WATER ISAC

Water Information Sharing and Analysis Center

Water Sector Monthly Cyber Threat Web Briefing
December 15, 2021

Housekeeping

- This webinar is being recorded.
- The recording and slide deck will be available by tomorrow at waterisac.org/webcasts.
- There will be a Q&A session.

Presenter

- Jennifer Lyn Walker, WaterISAC

15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Download the guide – **https://www.waterisac.org/fundamentals**

1. Perform Asset Inventories
2. Assess Risks
3. Minimize Control System Exposure
4. User Access Control
5. Physical Access
6. Cyber-Physical Safety
7. Vulnerability Management
8. **Cybersecurity Culture**
9. Governance
10. Threat Detection
11. Business Continuity
12. **Insider Threats**
13. Supply Chain Risk
14. **Smart Device Management**
15. Information Sharing

8. Create a Cybersecurity Culture

*Create a culture of cybersecurity from the boardroom to the break room**

Why it's important: *It's easier to "hack" a person than a computer*

- Leadership engagement is pivotal
- Basic cybersecurity "hygiene" is a soft-skill

Resources

ICS Cybersecurity for the C-Level (CISA)

Creating Environments for Successful Awareness Programs: Security Awareness for Executives (SANS Institute)

Notable Results from WSCC Survey on Training

- **No awareness program (42%)**
- Annually (36%)
- Monthly (15%)
- *Daily or weekly (11 respondents)*
- Participation in tabletop exercises, mock drills, tech failures, or emergency management exercises (~25%)

Be a good neighbor! Help protect all of critical infrastructure.

12. Tackle Insider Threats

Employ strategies to deter and detect insider threats

Why it’s important: ***Insider Threat is a people (not a technology) problem***

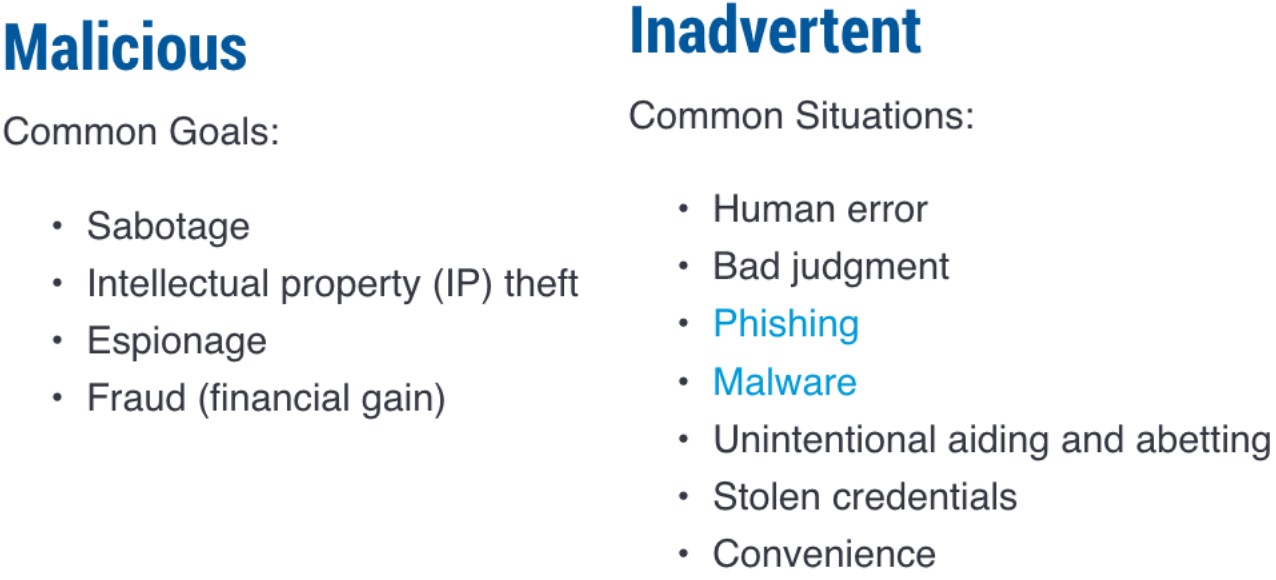
- Recruitment through separation/termination
- Cybersecurity culture helps

