Introduction to Cybersecurity: Workshop and Response Exercises

OCTOBER 2020

United States
Environmental Protection
Agency

Introduction to Cybersecurity: Workshop and Response Exercise (Virtual)
October 13-14, 2021

Day 1 – October 13, 2021

1:00 PM: Welcome, Introductions, and Logistics (Horsley Witten Group, Inc.)

1:10 PM: Threat Overview (Booz Allen Hamilton)

2:10 PM: Cybersecurity Drivers and Resources in the Water Sector (Horsley Witten Group, Inc.)

2:30 PM: Break

2:45 PM: Cybersecurity Best Practices: Case Study from Virginia Waterworks Assessments and Cybersecurity Technical Assistance Project (Booz Allen Hamilton)

4:25 PM: Closing Remarks/Evaluations (Horsley Witten Group, Inc.)

4:30 PM: Adjourn

Day 2 – October 14, 2021

1:00 PM: Welcome, Introductions, and Logistics (Horsley Witten Group, Inc.)

1:05 PM: Cybersecurity Incident Response Plan (Horsley Witten Group, Inc.)

1:20 PM: Cybersecurity and Infrastructure Security Agency Resources (DHS CISA: Ron Ford, Cybersecurity Advisor, Region I)

2:10 PM: Federal Bureau of Investigation Incident Response (FBI: Jae Park, Supervisory Special Agent and Marylu Smith, Intelligence Analyst)

2:30 PM: Break

2:45 PM: Cybersecurity Response Exercise (Booz Allen Hamilton and Horsley Witten Group, Inc.)

4:30 PM: Cybersecurity Resources/Q&A (Booz Allen Hamilton)

4:55 PM: Closing Remarks/Evaluations (Horsley Witten Group, Inc.)

5:00 PM: Adjourn

EPA's Introduction to Cybersecurity Workshop and Response Exercise

Workshop Facilitators

Kyle Miller

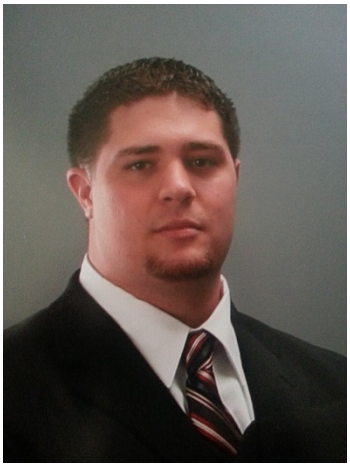
Principal/Director
OT Cybersecurity Practice Lead
Booz Allen Hamilton
LinkedIn: https://www.linkedin.com/in/kyle-miller-459b5410/

As a Principal/Director at Booz Allen Hamilton, Mr. Miller oversees the firm's Operational Technology (OT) Cybersecurity practice within the Global Commercial account. He acts as an ICS/SCADA cybersecurity subject matter expert to a myriad of clients, serves as technical director for internal ICS investment efforts, as well as leads client delivery across a number of market areas.

With over fifteen years of professional experience, Mr. Miller has worked with a multitude of clients across the manufacturing, oil & gas, mining, defense, energy, and water/wastewater critical infrastructure sectors. Specifically within the water/wastewater sector, Mr. Miller has supported various cybersecurity projects over the past 7 years for the U.S. Environmental Protection Agency (EPA). As an ICS/SCADA cybersecurity SME on these efforts, Mr. Miller has had the opportunity to develop cybersecurity assessment frameworks, conduct on-site assessments at dozens of water utilities, and train utility personnel on cybersecurity threats and best practices through a multi-year series of in-person and virtual trainings.

Jesse Stewart

Lead Associate
Booz Allen Hamilton
Email: stewart_jesse@bah.com



Mr. Jesse Stewart is a Lead Associate at Booz Allen with over 14 years of Cyber Security experience that spans Information Technology (IT) and Operational Technology (OT) in both the Commercial and Government sectors. He brings both team and project lead experience and has technical knowledge of many IT and OT tools and concepts. Jesse has supported clients in various OT environments including Automotive, Manufacturing, Pharmaceutical, and Utilities. Most recently he supported the development of an OT Incident Response program for a large multinational pharmaceutical company.

Sarah Bartlett

Staff Scientist
Horsley Witten Group
Email: sbartlett@horsleywitten.com

Sarah Bartlett is a staff scientist with the Horsley Witten Group. She works with utilities on emergency preparedness and response. She has assisted multiple water and wastewater utilities developing their Emergency Response Plans and Incident Specific Response Procedures to comply with the updated America's Water Infrastructure Act of 2018 (AWIA). Sarah has provided cybersecurity technical assistance to multiple water and wastewater utilities across the country and developed customized cyber action plans to help reduce their cyber risk. She also been communicating with you about this workshop and will be helping out with technical support during our workshop.

Gemma Kite, P.E.

Senior Environmental Engineer
Horsley Witten Group
Email: gkite@horsleywitten.com

Gemma has more than thirteen years of professional experience as an environmental engineer specializing in hydrogeologic investigations and modeling, water sector training, watershed planning and assessment, and stormwater design. As a Senior Environmental Engineer with the Horsley Witten Group, Ms. Kite works on a variety of projects with a focus on sustainability, including assisting utilities and EPA with emergency preparedness and response, particularly, with regards to cybersecurity. Gemma has assisted EPA in developing a variety of cyber resources and trainings for the water sector. On behalf of EPA, Gemma is leading a project to provide one-on-one cyber technical assistance with utilities.

Cybersecurity Threat Overview

Speaker Introduction

Kyle Miller

Principal/Director

OT Cybersecurity

Booz | Allen | Hamilton

EXPERIENCE SUMMARY

- 15+ years of professional experience, including as an ICS/SCADA security consultant across the manufacturing, oil & gas, mining, defense, nuclear, energy, and water/wastewater critical infrastructure sectors both within the U.S. and internationally
- Specialized in Systems Security Engineering, Security Test and Evaluations, and Risk Assessments for SCADA and ICS as well as enterprise-level IT systems

Certifications

- Certified Information Systems Security Professional (CISSP)
- Global Industrial Cyber Security Professional (GICSP)
- Certified Ethical Hacker
- Computer Hacking Forensic Investigator
- ISO 27001 Lead Auditor (BSI Group)
- Project Management Professional
- Splunk Certified Architect

Education

- M.S., Cybersecurity, University of Maryland Global Campus
- B.S., Information Technology, George Mason University

Jesse Stewart

Lead Associate

OT Cybersecurity

Booz | Allen | Hamilton

EXPERIENCE SUMMARY

- 10+ years of professional experience as a cyber security consultant spanning both OT and IT across the energy, defense, manufacturing, nuclear, and pharmaceutical, sectors both within the U.S. and internationally
- Specialized in Network Security Architecture, Certification and Accreditation, and Risk Assessments for both IT and OT environments, systems, and components.

Certifications

- Global Industrial Cyber Security Professional (GICSP)
- CompTIA Security+

Education

- B.S., Security & Risk Analysis; Information & Cyber Security, The Pennsylvania State University

Agenda

- **Introduction to OT/ICS/SCADA**
  - Introduction
  - Common Components and Terms
  - Cybersecurity Challenges
- **Water Sector Threats**
  - Evolving threats to water sector
  - Growing threats to SCADA systems
  - Escalation in ransomware
- **Cybersecurity Threat Overview Conclusion**

Agenda

- **Introduction to OT/ICS/SCADA**
  - Introduction
  - Common Components and Terms
  - Cybersecurity Challenges
- **Water Sector Threats**
  - Evolving threats to water sector
  - Growing threats to SCADA systems
  - Escalation in ransomware
- **Cybersecurity Threat Overview Conclusion**

What is OT/ICS/SCADA?

OPERATIONAL TECHNOLOGY (OT)

- Term that encompasses *multiple types of process and Industrial Control System (ICS)* that support physical processes
- Although different, often *used interchangeably* with the term *Supervisory Control and Data Acquisition (SCADA)*

FOUND ACROSS SEVERAL CRITICAL INFRASTRUCTURES

NON-EXHAUSTIVE

- OIL & GAS EXPLORATION, PRODUCTION, DISTRIBUTION, AND REFINING

- ELECTRIC POWER GENERATION, TRANSMISSION, AND DISTRIBUTION

- MANUFACTURING, LOGISTICS, AND DISTRIBUTION CENTERS

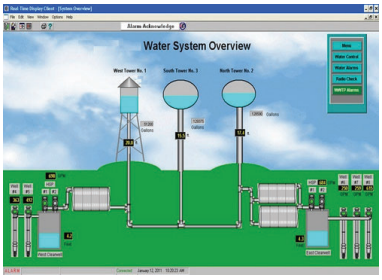
- WATER, WASTEWATER, NATURAL GAS, AND OTHER PUBLIC UTILITIES

- COMMERCIAL FACILITIES AND DATA CENTERS

EPA

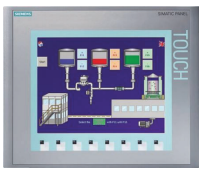
Common Components

Throughout the training we'll be referencing a number of SCADA system components, here are just a few key ones



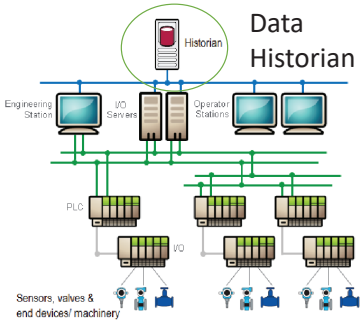
HUMAN MACHINE INTERFACE (HMI)

Used for operators to view SCADA system status and manipulate system setpoints



PROGRAMMABLE LOGIC CONTROLLER (PLC)

Embedded device programmed with logic to perform specific Input/Output (I/O) functions including controlling valves, pumps, and motors



DATA HISTORIAN

A centralized database supporting data analysis using statistical process control techniques

EPA

Insecure by Design

Many SCADA systems were not built with security in mind, so challenges exist in making them cyber-secure after the fact

- SCADA systems were built with uptime and availability in mind, not security
- Many common IT security capabilities such as encryption and authentication are not common in SCADA protocols
- Equipment lifespans are far longer in SCADA systems than in IT which leads to a high volume of legacy equipment
- Enhanced features of newer SCADA devices increases the attack surface
- New vulnerabilities are being identified all the time, but updating of firmware can be infrequent

EPA

SCADA Vulnerabilities

New vulnerabilities are identified and published weekly and highlight security gaps that attackers could take advantage of

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ADVISORIES

ICSA-21-236-02 : Hitachi ABB Power Grids Utility Retail Operations and CSB Products
ICSA-21-236-03 : Delta Electronics TPEditor
ICSA-21-168-03 : Advantech WebAccess/SCADA (Update A)
ICSA-19-253-03 : Siemens Industrial Products (Update N)
ICSA-21-189-01 : Rockwell Automation MicroLogix 1100
ICSA-21-189-02 : MDT AutoSave
ICSA-20-084-01 : VISAM Automation Base (VBASE) (Update A)
ICSMA-21-187-01 : Philips Vue PACS
ICSA-21-187-01 : Moxa NPort IAW5000A-I/O Series Serial Device Server

ALERTS

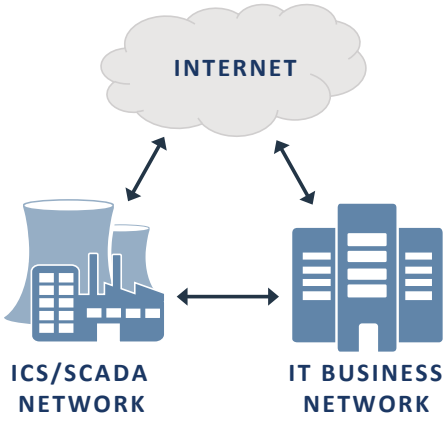
ICS-ALERT-20-217-01 : Robot Motion Servers
ICS-ALERT-20-063-01 : SweynTooth Vulnerabilities
ICS-ALERT-19-225-01 : Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A)

EPA

Increasing Number of Pathways

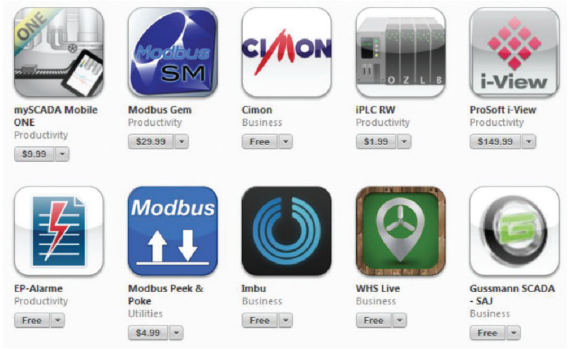
With advancements in technology and a blending of IT and SCADA, connectivity is growing between SCADA and the business

- Utility systems have become more automated (e.g., SCADA, on-line bill paying) to improve operational efficiency
- With the convenience of monitoring system status remotely, more waterworks are putting their SCADA systems online
- To achieve cost savings, vendors are increasing their use of remote access capabilities for troubleshooting
- Business users are more frequently requesting visibility into SCADA networks for monitoring utility operations



Remote Access Anywhere...

