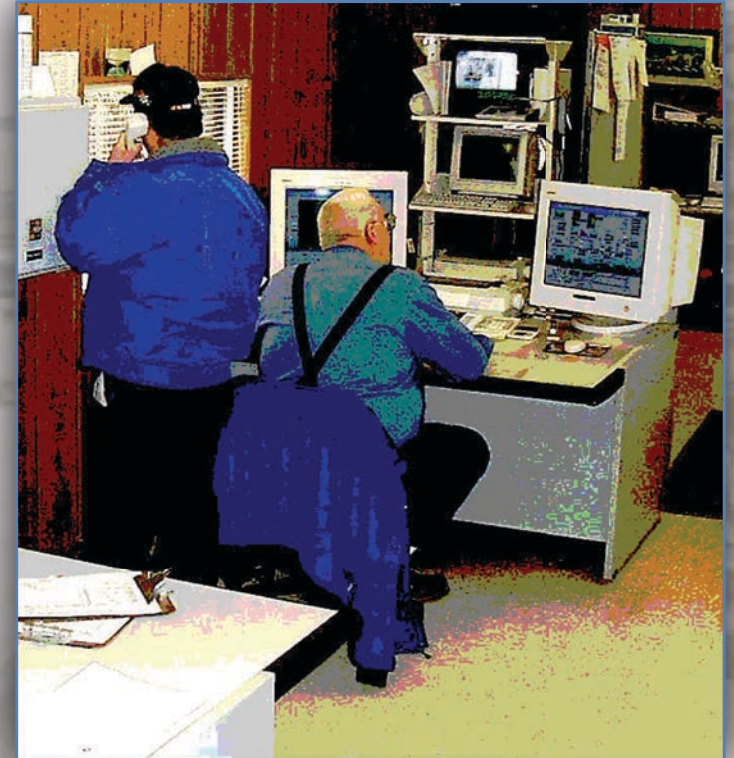
- Do not click on suspicious links.
- If you use remote access, secure and monitor it.
- Update your operating system and software.
- Use strong passwords (long).
- **Use multi-factor authentication.**



A.H-S

Monitoring and Reporting By SCADA Operators

- Problems with SCADA system access.
- Unfamiliar data windows or alerts.
- Abnormal operating parameters.
- Unauthorized SCADA system access.
- Unusual access times for a given individual.
- Unexplained SCADA system restarts.
- Unchanging parameter values that normally fluctuate.



A.H-S

Remote Access

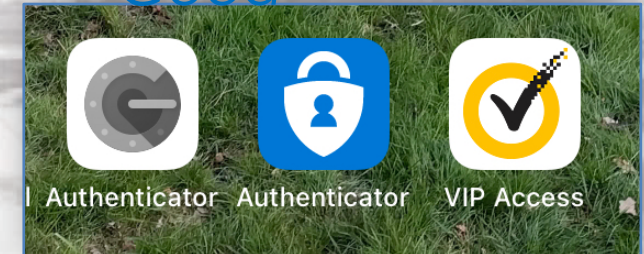
- Require **multi-factor authentication (MFA)**.
- Only for users with a verified need.
- Log and audit remote access.
- Manually start and stop access.
- Shut down retired access accounts.
- Configure to provide the least access required (read only).

MFA Options

Sun, Jul 11, 1:40 PM

G-791754 is your Google verification code.