Resources

Common Sense Guide to Mitigating Insider Threats, Sixth Edition (CERT Insider Threat Center)

Insider Risk Mitigation Self-Assessment Tool (CISA | CERT Insider Threat Center)

Types of Insider Threats



Malicious

Common Goals:

- Sabotage
- Intellectual property (IP) theft
- Espionage
- Fraud (financial gain)

Inadvertent

Common Situations:

- Human error
- Bad judgment
- Phishing
- Malware
- Unintentional aiding and abetting
- Stolen credentials
- Convenience

14. Address All Smart Devices

Address all connected devices (mobile, IoT, IIoT)

Why it's important: ***Smart devices often create holes that may not have previously existed***

- Asset and vulnerability management
- Supply chain concerns
- Network segmentation

Resources

IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog (NIST SP 800-213A)

Requiring SBOMs and their Impact on OT (Dale Peterson)

Get your Stuff Off Search – S.O.S. (CISA)

Holiday Special Notice

CISA strongly urges organizations to take the following immediate actions to strengthen defenses.

- **Increase organizational vigilance**
- **Prepare your organization for rapid response**
- **Ensure your network defenders implement cybersecurity best practices**
- **Stay informed about current cybersecurity threats and malicious techniques.**
- **Lower the threshold for threat and information sharing**

Don’t let your guard down

Resources

- https://dale-peterson.com/2021/04/27/requiring-sboms-and-their-impact-on-ot/
- https://www.cisa.gov/publication/stuff-off-search
- https://www.proofpoint.com/us/blog/insider-threat-management/4-security-missteps-make-employees-and-companies-vulnerable-insider
- https://www.proofpoint.com/us/threat-reference/insider-threat
- https://www.cisa.gov/sites/default/files/publications/IRMPE_Assessment_v1_2021-08-25.pdf
- https://csrc.nist.gov/publications/detail/sp/800-213a/final
- https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf

Cybersecurity Updates

Threats and Vulnerabilities | Reports | Tips and Resources | Analyst Spotlight

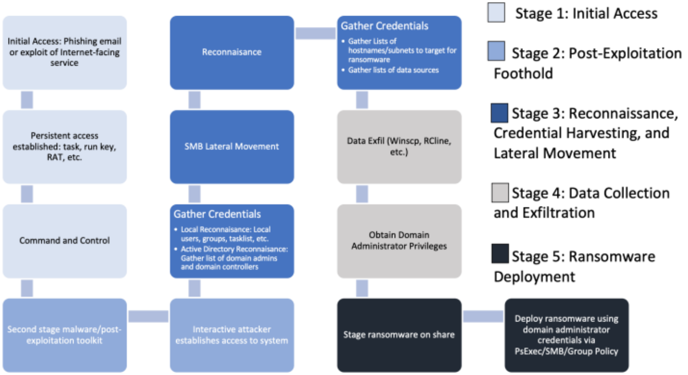
Threats and Vulnerabilities

- Log4j Vulnerability (Read more)

- Emotet Campaign Continues (Read more)
- APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus (Read more)
- FBI FLASH: Indicators of Compromise Associated with Cuba Ransomware (Read more)

Reports

- Cybercrime Services and Supply Chain Fueling Cyber Attacks (Read more)
- Unpacking a Ransomware Attack (Read more)



Initial Access: Phishing email or exploit of Internet-facing service

Persistent access established: task, run key, RAT, etc.

Command and Control

Second stage malware/post-exploitation toolkit

Interactive attacker establishes access to system

Gather Credentials
- Local Reconnaisance: Local users, groups, tasklist, etc.
- Active Directory Reconnaisance: Gather list of domain admins and domain controllers

SMB Lateral Movement

Reconnaisance

Gather Credentials
- Gather Lists of hostnames/subnets to target for ransomware
- Gather lists of data sources

Data Exfil (Winscp, RCline, etc.)