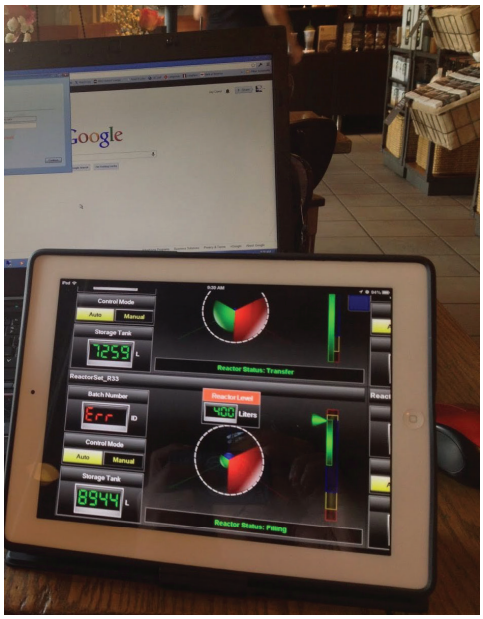
MOBILE APPLICATIONS

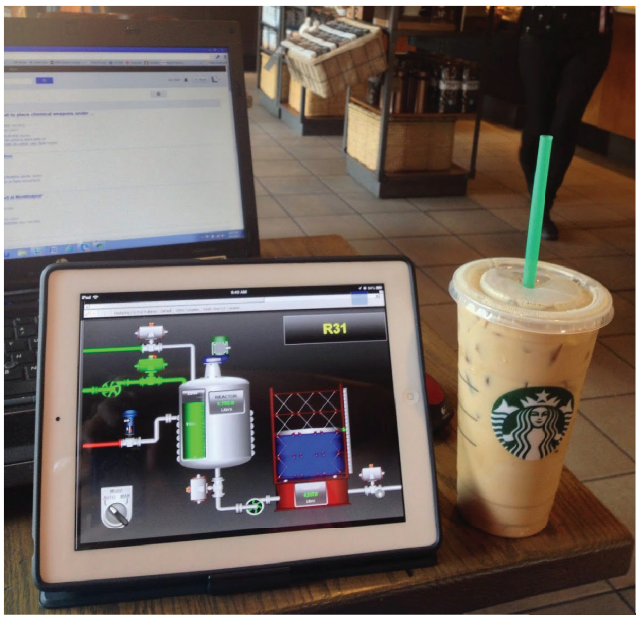


REMOTE ACCESS SOFTWARE

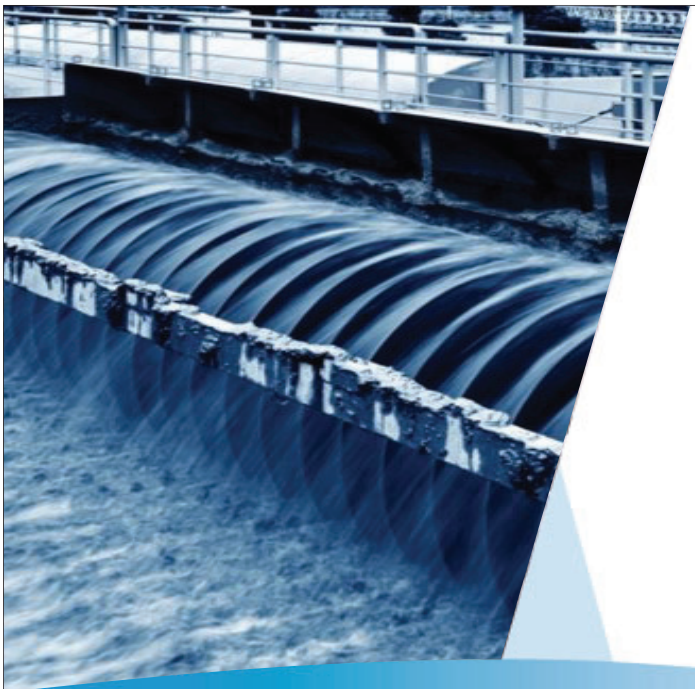
TeamViewer, VNC, CITRIX®, Symantec pcAnywhere, LogMeIn

No, Really, Remote Access Anywhere!





EPA



Agenda

- **Introduction to OT/ICS/SCADA**
  - Introduction
  - Common Components and Terms
  - Cybersecurity Challenges
- **Water Sector Threats**
  - Evolving threats to water sector
  - Growing threats to SCADA systems
  - Escalation in ransomware
- **Cybersecurity Threat Overview Conclusion**

EPA

"It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to its strategic position in keeping the wheels of industry turning and in preserving the health and morale of the American populace."

13

Evolving From a Traditional Resiliency Focus...

Responding to and recovering from a variety of non-cyber threats is part of a water utilities everyday focus

NATURAL INCIDENTS

- Hurricanes
- Ice storms
- Droughts

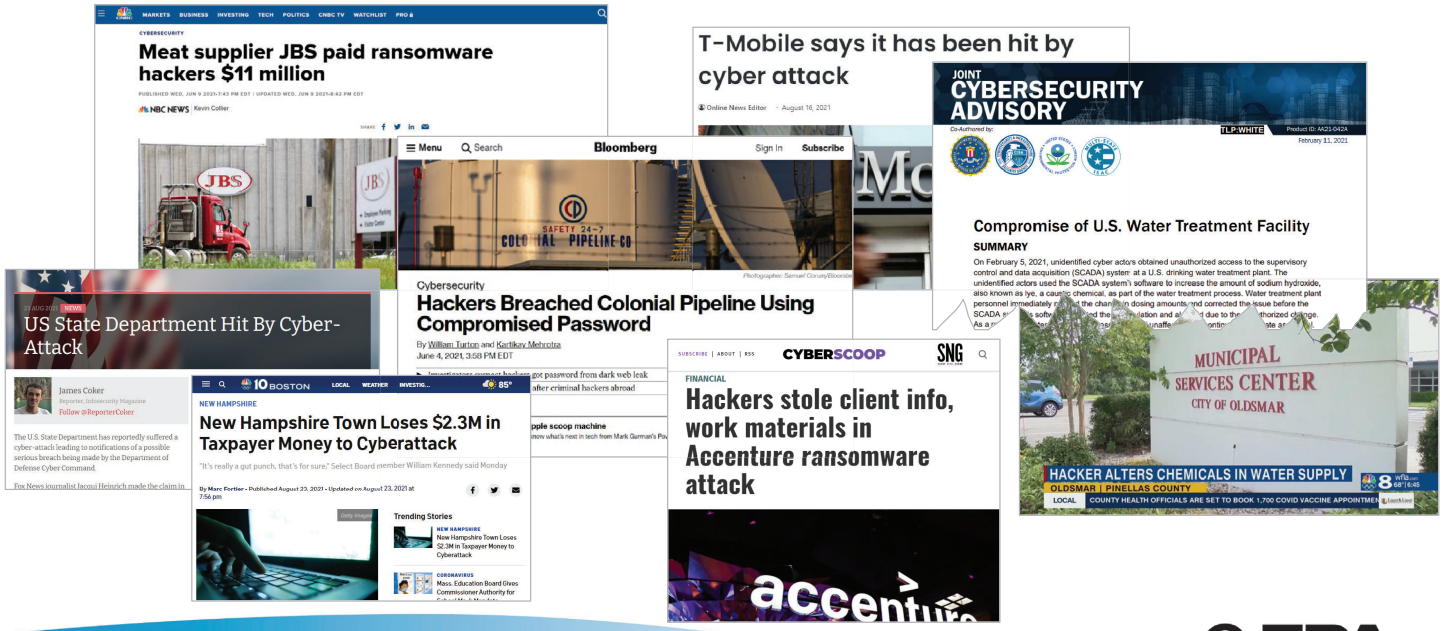
MAN-MADE INCIDENTS

- Power outages
- Spills
- Water main breaks

14

... to a Focus That Includes The Risk of Cyber Threats

The past couple years have seen an aggressive increase in cyber events impacting businesses and utilities alike



Increasing Threats and Impacts to SCADA

In the recent past, we have seen **publicly known** increasingly sophisticated attacks targeting core industrial sectors

- **Ukrainian Power Grid**
  - Power cut affected large parts of Ukraine in 2015 and 2016
  - Believed to be the first instance of a power outage caused by a cyber attack
- **NotPetya**
  - Impacted several companies across a variety of industries
  - Merck & Co. , for example, reported nearly $1.3B worth of losses
- **Triton/ Trisis**
  - Malware infected Schneider's Triconex safety system and was able to shut down a chemical plant
  - Analysis indicated the attack was sponsored by a nation-state
- **Norsk Hydro**
  - A ransomware attack forced Norsk Hydro, a Norwegian aluminum maker, to shut down several of its automated product lines
- **EKANS Ransomware**
  - ICS-focused ransomware interrupts Honda's business operations and production
- **Oldsmar Water Utility**
  - Cyber attackers gained access to the control systems of a water treatment plant in FL
  - Raised the feed rate for sodium hydroxide to a level harmful to humans
- **Colonial Pipeline**
  - Pipeline operator CP halted operations due to a ransomware attack by DarkSide
  - Led to gasoline supply shortages in several states in the southeast United States
- **JBS Foods**
  - Cyber attack on meat supplier JBS foods temporarily knocked out plants that process roughly one-fifth of the USA's meat supply

2015 → PRESENT

Cyber Threats Can Exist Anywhere

Enterprise IT / Business Threat Vectors

- Third Party Vendors – Billing / Equipment Suppliers
- Partner Network Connections
- Email – Phishing / Accidental Transmission

Operational Technologies / SCADA Threat Vectors

- Non-Hardened Devices
- Connectivity for Isolated / Remote Devices
- Insecure Ports and Protocols

Human Input / Human Error Threat Vectors

- Accidental transmission
- Misconfiguration
- Malicious Insider

Water Sector Cyber Event Case Studies

HARRISBURG, PA WATER TREATMENT PLANT

Date: October 2006

RISK VECTOR
Laptop computer connecting to both the public internet as well as the plant network

ATTACK SEQUENCE
An employee laptop used to check tank levels across multiple locations was compromised while connected to the public internet and used as an entry point to install a virus and spyware on the plant computers.

IMPACT
Luckily, the water treatment plant did not appear to be the target of an attack and the installed virus appeared to only use the host network to redistribute malicious email messages

LESSONS LEARNED
Engineering / maintenance equipment should never be allowed to connect to the public internet and then to the plant network or equipment. If the device can not be isolated from the internet, a virus / malware scanning kiosk should be used before connecting to the plant environment.

LANSING, MI BOARD OF WATER AND LIGHT

Date: April 2016

RISK VECTOR
Malicious email containing a ransomware infected attachment sent by attacker

ATTACK SEQUENCE
An employee opened a suspicious email containing a malicious attachment which then propagated across the environment encrypting files for ransom.

IMPACT
Files and folders of the boards communication system were encrypted and held ransom. The board shut down phone lines including the customer service line before ultimately paying the $25,000 ransom

LESSONS LEARNED
Suspicious emails should never be opened and a robust cyber awareness program and training should be implemented to raise cyber awareness for all employees

Water Sector Cyber Event Case Studies

ELLSWORTH, KS RURAL WATER UTILITY

Date: March 2019

RISK VECTOR
Shared or common credentials were utilized but were not changed or revoked upon employee termination or internal job role changes

ATTACK SEQUENCE
A former employee was able to use remote access software and the credentials from when he was employees at the utility to log into the system and disable the sanitation processes.

IMPACT
The attacker was able to remotely shut down the processes behind the facilities cleaning and disinfecting procedures but was caught before it impacted any customers.

LESSONS LEARNED
Password policies and procedure that address password revocation, expiration, and complexity should be in place and enforced

OLDSMAR, FL WATER TREATMENT PLANT

Date: February 2021

RISK VECTOR
Remote access tool, TeamViewer, hosted on a machine that contained an HMI

ATTACK SEQUENCE
TeamViewer credentials allowed unauthorized access to a computer system hosting a plant HMI: remotely, PLCs were manipulated to increase the levels of sodium hydroxide from 100 to 11,100 ppm.

IMPACT
The incident was identified by an alert operator before significant compromise of the water and the sodium hydroxide levels were returned to normal. Potential impact was a poisoned water supply.