SMS Code -
Good



Authenticator App -
Better



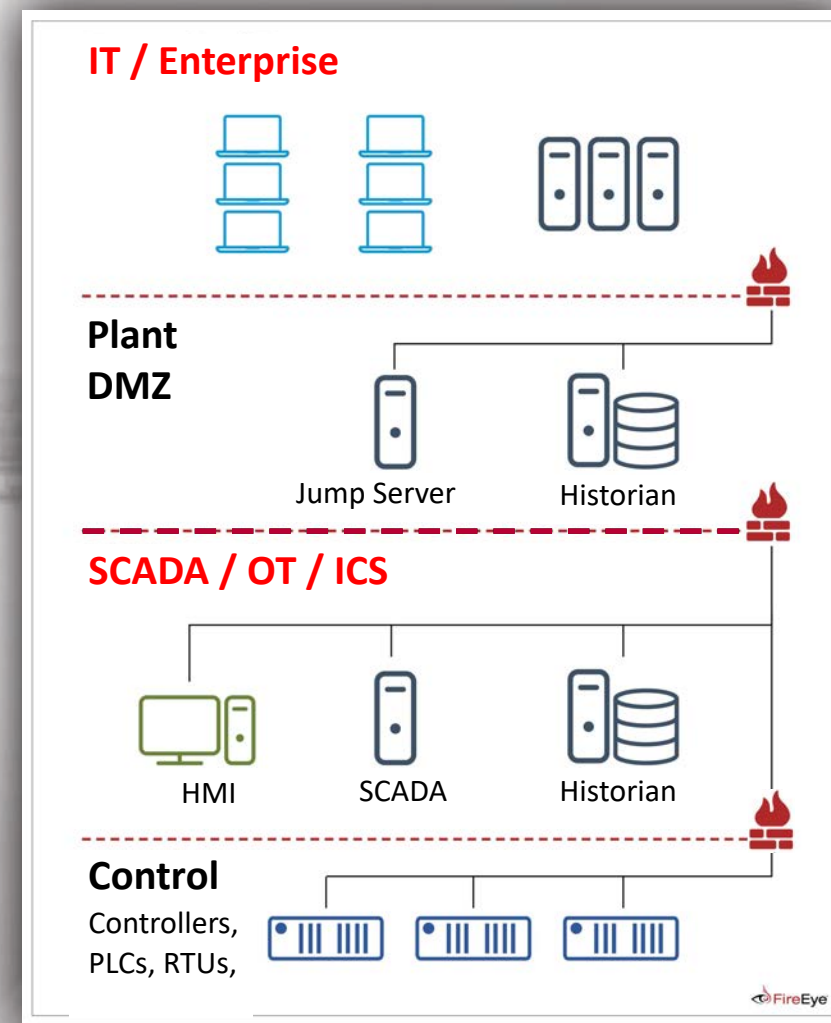
A.H-S

Physical Key -
Best

Network

- **Separate** the SCADA system from the utility's enterprise IT system.
- Map the full network, identify assets and remove anything no longer needed.

Separation



based on ICS Reference Architecture
Zafra, et.al., ICS Tactical Security Trends, FireEye

Planning and Operational

- Have emergency response plans for cyber attacks that modify or disable SCADA system displays and that modify or prevent system control.
- Include fail-over plans for alternate control systems and **manual operations**.
- Practice the plan annually with tabletop exercises and field exercises.

Manual Operations



Hand/Off/Auto switch
SCADAware.com

Safety System

- Install independent **cyber-physical safety systems** to prevent physical damage by a successful cyber adversary.

WaterISAC project – Looking for a utility that we can work with on identifying additional cyber-physical safety systems.

Examples



A.H-S

Pressure Switch



Schlumberger

Valve Operator
Gears

Additional Measures

- Foster a culture of cybersecurity readiness.
- **Update** software, firmware and OS.
- Regular antivirus/antimalware scans.
- User account management.

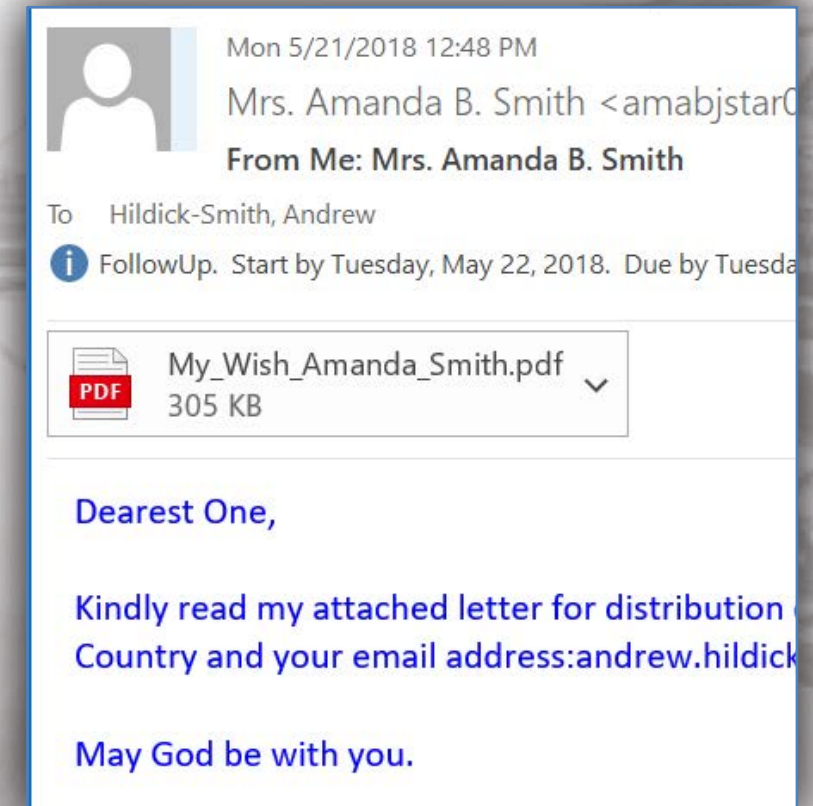


CISA PLC Firmware Update Advisory

Additional Measures, continued

Phishing Awareness

- If possible use SCADA device authentication, encrypted SCADA protocols and encrypted wireless communications.
- Regular data backups and testing.
- Application execution controls.
- Train users on **phishing and social engineering awareness**.



A.H-S

Cybersecurity Incident Reporting

- MA DEP – 888-304-1133
- WaterISAC – 866-426-4722, for threat sharing
<https://www.waterisac.org/report-incident>
- FBI Boston – 857-386-2000, ransomware or financial incident,
- Other organizations:
 - Commonwealth Fusion Center – 978-451-3700
 - MS-ISAC – 866-787-4722
 - CISA – 888-282-0870

Resources

- DHS Cyber Hygiene service
- WaterISAC membership
- MA ITS78 State Contract for cybersecurity services
- MS-ISAC membership
- InfraGard membership



Johns Island, South Carolina, A.H-S

Resources, continued

- WaterISAC, "15 Cybersecurity Fundamentals for Water and Wastewater Utilities"
- AWWA, Cybersecurity Guidance and Assessment Tool
- EPA, Cybersecurity Incident Action Checklist
- DHS CISA, StopRansomware.gov web site
- DHS CISA, Virtual Learning Platform (Idaho National Lab SCADA/ICS classes)



Questions and Contact Information

www.waterisac.org
1-866-H2O-ISAC

Chuck Egli
Director of Preparedness and
Response
egli@waterisac.org

Andrew Hildick-Smith
Advisor
hildick-smith@waterisac.org