Obtain Domain Administrator Privileges

Stage ransomware on share

Deploy ransomware using domain administrator credentials via PsExec/SMB/Group Policy

□ Stage 1: Initial Access

▨ Stage 2: Post-Exploitation Foothold

■ Stage 3: Reconnaissance, Credential Harvesting, and Lateral Movement

□ Stage 4: Data Collection and Exfiltration

■ Stage 5: Ransomware Deployment

- Conti Ransomware Report (Read more)

Tips and Resources

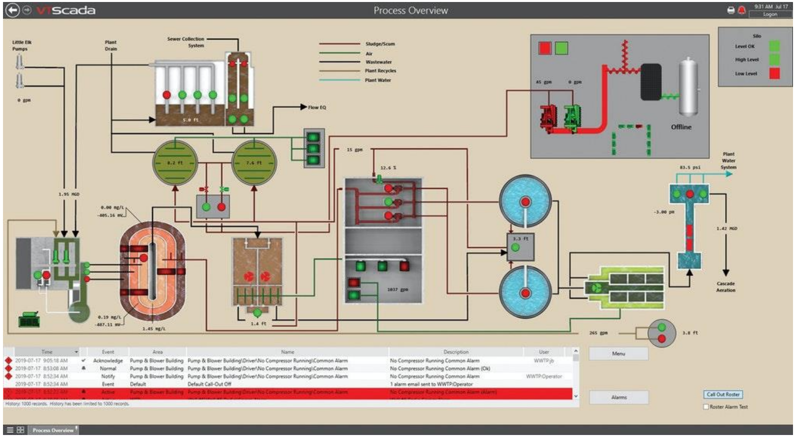
- Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends (Read more)
- New Decryption Key for STOP Ransomware Released (Read more)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

- CISA Releases Guidance on Protecting Organization-Run Social Media Accounts (Read more)

Analyst Spotlight

- Critical Infrastructure Resilience – Control Systems Upgrade Done Right Involves Cybersecurity (Read more)
- OT/ICS Security and Resilience – Humans, Basics, and Use Cases (Read more)



	Time		Event	Area	Name	Description	User
◆	2019-07-17 9:05:18 AM	✓	Acknowledge	Pump & Blower Building	Pump & Blower Building\Driver\No Compressor Running\Common Alarm	No Compressor Running Common Alarm	WWTP:jb
◆	2019-07-17 8:53:08 AM		Normal	Pump & Blower Building	Pump & Blower Building\Driver\No Compressor Running\Common Alarm	No Compressor Running Common Alarm (Ok)	
◆	2019-07-17 8:52:34 AM		Notify	Pump & Blower Building	Pump & Blower Building\Driver\No Compressor Running\Common Alarm	No Compressor Running Common Alarm	WWTP:Operator
	2019-07-17 8:52:34 AM		Event	Default	Default Call-Out Off	1 alarm email sent to WWTP:Operator	
	2019-07-17 8:52:22 AM		Active	Pump & Blower Building	Pump & Blower Building\Driver\No Compressor Running\Common Alarm	No Compressor Running Common Alarm (Alarm)	

History: 1000 records. History has been limited to 1000 records.

Upcoming WaterISAC Events

- Monthly Water Sector Cyber Threat Briefing
  - Wednesday, January 26, 2022; 2:00 – 3:00 PM ET

Register on WaterISAC's Events webpage:
https://www.waterisac.org/events

Thank You

WaterISAC Contact Information:

1-866-H2O-ISAC

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Charles Egli
Preparedness and Response Director
egli@waterisac.org

Alec Davison
All-Hazards Risk Analyst
davison@waterisac.org

Kaitlyn Palatucci
Membership Engagement Director
palatucci@waterisac.org

Jennifer Lyn Walker
Infrastructure Cyber Defense Director
walker@waterisac.org

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