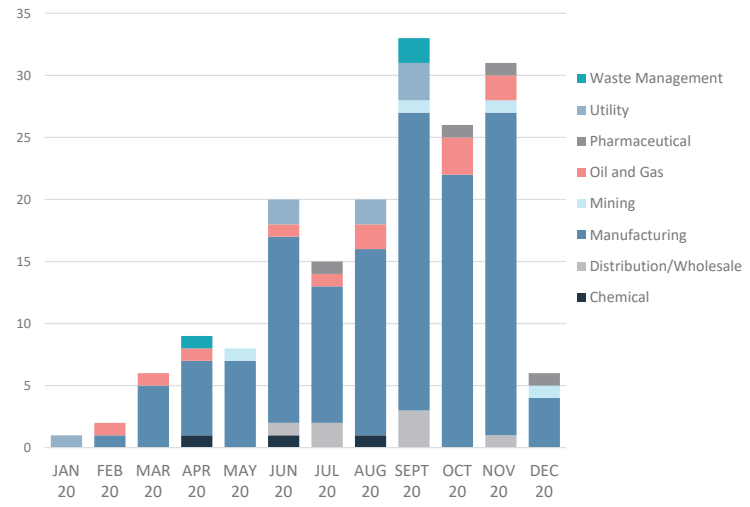
LESSONS LEARNED
Monitor for remote access and use an anomaly detection tool to protect systems with defined parameters. Underfunded and less protected systems can lead to an easier target.

EPA

Attackers are Increasingly Targeting SCADA

The escalation of post-compromise ransomware and the convergence of IT and OT has led to a corresponding spike in adversaries who view the cyber-immature OT environments as easy vectors to launch debilitating attacks

Number Of Threats Impacting OT-Driven Organizations

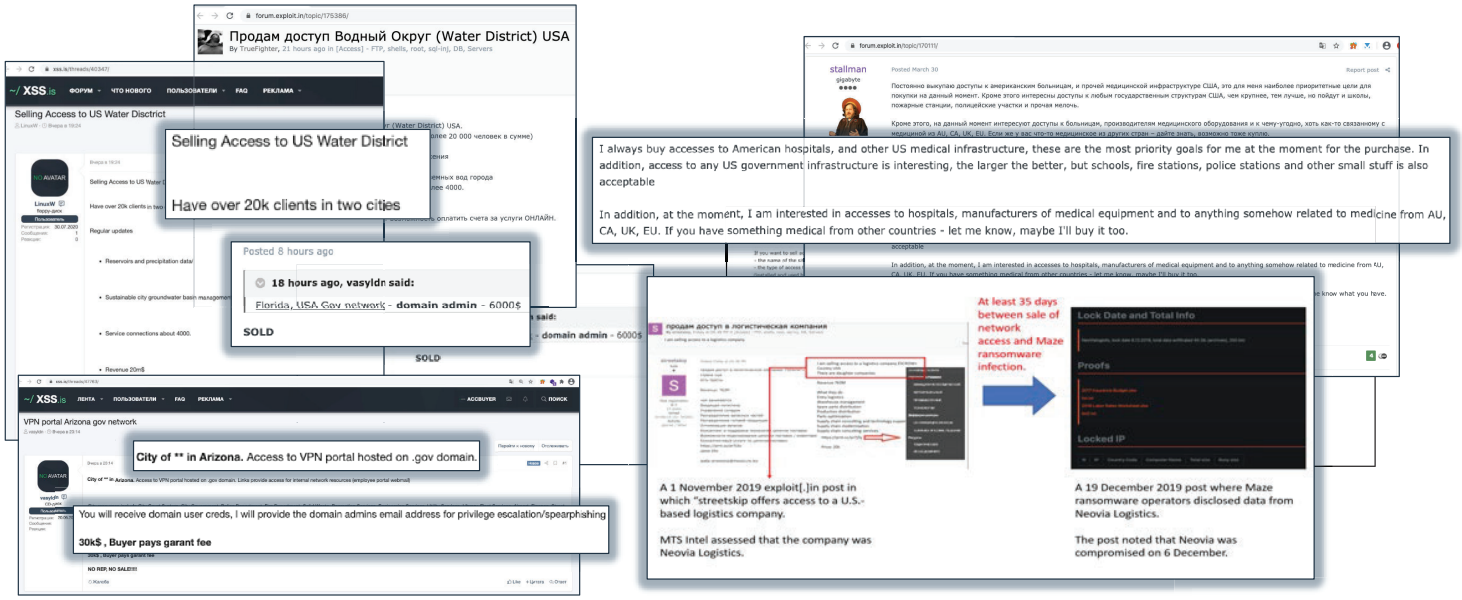


- 2020, and now 2021 has seen a significant uptick in threat actors targeting softer OT environments
- Researchers found attackers are gathering info on target networks to identify and deploy malware to critical assets and negotiate from a privileged position
- Attackers now leverage extortion in most ransomware attacks after recognizing the significant costs associated with operational disruptions

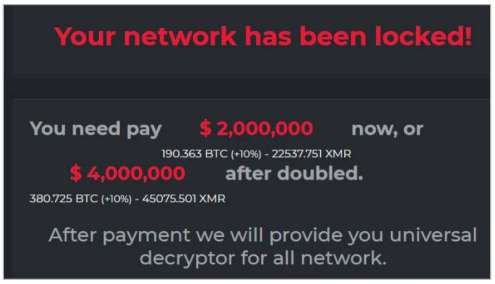
EPA

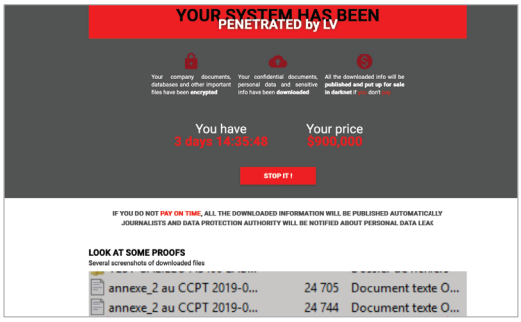
Growing Dark Web Activity

Across the "dark web", threat actors communicate with each other and offer to buy and sell cyber access to organizations



Explosive Growth of Ransomware





RANSOMWARE BY THE NUMBERS

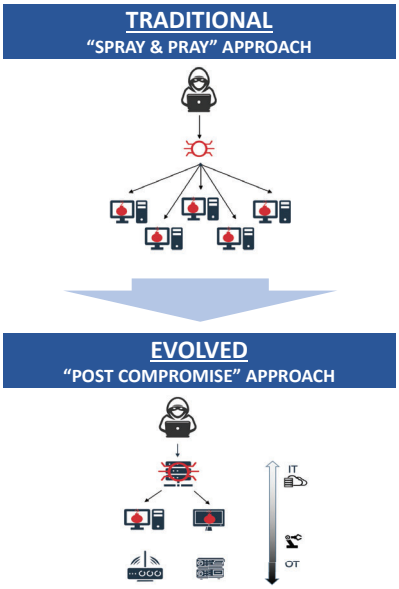
- **51%** of companies faced ransomware attacks
- **26%** of companies paid the ransom
- The average ransom amount in 2020 was **$180,000** for **big companies**
- The average ransom amount in 2020 for **small businesses** was **$6,000**
- A set of software tools needed to launch a ransomware attack costs about **$50 on the darknet**
- A new ransomware attack is detected every **11 seconds**

SOURCE: https://www.eweek.com/security/new-ransomware-trends-causing-fear-in-2021/

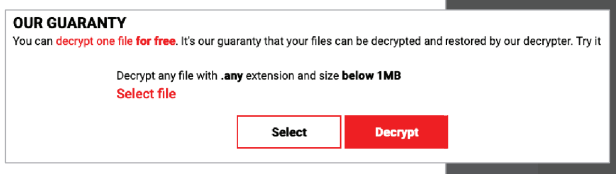
Evolution of Ransomware

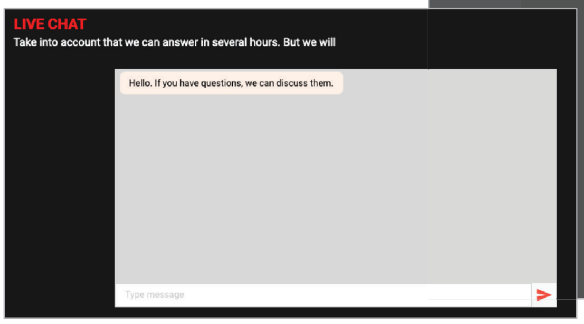
Ransomware has not just exploded in volume, but evolved in technique over the past several years

- Cybercriminal enterprises see themselves as businesses and many operate 24x7 in a shift model with support staff
- Evolved from traditional "spray and pray" to more targeted and sophisticated "post compromise" tactics
- Extortion is a common element, threatening to release sensitive files – backups are not a solution anymore
- Hundreds of millions of dollars in ransoms collected by ransomware groups
- No typical victim – from small businesses with <50 employees, to multi-nationals with Billions in revenue
- Starting Ransom demand is typically set based on victim size and exposure (e.g., $10M+ for B+ revenue companies)



Evolution of Ransomware





IT'S JUST A BUSINESS

We'll receive money anyway: from you or from the darknet

IF YOU DO NOT PAY

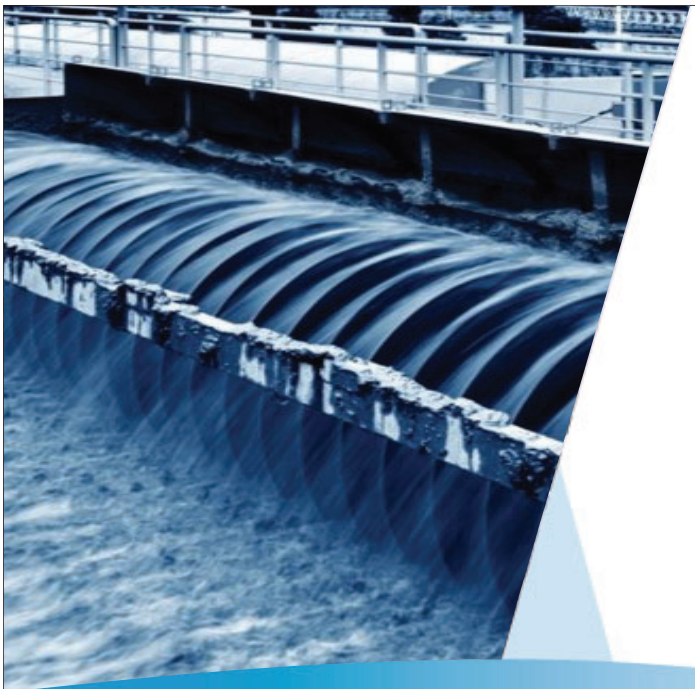
- You'll NEVER decrypt your files
- Your confidential data and the most important info, your clients' and employees' personal data will be published and sold out in DARKNET
- Your clients, employees, partners will be notified by e-mail that you haven't prevent their data leakage. That you've SOLD their personal data
- Journalists, data protection authority will be aware about the personal data leakage and breaking the Law (with PENALTIES per record)
- You'll LOOSE lots of time and data and reputation and money and clients. And they will be right cause you didn't meet consumer data protection obligations!

IF YOU PAY ON TIME

+ You'll RESTORE all your encrypted files and data IN MINUTES
+ You'll PREVENT news article that you didn't meet consumer data protection obligations. You'll save your reliable REPUTATION
+ You'll AVOID your company sensitive info publication and selling out in darknet for future EXPLOITATION
+ You'll PREVENT problems with state regulatory authority and ESCAPE punishment and penalties for violations and even court
+ We'll completely and permanently delete ALL your data from our disks
+ You'll continue work as reliable company and everything will be GOOD for you

Consequences of Attacks

BUSINESS IMPACTS
• Loss of data and **data integrity**
• Loss of plant **security**
• Operational **denial or disruption** of business services or production
• **Regulatory intervention** and legal liability
• **Monetary losses**
• **Costs** to the utility and region
• Brand/**reputation damage**
• Physical damage, injury, or **loss of life**
• **Erosion** of public **confidence**



Agenda

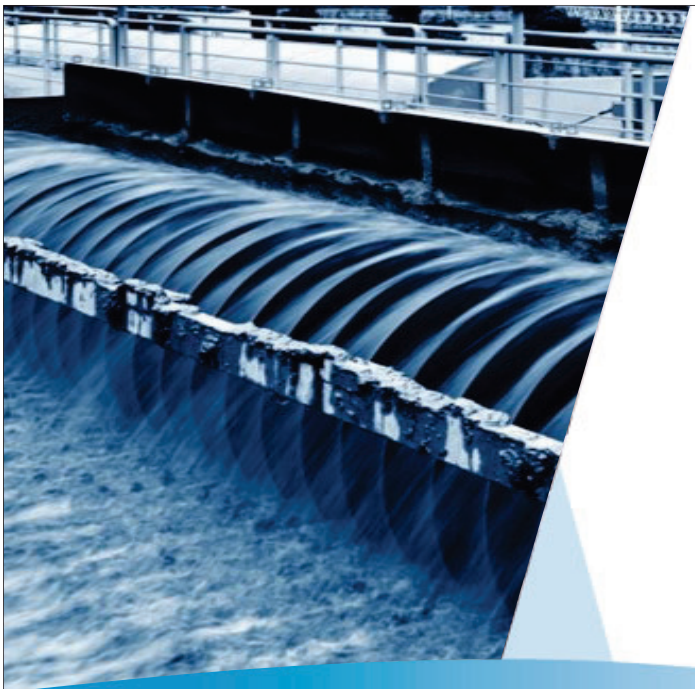
- **Introduction to OT/ICS/SCADA**
  - Introduction
  - Common Components and Terms
  - Cybersecurity Challenges
- **Water Sector Threats**
  - Evolving threats to water sector
  - Growing threats to SCADA systems
  - Escalation in ransomware
- **Cybersecurity Threat Overview Conclusion**

Threat Overview Conclusion

- Advancements in technology around SCADA systems is leading to **additional threat exposure** through **hyper-connectivity** and **remote access**
- Built with **uptime and availability** as priority, SCADA equipment has a longer lifespan, keeping **legacy equipment** in production and increasing **attack surface**
- **Ransomware**, in particular, is a large and **growing threat** to utilities of all sizes and requires **additional focus on cybersecurity best practices**
- With advancing threats and growing potential impacts of a cyber attack, having an **actionable cyber incident response plan** is critical
- Cyber threats across **both the business and SCADA** environments are **increasing** and **evolving** as time goes on

EPA

Cybersecurity Drivers and Resources in the Water Sector



Agenda

- **Cybersecurity Drivers**
  - America's Water Infrastructure Act
- **Cybersecurity Resources**
  - WaterISAC 15 Cybersecurity Fundamentals
  - EPA Cyber Incident Action Checklist
  - AWWA Tool
  - Cybersecurity Technical Assistance

Agenda

- **Cybersecurity Drivers**
  - America's Water Infrastructure Act
- **Cybersecurity Resources**
  - WaterISAC 15 Cybersecurity Fundamentals
  - EPA Cyber Incident Action Checklist
  - AWWA Tool
  - Cybersecurity Technical Assistance

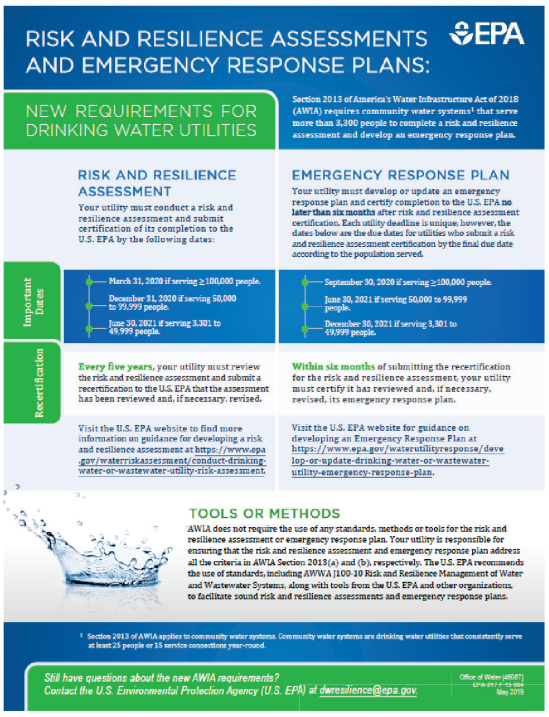
EPA

AWIA Section 2013 Overview

Requirements for Community Water Systems:

- Risk and Resilience Assessment
- Emergency Response Plan

https://www.epa.gov/waterresilience/americas-water-infrastructure-act-risk-assessments-and-emergency-response-plans



EPA

Cyber Components for Risk and Resilience Assessment

As specified in AWIA § 2013 (SDWA § 1433):

- Electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system
- The monitoring practices of the system (including network monitoring)
- The financial infrastructure of the system (meaning accounting and financial enterprise IT systems operated by a utility, such as customer billing and payment systems).

EPA

Cyber Components for Emergency Response Plan

As specified by AWIA § 2013:

1. Strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system
2. Plans, procedures, and equipment for responding to a malevolent act or natural hazard
3. Actions, procedures, and equipment to lessen the impact of a malevolent act or natural hazard, including alternative source water, relocation of intakes, and flood protection barriers
4. Strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

EPA

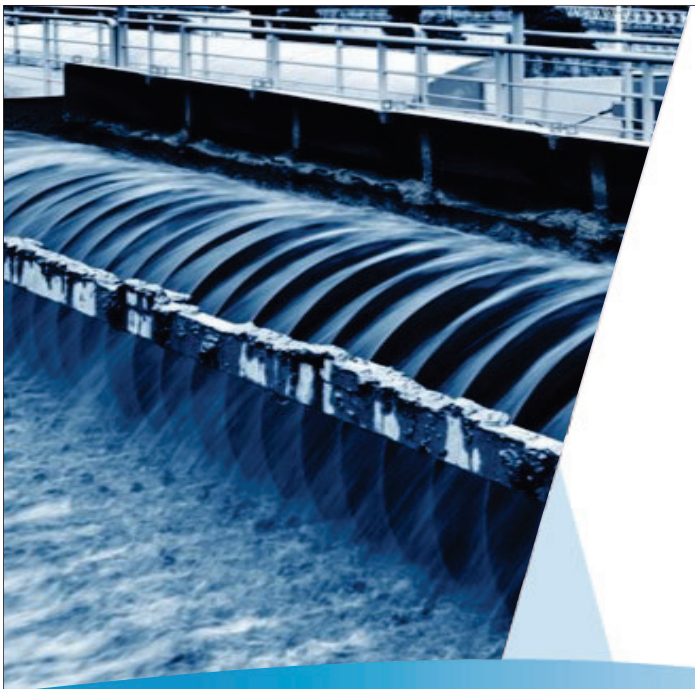
Example of Cybersecurity in Emergency Response Plan

[CWS Name] Emergency Response Plan

AWIA ERP TEMPLATE

Cybersecurity	
Item	**Description**
Disconnect procedure	*If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware.*
Notification	*List who should be called in the event of a cyber incident, such as your utility information technology (IT) supervisor or your contracted IT service provider. Also list any external entities that may have remote connections to your network.* *Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) (888-282-0870 or NCCIC@hq.dhs.gov).*
Assess procedure	*Assess any damage to utility systems and equipment, along with disruptions to utility operations.*
Implementation processes	*Implement actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary) and provide public notification (if required).*
Documentation	*Include forms to document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).*
Other	

EPA



Agenda

- **Cybersecurity Drivers**
  - America's Water Infrastructure Act
- **Cybersecurity Resources**
  - WaterISAC 15 Cybersecurity Fundamentals
  - EPA Cyber Incident Action Checklist
  - AWWA Tool
  - Cybersecurity Technical Assistance

EPA

15 Cybersecurity Fundamentals

- Free resource, download at waterisac.org/fundamentals
- Provides overview of important security measures
- Links to additional information about each measure

EPA

Cyber Briefings and Alerts to Members

- Security & Resilience Updates (SRUs)
  - Twice-per-week (Tuesdays and Thursdays)
  - Includes sections on cybersecurity incidents, threats, and tools and upcoming events
- Cyber Threat Web Briefings
  - Monthly
  - Presenters from DHS NCCIC, cybersecurity firms, and WaterISAC
- Threat Notifications and Advisories
  - As necessary
  - Provide members with actionable information on urgent cybersecurity threats and incidents

In addition to these recommendations, CISA and FBI urge critical infrastructure asset owners and operators to review the following resources for best practices on strengthening cybersecurity posture:

- Ransomware Guide (CISA and MS-ISAC)
- CISA Ransomware Webpage: Ransomware Guidance and Resources
- CISA Insights: Ransomware Outbreak
- CISA Pipeline Cybersecurity Initiative
- CISA Pipeline Cybersecurity Resources Library

CISA encourages victims of ransomware to report incidents immediately to CISA, a local FBI Field Office, or a Secret Service Field Office.

National Critical Functions Assessment of Colonial Pipeline Shutdown
Also today, CISA published an UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) National Critical Functions (NCFs) Assessment of Colonial Pipeline's halt of operations. This product provides an overview of Colonial Pipeline's operations and services and the emerging and projected impacts of fuel disruptions on NCFs.

Read the assessment at WaterISAC. *FOR U.S. MEMBERS.*

Next Steps
WaterISAC will continue to share information with its members and partners as more is learned about this developing incident. Members are encouraged to share information with WaterISAC by emailing analyst@waterisac.org, calling 866-H20-ISAC, or using the online incident reporting form.

- The WaterISAC Team

EPA

EPA's Incident Action Checklist for Cybersecurity

Customizable checklist to help utilities prepare for, respond to and recover from a cyber incident

Actions to Prepare for a Cyber Incident

Utility

- ☐ Identify all mission critical information technology (IT) systems, considering business enterprise, process control and communications. Document the key functions of the mission critical objectives, and identify the personnel or entity responsible for operating and maintaining each IT system.
- ☐ Identify an overall IT security lead to coordinate with each IT system manager and oversee all cyber-related duties.
- ☐ Ensure that IT system managers enforce cybersecurity practices on all business enterprise, process control and communications systems. For example, verify adherence to user authentication, current anti-virus software and installation of security patches.
- ☐ Review and update the utility's emergency response plan (ERP) to address a cyber incident impacting business enterprise, process control and communications systems. Account for all potential impacts on operations, and ensure emergency contacts are current.
- ☐ Prevent unauthorized physical access to IT systems through security measures such as locks, sensors and alarms. Include workstations and process control systems (e.g., programmable logic controllers or PLCs).
- ☐ Train all essential personnel to perform mission critical functions during a cyber incident that disables business enterprise, process control and communications systems. Include the manual operation of water collection, storage, treatment and conveyance systems.

EPA

AWWA Cybersecurity Guidance and Tool

- Water sector guidance that provides a consistent and repeatable result
- Developed by a panel of utility representatives, vendors, consultants and federal agencies
- Facilitates compliance with AWIA
- Consistent with NIST Cybersecurity Framework
- Aligns with other AWWA practices and standards
- Access the tool and guidance: www.awwa.org/cybersecurity

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

EPA

EPA Cybersecurity Technical Assistance

- EPA is providing free cybersecurity technical assistance to water and wastewater utilities across the country to improve cyber incident preparation, response, and recovery in order to maintain critical operations and meet water quality goals
- To date, EPA has provided assistance to over 100 utilities
- Participating utilities information remains confidential. Only anonymized, aggregated data is shared with EPA
- To register your utility: www.horsleywitten.com/cybersecurityutilities

EPA

Other Resources

- NIST Cybersecurity Framework
- AWWA Cybersecurity Risk and Responsibility Guide
- EPA's VSAT
- EPA's ERP Guidance and Template
- EPA's Baseline Information on Malevolent Threats
- NIST Standards
- DHS Cybersecurity Resources
- ISO Standards

EPA

Cybersecurity Best Practices:
Case Study from Virginia Waterworks Assessments and Cybersecurity Technical Assistance Project

Agenda

- **Assessment Case Study Background and Findings**
  - Virginia Waterworks Assessment Project
  - Cybersecurity Technical Assistance Project
- **Cybersecurity Best Practices**
  - Cybersecurity Leadership, Roles, and Responsibilities
  - Asset inventory and Vulnerabilities
  - Emergency Response Plan
  - Secure Data Backup
  - Vulnerability Management and Endpoint Protection
  - Minimize Exposure of Control Systems to Cyber Attacks
  - Enforce Access Controls
- **Cybersecurity Best Practices Conclusion**

Agenda

- **Assessment Case Study Background and Findings**
  - Virginia Waterworks Assessment Project
  - Cybersecurity Technical Assistance Project
- **Cybersecurity Best Practices**
  - Cybersecurity Leadership, Roles, and Responsibilities
  - Asset inventory and Vulnerabilities
  - Emergency Response Plan
  - Secure Data Backup
  - Vulnerability Management and Endpoint Protection
  - Minimize Exposure of Control Systems to Cyber Attacks
  - Enforce Access Controls
- **Cybersecurity Best Practices Conclusion**

EPA

Water Utility Assessment Case Studies

Two separate efforts, both sponsored by EPA, to assess the current cybersecurity posture of water utilities and provide assistance through detailed assessment reports or action plans

Virginia Waterworks Assessment Project

- Sponsored by EPA Region III and Virginia Department of Health (VDH)
- Took place over 2014, 2015, and 2016
- 30 water utilities across six VDH Regions serving a total population of approx. 1,740,000 people
  - Smallest utility: ~700 people
  - Largest utility: ~289,000 people

Year 1	Year 2	Year 3
2013-2014	2014-2015	2015-2016
14 New Sites	10 New Sites	6 New Sites 6 Return Sites

Cybersecurity Technical Assistance Project

- Sponsored by EPA Water Security Division
- Began in 2020, continuing through today
- ~130 water utilities currently assessed across 20 states serving a total population of approx. 1,800,000 people
  - Smallest utility: ~150 people
  - Largest utility: ~176,000
- Consisted of an initial assessment, followed by two follow-up assessments for each participating utility

EPA

Virginia Waterworks Assessment Project

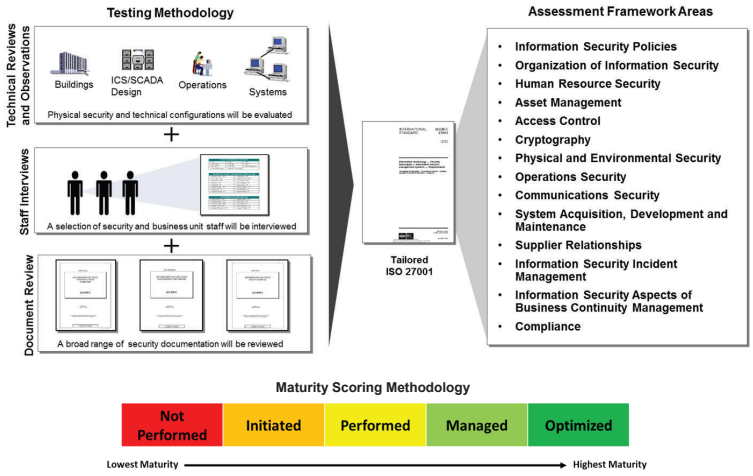
Logistics

- On-site assessments reviewed both **control systems and connected business systems**
- Measured cybersecurity **maturity** (against ISO 27001) and qualitative **risk**

Outputs

- Each utility received a detailed assessment report with their **findings** and **recommended remediations**
- Focused on **low and no cost** solutions
- Only **aggregated, anonymized** results shared

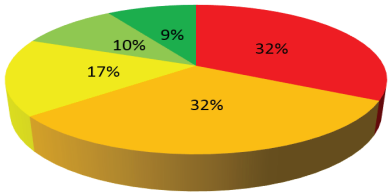
Methodology



Virginia Waterworks Assessment Project

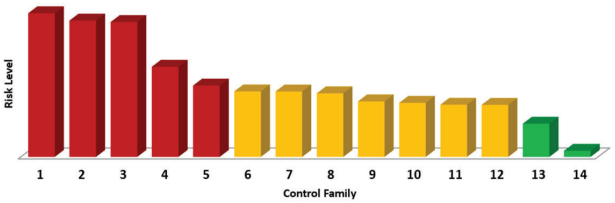
Results from all 30 of the assessments were anonymized and aggregated to identify the most common gaps and largest risks

Results: Overall Maturity



Maturity Level	Description
Not Performed	No action has been taken
Initiated	Basic actions are performed, but frequency is ad-hoc
Performed	Basic actions are performed regularly and have been documented
Managed	Best practices are performed regularly, have been documented, but there are more effective actions that could be taken
Optimized	Best practices are performed regularly, have been documented, and the most secure methods are utilized

Results: Risk by Category



Control Families	
1. Access Control	8. Organization of Information Security
2. Communication Security	9. Info Security Business Continuity Mgmt.
3. Operations Security	10. Supplier Relationships
4. Physical and Environmental Security	11. Incident Management
5. Asset Management	12. Compliance
6. System Acquisition, Development, and Maint.	13. Cryptography
7. Human Resource Security	14. Information Security Policies

Cybersecurity Technical Assistance Project

Logistics

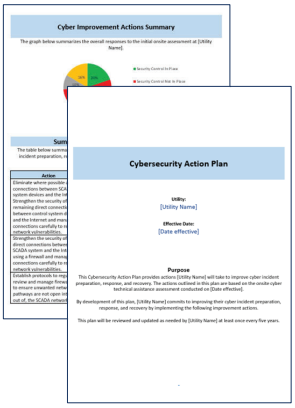
- **Virtual interview** workshops held with utility stakeholders
- Evaluated **61 question responses** across **30 categories** and **7 families**

Control Families
1. Cybersecurity Leadership, Roles and Responsibilities
2. Asset Inventory and Vulnerabilities
3. Emergency Response Plan
4. Secure Data Backup
5. Vulnerability Management and Endpoint Protection
6. Minimize the Exposure of Control Systems to Cyber Attacks
7. Enforce Access Controls

- **Two follow-up** virtual workshops scheduled approx. 6 months apart
- The **initial results**, **progress** against the action plan, and **challenges** were tracked

Outputs

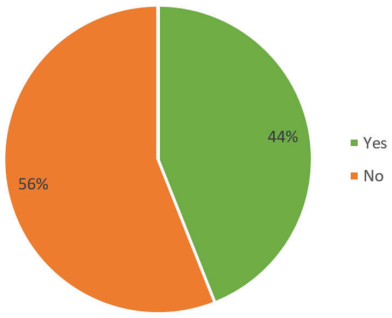
- After the **initial** assessment, each utility received a customized **Cybersecurity Action Plan**
- Action plans were then **owned and managed** by the utility and could be **adjusted as needed**
- During the follow-up workshops, **progress** against each action plan item was captured along with any **challenges** or **concerns** in completing items



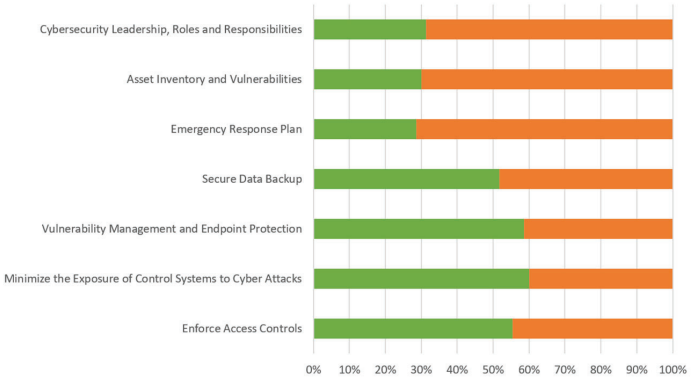
Cybersecurity Technical Assistance Project

Overall results from the first 129 initial assessments is aggregated, anonymized, and displayed below

Results: Overall Question Responses



Results: Responses by Control Family

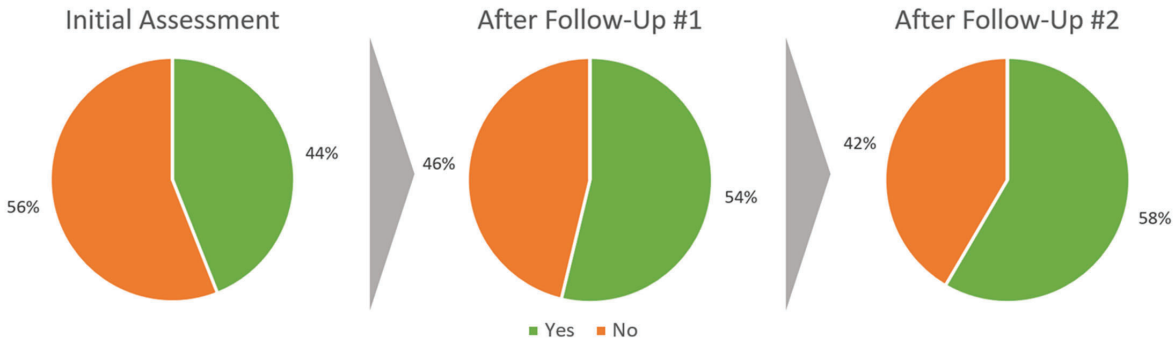


*NOTE: 'Not Applicable' and 'I Don't Know' responses excluded

Cybersecurity Technical Assistance Project

Upon completion of each follow-up assessment, progress against the initial responses was tracked

Results: Overall Yes/No Question Responses After Follow-Ups



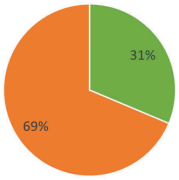
*NOTE: 'Not Applicable' and 'I Don't Know' responses excluded

EPA

Agenda

- **Assessment Case Study Background and Findings**
  - Virginia Waterworks Assessment Project
  - Cybersecurity Technical Assistance Project
- **Cybersecurity Best Practices**
  - Cybersecurity Leadership, Roles, and Responsibilities
  - Asset inventory and Vulnerabilities
  - Emergency Response Plan
  - Secure Data Backup
  - Vulnerability Management and Endpoint Protection
  - Minimize Exposure of Control Systems to Cyber Attacks
  - Enforce Access Controls
- **Cybersecurity Best Practices Conclusion**

EPA



Control Family #1

Cybersecurity Leadership, Roles, and Responsibilities

Covers the implementation of a cybersecurity lead, roles and responsibilities, and cybersecurity training

EPA

Cybersecurity Leadership, Roles, and Responsibilities

Cybersecurity Lead

- Assign an individual with overall lead responsibility for cybersecurity
  - Assign specific duties
  - Provide training opportunities
  - Assign a backup staff member

Cybersecurity Roles and Responsibilities

- Assign clear roles and responsibilities to utility managers and staff around cybersecurity
- Develop a list of cybersecurity best practices
- Require an Acceptable Use Agreement to be signed
- Conduct employee training regarding cybersecurity
- Include execution of cybersecurity roles as part of employee performance evaluations

Key Assessment Results

60% — Have assigned an individual as cybersecurity lead

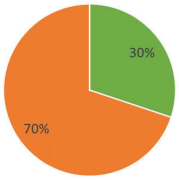
33% — Provide training opportunities for cybersecurity lead

21% — Have developed a list of cybersecurity best practices

38% — Require staff to sign an Acceptable Use Agreement

*NOTE: Based on initial assessment results

EPA



Control Family #2

Asset inventory and Vulnerabilities

Covers the inventory of a utility's IT and SCADA assets as well as the conducting of vulnerability/risk assessments

EPA

Asset inventory and Vulnerabilities

Asset Inventory

- Conduct an inventory of IT and SCADA related assets
- Include details such as brand/model, software/firmware version, physical location, and asset owner
- Keep inventory up-to-date as equipment is replaced and software is upgraded

Vulnerability/Risk Assessments

- Conduct a vulnerability or risk assessment of critical business and SCADA systems
- Establish protocol for regularly conducting these assessments
- Document and prioritize assessment outcomes, tracking progress against the action plan

Key Assessment Results

47% Have conducted an asset inventory of IT and SCADA

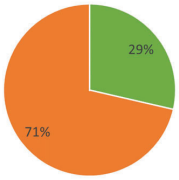
21% Include details of assets within asset inventory

25% Conduct a vulnerability or risk assessment

18% Prioritize actions as a result of an assessment

*NOTE: Based on initial assessment results

EPA



Control Family #3

Emergency Response Plan

Covers the inclusion of various cybersecurity domains within a utility's ERP/ISRP as well as conducting drills and response exercises for responding to a cyber incident

EPA

Emergency Response Plan

Inclusion of Cybersecurity within ERP/ISRP

- Ensure ERP/ISRP includes key elements of cybersecurity:
  - Protocols for manual overrides of SCADA
  - Cyber incident escalation (internal and external)
  - Data breach response actions
  - Isolation of compromised equipment
  - Clear or replace compromised equipment
  - Secure backup restoration

ERP/ISRP Exercises and Debriefs

- Conduct regular drills and exercises on how to respond to a cyber incident
- Debrief findings after an exercise or incident

Key Assessment Results

26% — Include cybersecurity within the ERP/ISRP

40% — Have cyber incident escalation paths documented

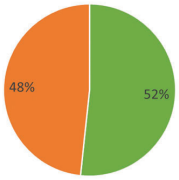
19% — Address sensitive data breaches within ERP/ISRP

4% — Conduct drills/exercises for responding to a cyber incident

*NOTE: Based on initial assessment results

EPA

16



Control Family #4

Secure Data Backup

Covers key protocols around the backup of critical data, testing of backups, and secure storage of backups

EPA

Secure Data Backup

Critical Data Identification

- Identify all business-critical data
- Identify all SCADA and operations critical data

Data Backups

- Regularly backup all critical data
- Store data backups in physically separate location
- Keep backups logically disconnected from primary network

Testing of Backups

- Regularly test all data backups
- Conduct test restoration of systems to validate backups

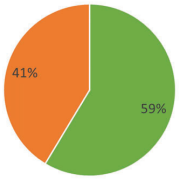
Key Assessment Results

50%	Identify critical data across business and SCADA systems
70%	Regularly backup all critical data
35%	Regularly test data backups
19%	Complete a system restore to validate backups

*NOTE: Based on initial assessment results

EPA

18



Control Family #5

Vulnerability Management and Endpoint Protection

Covers the defense of system endpoints through patching, updates, anti-malware protection, and alert/advisory monitoring

EPA

Vulnerability Management and Endpoint Protection

Updates and Patches

- Regularly apply Windows/OS level updates/patches
- Regularly apply application-level updates/patches
- Regularly apply device-level firmware updates/patches
- Formalize a process to ensure regular updating

Cybersecurity Alerts and Advisories

- Monitor sources of cybersecurity alerts and advisories
- Implement a process to respond to critical alerts

Anti-Malware/antivirus Protection

- Ensure anti-malware protection is installed, where possible, on business and SCADA systems
- Enable automatic updating or regularly install signatures

Key Assessment Results

59% — Regularly apply all Windows updates to IT and SCADA

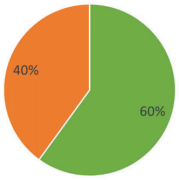
50% — Regularly apply application and device level updates

40% — Have designated personnel receive DHS alerts/advisories

71% — Have anti-malware protection installed

*NOTE: Based on initial assessment results

EPA



Control Family #6

Minimize Exposure of Control Systems to Cyber Attacks

Covers key areas of network segmentation and perimeter security particularly around restricting connectivity between SCADA, business, and the Internet

EPA

Minimize Exposure of Control Systems to Cyber Attacks

Network Connectivity Survey

- Conduct a network survey to identify all possible routes between SCADA and the Internet

Network Perimeter Security

- Eliminate any direct connections between SCADA components and the Internet
- Utilize a firewall to secure the pathways between SCADA components and the Internet or business network
- Manage and review firewall rules on a regular basis

Network Segmentation

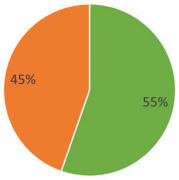
- Eliminate any unnecessary connections between SCADA networks and business networks
- Where possible, implement further zone-based network segmentation to limit blast radius

Key Assessment Results

42%	Conduct a network survey to identify possible routes
53%	Eliminate direct connections between SCADA and Internet
75%	Utilize a firewall between SCADA and other networks
44%	Manage and review their firewall rulesets

*NOTE: Based on initial assessment results

EPA



Control Family #7

Enforce Access Controls

Covers several areas of cybersecurity including user and password management, remote access, logging, and monitoring

EPA

Enforce Access Controls

Account Management

- Implement account access/permissions based on role
- Restrict administrator level accounts to only admins

Password Management

- Enforce good password hygiene
- Change all default passwords
- Lock out accounts after multiple incorrect attempts

Logging and Monitoring

- Enable logging on key systems and audit logs regularly
- Deploy network monitoring systems where possible

Remote Access Management

- Practice secure remote access methods (e.g., VPN)
- Employ multi-factor authentication for remote access

Key Assessment Results

70% — Implement role-based user access control

64% — Change default passwords when devices are installed

26% — Utilize cybersecurity network monitoring systems

48% — Have audit logging enabled on internal systems

*NOTE: Based on initial assessment results

EPA

24

Enforce Access Controls

Time it takes a Hacker to Brute Force your password

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Agenda

- **Assessment Case Study Background and Findings**
  - Virginia Waterworks Assessment Project
  - Cybersecurity Technical Assistance Project
- **Cybersecurity Best Practices**
  - Cybersecurity Leadership, Roles, and Responsibilities
  - Asset inventory and Vulnerabilities
  - Emergency Response Plan
  - Secure Data Backup
  - Vulnerability Management and Endpoint Protection
  - Minimize Exposure of Control Systems to Cyber Attacks
  - Enforce Access Controls
- **Cybersecurity Best Practices Conclusion**

Cybersecurity Best Practices Conclusion

- While it appears many utilities are making an effort to improve, the state of water utility cybersecurity is still in need of **significant improvement**
- Many of the cybersecurity gaps identified throughout these projects highlight a need to focus on **basic cyber hygiene** as a first step for most utilities
- Several **no-cost** and **low-cost** measures exist that can greatly reduce cybersecurity risk
- Cybersecurity **threats are evolving**, and **new vulnerabilities** are being discovered every day
- A **proactive cybersecurity program** should be introduced at utilities and include ongoing assessments, action plan tracking, and monitoring of threats

EPA

27

Sign up to be part of the Cybersecurity Technical Assistance Project Now!

- Participating utilities can expect to receive a straightforward overview of their vulnerabilities and suggested best practices to reduce risks to business enterprise, SCADA, and communications systems
- Additionally, the utility will develop a cyber action plan with HWG and work to implement any recommended best practices at its own pace.
- HWG will contact the utility on two separate occasions after the development of the cyber action plan to gauge progress and see if additional assistance is required.
- All individual utility information gathered during the assessment will be protected and remain confidential

To register your utility, please visit:
www.horsleywitten.com/cybersecurityutilities

EPA

28

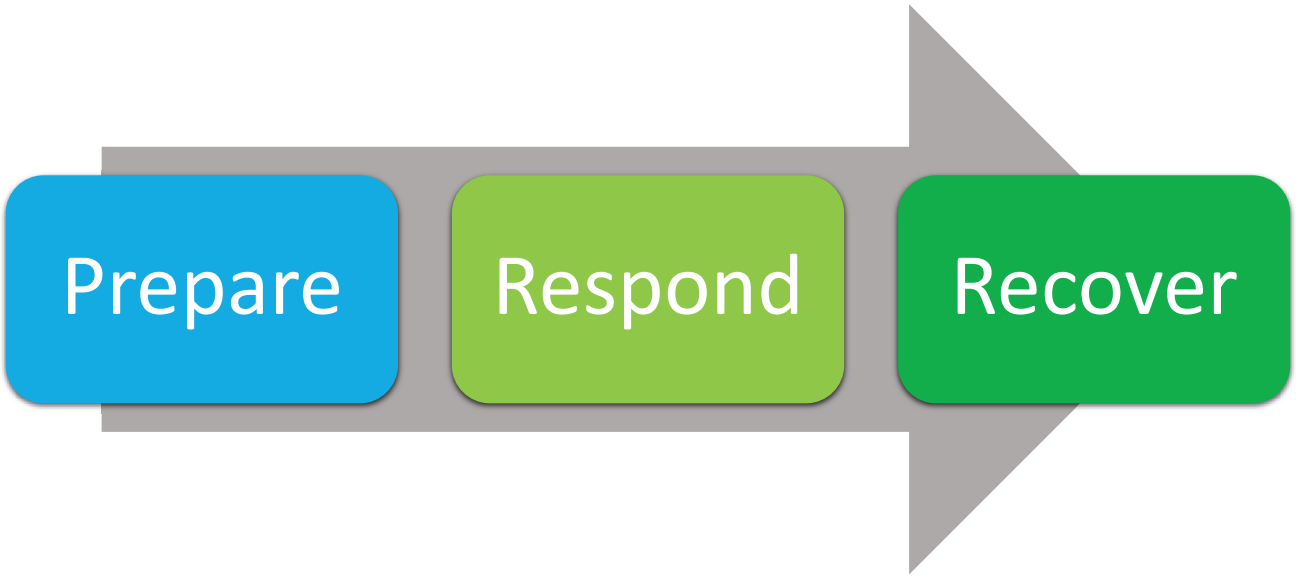
Cybersecurity Incident Specific Response Plan

What is Cybersecurity Incident Response?

"Cyber incident response is the way in which an organization responds to a perceived cyber-related incident that may impact ICS owner assets or their ability to operate. "

– ICS-CERT

Incident Response Life Cycle



Why is a Cybersecurity Incident Response Plan needed?

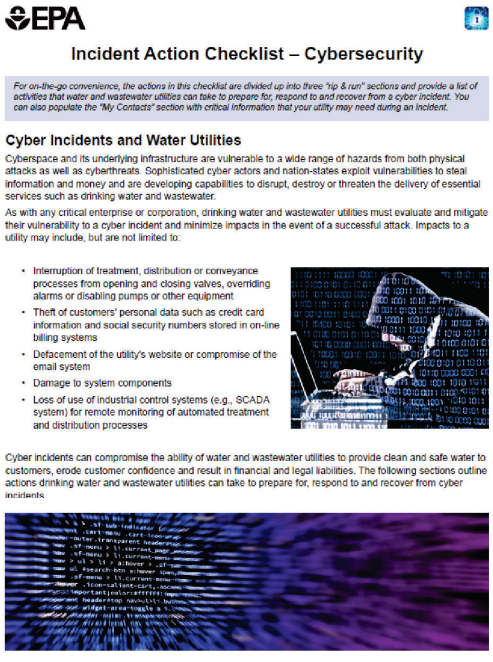
- All IT and OT systems are at risk of being disabled by a cyber-attack. An incident response plan can help you to:
  - Recover faster and at lower cost
  - Maintain essentially services (e.g., water delivery)
  - Understand what to do, who to tell, and how to get help
- A Cyber Incident Response Plan is a low/no-cost action that does not require cybersecurity expertise.
  - If you do nothing else, have an Incident Response Plan!

Incident Preparation

1. Create a Cyber Incident Specific Response Plan (ISRP)
   - Keep up-to-date contact information (e.g., law enforcement, CISA)
   - Exercise your IRP regularly and walk through scenarios

2. Implement cybersecurity best practices (e.g., AWWA Guidance, NIST Cybersecurity Framework)

Cyber ISRP Resource



EPA

Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three "rip & run" sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the "My Contacts" section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers' personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility's website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes

Cyber incidents can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence and result in financial and legal liabilities. The following sections outline actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents.

Incident Action Checklist

https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf

Elements of a Cyber ISRP

1. Actions to Respond to a Cyber Incident
   - Detection and Analysis
   - Containment
   - Reporting
2. Actions to Recover from a Cyber Incident
   - Eradication
   - Restoration
3. Contacts and Resources
4. Example Documentation Form

Example Actions to Respond to a Cyber Incident

- Disconnect compromised computers and devices from network to isolate
- Notify personnel that emergency assistance is needed, including external entities (e.g., vendors)
- Document the incident and response actions
- Execute the utility's Emergency Response Plan as needed
- Review system and network logs
- Take a forensic image of the affected systems
- Identify if Personally Identifiable Information (PII) has been compromised
- Report the incident

Example Actions to Recover from a Cyber Incident

- Obtain resources and assistance for recovery
- Eradicate any malware, corrupted files or other changes made due to incident
- Restore systems and files as required
- Make any changes to harden the system against any known vulnerabilities exploited during the incident
- Notify any affected employees and customers
- Debrief and develop a lessons learned document or After Action Report

EPA

Example Contacts and Resources

- Contact information for all utility personnel who would respond to incident:
  - IT and SCADA Staff/Vendor
  - Human Resources
- Contact information for external organizations/agencies that would be reported to:
  - Local law enforcement
  - State primacy agency
  - DHS/CISA
  - FBI
  - Other State cyber organizations

EPA

Example Documentation Form

Example Documentation Form		
Incident Details	Date/time that the incident was discovered:	
	Indicators observed:	
	Suspicious or relevant communications (before or during incident):	
	Description of the incident (e.g., how it was detected, what occurred):	
	Damage to Department OT systems:	

EPA

Example Documentation Form

	Response actions performed (e.g., disconnected computer from network):
	Other organizations contacted (e.g., software vendor, law enforcement):
General comments:	

EPA

Cyber ISRP Updates

- Ensure your ISRP is up to date, including:
  - Lessons learned from an incident or after exercising your plan
  - Latest contact information
  - Actions in response to new vulnerabilities and attack methods
- Communicate the plan and updates to staff and management

CYBERSECURITY THREAT LANDSCAPE AND FEDERAL RESOURCES

Jason Burt
Cybersecurity Advisor, Region IV
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Divisions of CISA

- CISA consists of:

Cybersecurity Division

Infrastructure Security Division

Emergency Communications Division

National Risk Management Center

CISA Mission and Vision

Cybersecurity and Infrastructure Security Agency (CISA)

Mission:

- Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

Vision:

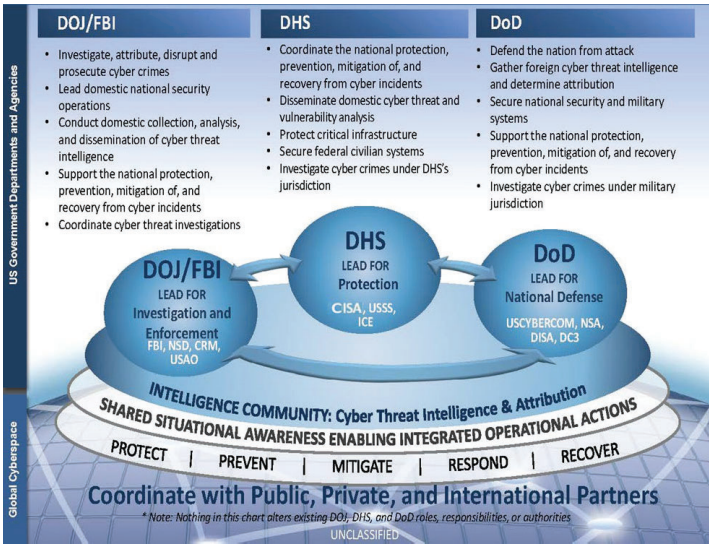
- A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

Federal Cybersecurity

TLP:WHITE

Whole of Government Response (DOJ/FBI, DHS/CISA, DoD)

- Presidential Directives
  - HSPD 5 — Domestic Incidents
  - PPD 8 — National Preparedness
  - PPD 21 — Critical Infrastructure Security & Resilience
  - PPD 41 — US Cyber Incident Coord Activities Defined
- Disseminates Domestic Cyber Threat Information
- Protects Critical Infrastructure
- Secures Federal Civilian Executive Branch Systems
- Directives are implemented through doctrine, policy, plans
  - National Cyber Strategy
  - National Preparedness System
  - National Infrastructure Protection Plan (NIPP)
  - National Cyber Incident Response Plan (NCIRP)



Federal Incident Response

Federal Incident Response

- **FBI - Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.

- **CISA - Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.

CISA CYBER+INFRASTRUCTURE

Federal Incident Response

Threat Response	Asset Response
Federal Bureau of Investigation 855-292-3937 or cywatch@ic.fbi.gov **FBI Internet Crime Complaint Center** ic3.gov	**Cybersecurity and Infrastructure Security Agency** **CISA CENTRAL (24x7 Operations Center)** 888-282-0870 or Central@cisa.dhs.gov Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
U.S. Secret Service secretservice.gov/contact/field-offices	
Immigration and Customs **Homeland Security Investigations** 866-347-2423 or ice.gov/contact/hsi	

CISA CYBER+INFRASTRUCTURE

CISA Cybersecurity Offerings

TLP:WHITE

Local CSA Provided

- **Preparedness Activities**
  - Information/Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices / MS-ISAC – EI-ISAC
  - **Cybersecurity Service Offerings**
    - Cyber Resilience Reviews (**CRR**)
    - External Dependency Management (**EDM**)
    - Cyber Infrastructure Surveys (**C-IST**)
    - Cyber Security Evaluation Tool (**CSET**)

CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

Cybersecurity Advisors (CSA)

- Assessments
- Working group collaboration
- Resiliency Workshops
- Best Practices private-public
- Incident assistance coordination

Protective Security Advisors

- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection
- Support for National Special Security Events

Delivered by CISA Vulnerability Mgt Team

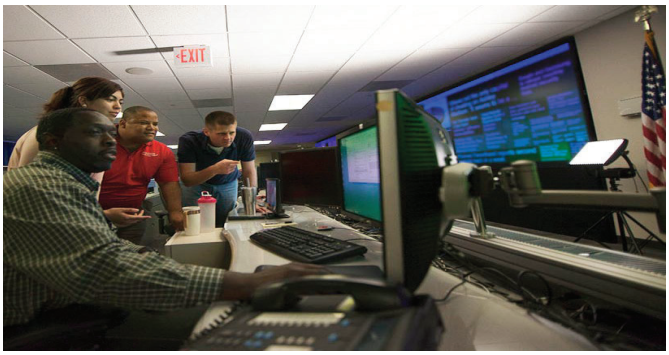
- Phishing Campaign Assessment (PCA)
- Cyber Hygiene Scanning (CyHy)
- Web Application Scanning (WAS)
- Remote Penetration Testing (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)
- Validated Architecture Design (VADR)
- Critical Product Evaluation (CPE)
- CISA Qualification Initiative (CQI)

CISA 24x7 Operations Center

CISA Central:

- **Operations**
  - Cyber Threat Hunting and Incident Response Teams
  - Vulnerability Management Team (VM)
    - Risk and Vulnerability Assessments (RVAs)
    - Phishing Campaign Assessments (PCA)
    - Vulnerability Scanning
    - Validated Architecture Design Review (VADR)
  - Cybersecurity Advisors
  - Cyber Security Evaluation Tool (CSET™)

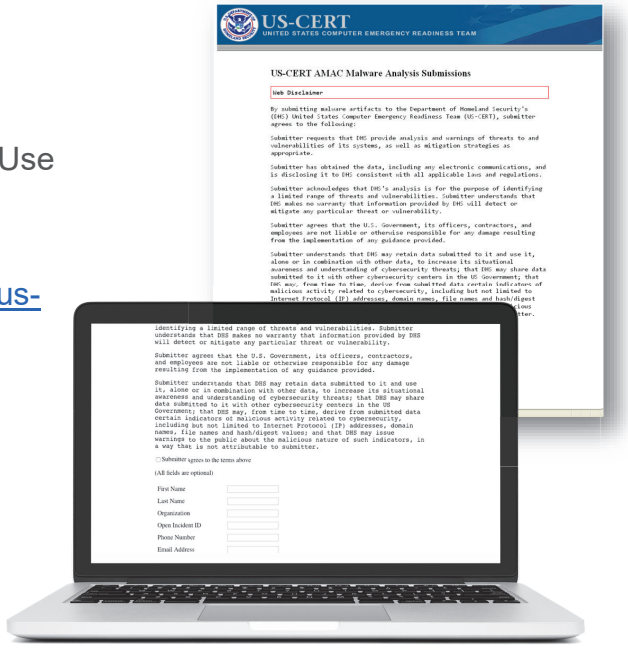
- **Cyber Threat Detection and Analysis**
  - Cyber Exercises
  - Malware Analysis
  - National Cyber Awareness System
  - Publications and Communications



Malware Analysis

To submit malware:

- Email submissions to NCCIC at: submit@malware.us-cert.gov
  - Send in password-protected zip file(s). Use password “infected.”
- Upload submission online: https://malware.us-cert.gov



Oldsmar Water Treatment Incident

Event: SCADA operator noticed remote access to control system.

Impact: Sodium Hydroxide level increased from 100 ppm to 11,100 ppm.

Specifics: Two separate incidents. Operator stated that TeamViewer was used to remotely access SCADA control system. Chemical level increased. Operator adjusted level back to normal value and disconnected the system from the network.

- HMI running Windows 7
- Multiple Remote Access programs running
- TeamViewer immediately uninstalled

Lessons learned:

- Never uninstall applications – Disconnect from NET and report.
- Limit Internet exposure to SCADA systems
- Segment Network
- Enforce Role-based Security & Logging

Sample of Cybersecurity Services (Voluntary & No-Cost to You)

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can't protect if you don't know what needs protection
- Can't fix what needs if you don't know what's wrong

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

VULNERABILITY SCANNING / HYGIENE

Vulnerability Scanning / Hygiene

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

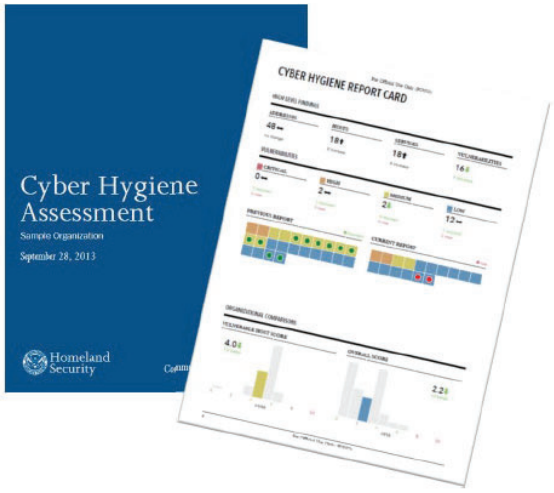
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

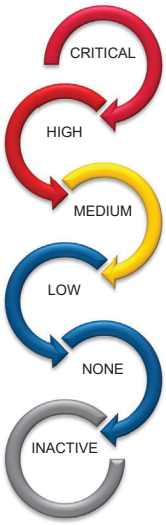
Network Vulnerability & Configuration Scanning:

- Identify network vulnerabilities and weakness



CyHy: Vulnerability Scanning

System & Application Vulnerability Scanning



- Automated scanning of Internet accessible systems (Top 1000 Ports / NMAP & NESSUS)
- Weekly report card that include current scan results, historic trends, and result comparisons to the national average
- Helps individual customers understand their exposure
- Informs national risk management efforts
- Federal agencies must mitigate critical vulnerabilities within 30 days of detection
- Scans can start within 72 hours!
- Unlimited capacity of subscribers

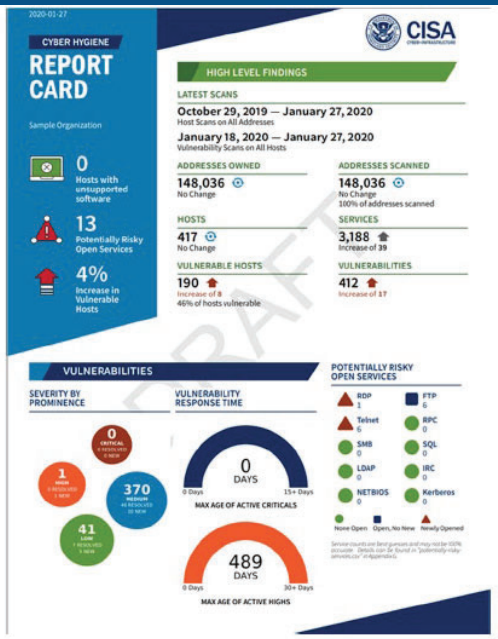
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

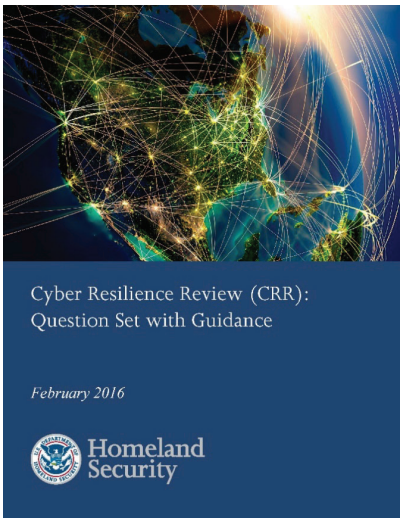
- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



CYBER RESILIENCE REVIEW

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**
- Delivery: Either
  - CSA-facilitated, or
  - Self-administered
- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



CRR Question Set & Guidance

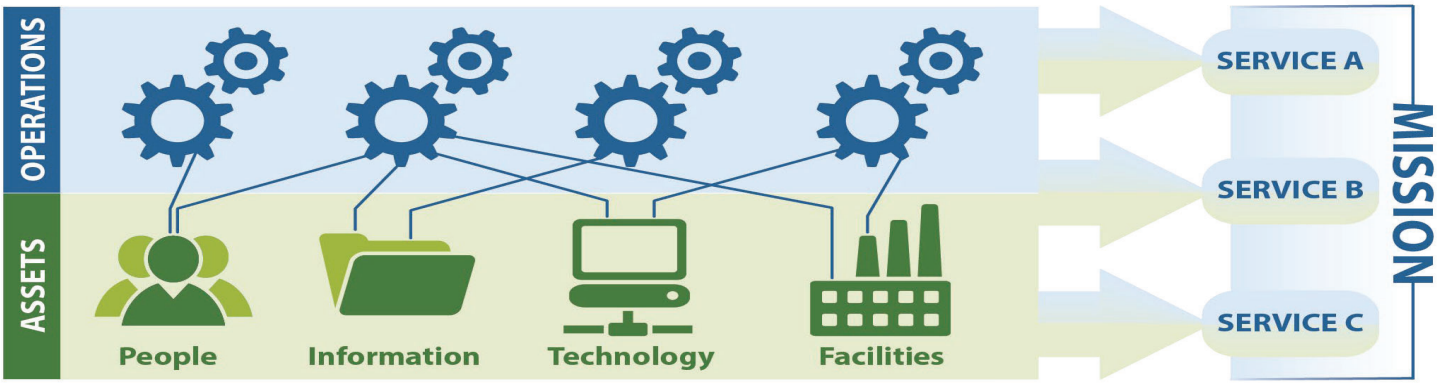
Cyber Resilience Review Domains

Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

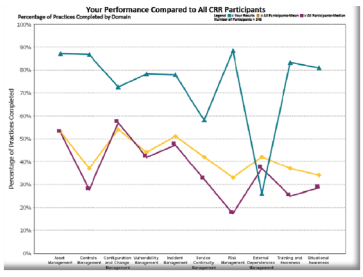
Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**



CRR Sample Report

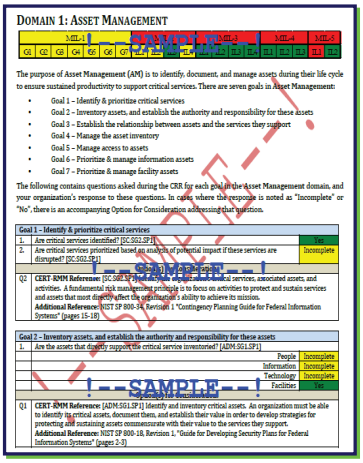
Each CRR report includes:



Comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

EDM Assessment Organization and Structure

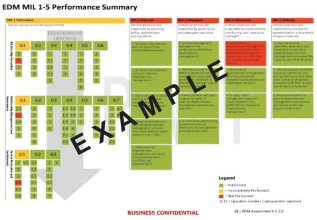
- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation *Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
Relationship Management and Governance *Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.*
Service Protection and Sustainment *Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.*

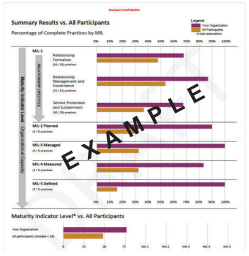
EDM Assessment Report

Each EDM report includes:

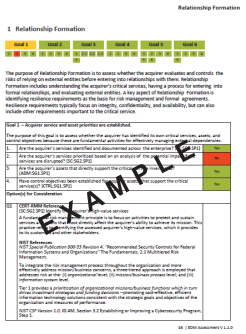
- Performance summary of existing capability managing external dependencies



- Comparison data with other EDM participants



- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



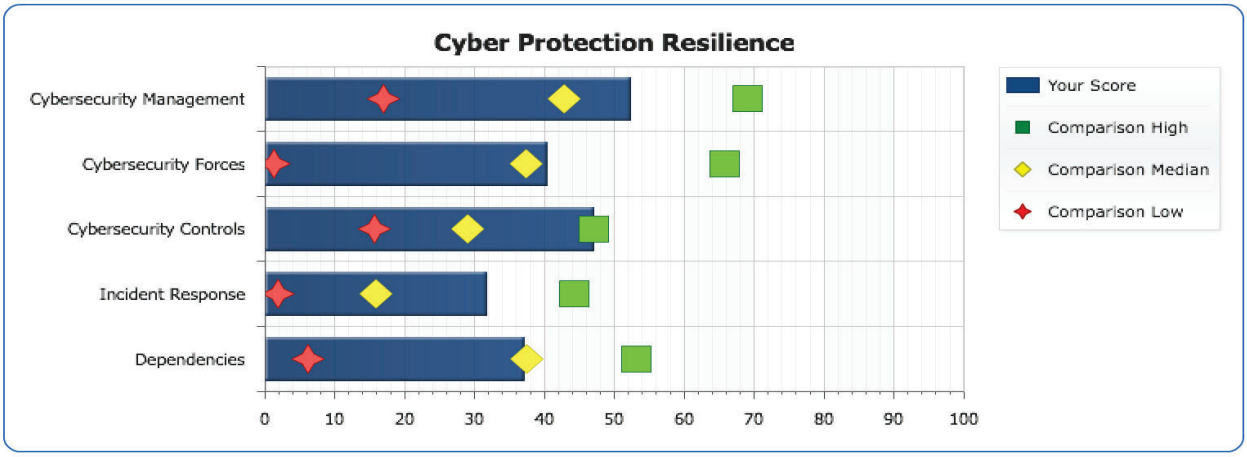
CYBER INFRASTRUCTURE SURVEY

Cyber Infrastructure Survey (CIS)

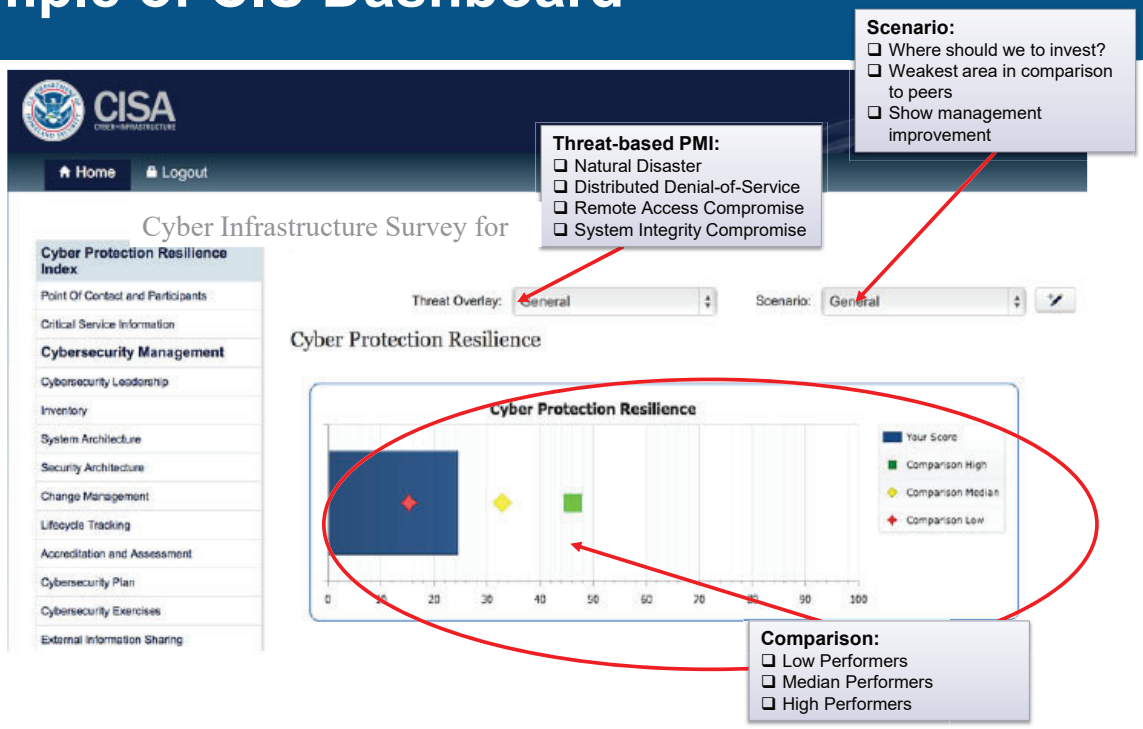
- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation.

CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate



Example of CIS Dashboard



29

CISA REGION 1

RON FORD

Cybersecurity Advisor, Region 1 (ME, MA)
Cybersecurity and Infrastructure & Security Agency
EMAIL: Ron.Ford@cisa.dhs.gov
CISARegion1@hq.dhs.gov
WEB: WWW.CISA.GOV
WWW.CISA.GOV/REGION-1

CISA CENTRAL - 24/7 Watch
(888) 282-0870;Central@cisa.dhs.gov

FBI's 24/7 Cyber Watch (CyWatch)
(855) 292-3937; CyWatch@fbi.gov

31

FBI Cyber Division
Water & Wastewater Sector

Jae Park
Supervisory Special Agent

UNCLASSIFIED

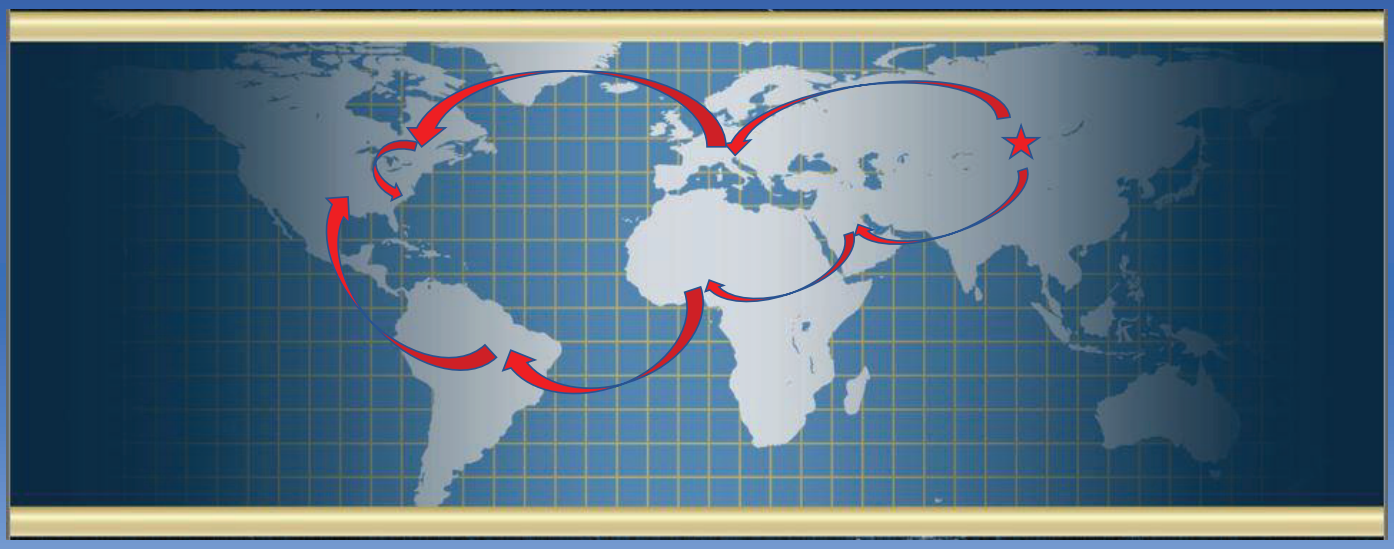
IMPOSING RISK AND CONSEQUENCES ON CYBER ADVERSARIES

Adversaries Target Our Critical Infrastructure

FBI CYBER

UNCLASSIFIED

An International Problem



Building Partnerships

- Big picture
- Coordination and partnerships across government and private sectors
- International collaboration

Cyber Division's Mission

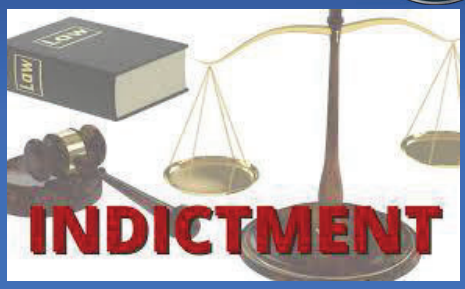
- Impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building upon a century of innovation

Working with the FBI

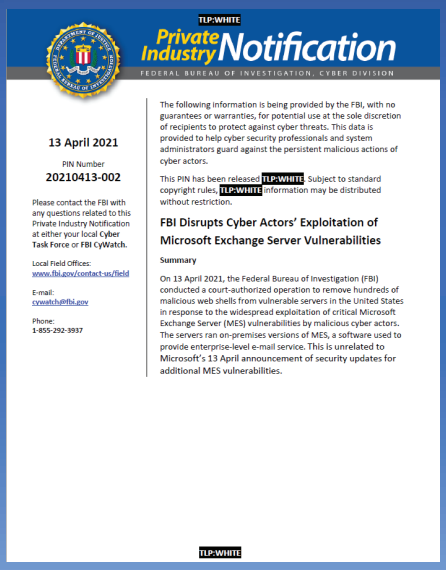
- We treat victims as victims
- Minimize disruptions to operations
- Seek only technical intrusion details
- FBI is law enforcement, not regulators
- Establish a relationship with your local Field Office

Indictment

- Unauthorized remote access into Post Rock Rural Water District systems in March 2019
- Shutdown facility's cleaning and disinfecting procedures
- On March 31, 2021, Wyatt Travnichek was indicted on federal charges and accused of tampering with a public water system
- Maximum prison time is up to 20 years in federal prison and a fine up to $250,000.
- Insider threat / former employee
- Lessons learned



FBI Information Sharing



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 April 2021

PIN Number
20210413-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local Cyber Task Force or FBI CyWatch.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

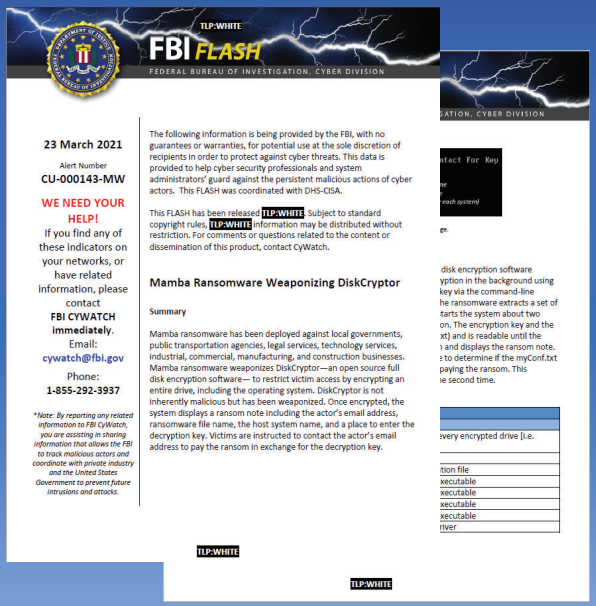
This PIN has been released TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

FBI Disrupts Cyber Actors' Exploitation of Microsoft Exchange Server Vulnerabilities

Summary

On 13 April 2021, the Federal Bureau of Investigation (FBI) conducted a court-authorized operation to remove hundreds of malicious web shells from vulnerable servers in the United States in response to the widespread exploitation of critical Microsoft Exchange Server (MES) vulnerabilities by malicious cyber actors. The servers ran on-premises versions of MES, a software used to provide enterprise-level e-mail service. This is unrelated to Microsoft's 13 April announcement of security updates for additional MES vulnerabilities.

TLP:WHITE



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 March 2021

Alert Number
CU-000143-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact FBI CYWATCH immediately.
Email:
cywatch@fbi.gov
Phone:
1-855-292-3937

*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators' guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For comments or questions related to the content or dissemination of this product, contact CyWatch.

Mamba Ransomware Weaponizing DiskCryptor

Summary

Mamba ransomware has been deployed against local governments, public transportation agencies, legal services, technology services, industrial, commercial, manufacturing, and construction businesses. Mamba ransomware weaponizes DiskCryptor—an open source full disk encryption software— to restrict victim access by encrypting an entire drive, including the operating system. DiskCryptor is not inherently malicious but has been weaponized. Once encrypted, the system displays a ransom note including the actor's email address, ransomware file name, the host system name, and a place to enter the decryption key. Victims are instructed to contact the actor's email address to pay the ransom in exchange for the decryption key.

TLP:WHITE

TLP:WHITE

Questions

- (U) Local Field Offices
- (U) Internet Crime Complaint Center
  - IC3.gov
- (U) Water-ISAC
  - Waterisac.org
- Email us at CyberOutreach_Water@fbi.gov