Public Water System, Certified Water Operators and Environmental Laboratories

COVID-19

Webinar # 2021-14

DRINKING WATER SECTION

Lori Mathieu

Environmental Health & Drinking Water Branch Chief

September 2, 2021

(1:00 PM – 2:00 PM)

CONNECTICUT DEPARTMENT *of* PUBLIC HEALTH

Keeping Connecticut Healthy

DPH

Connecticut Department of Public Health

Accredited Health Department • Public Health Accreditation Board •

PHAB

Advancing public health performance

DRINKING WATER SECTION

Webinar # 2021- 14
WEBINAR SERIES

Water Utilities

Certified Water Operators

Environmental Laboratories

09/02/2021

AGENDA

- Update from DPH COVID19
- DWS on Recent Developments
- Update from CTWC, Aquarion, RWA & MDC
- Update from other Municipal Water Systems
- Questions ?

DRINKING WATER SECTION

Webinar # 2021- 14
WEBINAR SERIES

Water Utilities

Certified Water Operators

Environmental Laboratories

09/02/2021

DPH/DWS Updates

- COVID19 – Updates
- Public Act Implementation
- DWS Circular Letters
- Cyber Security Updates
- Contaminants and Drinking Water Quality
- Operators Certifications Update
- Environmental Labs Certifications Update
- Drought Status
- DWSRF Reminder
- Key Provisions (IIJA)
- Drinking Water Infrastructure Needs Survey and Assessment
- WUCC Implementation

COVID -19 Updates

- **legislative Updates** 

  Gov. Ned Lamont's emergency powers extended through September

  The General Assembly voted for a 44-word resolution extending Gov. Ned Lamont's emergency powers through Sept. 30, making Connecticut among the last in the northeast under a COVID-19 state of emergency.

- **Executive Orders**

  - **Executive Order No. 13A** (08/05/2021)
    - **Authorization for municipal leaders to implement universal mask requirements; Modification of effective date on legislation that requires testing of nursing home staff.**

  - **Executive Order No. 13B** (08/06/2021)
    - **Requirement for employees of long-term care facilities to receive COVID-19 vaccinations.**

  - **Executive Order No. 13D** (08/19/2021)
    - **COVID-19 vaccination requirements for state employees, school employees, and childcare facility staff.**

  - **Executive Order No. 13C** (08/19/2021)
    - **Access to COVID-19 immunization information**

- **COVID-19 vaccine eligibility:**

  - All individuals who are 12 years of age or older and live, work, or attend school in Connecticut are eligible to receive the COVID-19 vaccine.
  - For more information on vaccinations and to learn how to get the vaccine, visit **ct.gov/covidvaccine**

- **FAQs - Vaccinations for Covered Workers in Schools** –

Public Act Implementation

- Public Act 21-121

- H.B. 6666 | **AN ACT CONCERNING THE DEPARTMENT OF PUBLIC HEALTH'S RECOMMENDATIONS REGARDING VARIOUS REVISIONS TO THE PUBLIC HEALTH STATUTES.**

- **Section by Section Breakdown of H.B. 6666 | Effective October 1st, 2021**

- **Section 1 and 2** revised Section 73 of Public Act 19-117 and Section 25-33(b) of the general statutes to remove specific population requirements for the replacement of an existing public well. This would permit the installation of a replacement well that does not meet the sanitary radius and minimum setback requirements, as specified in the Regulations of Connecticut State Agencies, when such a well is necessary for the water company to maintain and provide to its consumers a safe and adequate water supply.

- **Section 6** amends Section 19a-37 of the general statutes by adding the word “residential” to the definition of “private well” to clarify the difference between a private well and a semipublic well.

- **Section 7** includes language to require landlords to notify tenants of contaminants in their water supply not later than 48 hours upon notification of such contaminants.

Public Act Implementation

- Public Act 21-121 (continued)

- **Section 82** requires a water company, as defined in C.G.S. Section 25-32a, to provide an alternative source of drinking water to its customers when there is a water main break, loss of system pressure or other event that may affect the quality and quantity of drinking water being served and when the event will last more than twelve hours. The water company must also update their emergency response plan to address how such alternative source of drinking water will be provided.
- **Section 83** Requires water companies to produce tier 1 written notification to customers in three most languages predominantly spoken in the service area, water companies must update their emergency response plans to note in which languages the communication will be offered
- **Section 84** requires that all community water systems promptly report operational status to WebEOC within eight hours after the Governor issues a civil preparedness or public health emergency declaration.
- **Section 85** requires that, **by January 1, 2025**, owners of certain small community water companies produce capacity implementation plan (CIPs) to assist these owners in recognizing, funding and addressing upgrades to their systems prior to a failure of a system component, water quality issue, or development of a system deficiency.

Public Act Implementation

- Public Act 21-121 (continued)

- **Sections 86 and 87** require that bottlers collect samples prior to any water treatment and test each DPH approved bottled water source in Connecticut for unregulated contaminants such as PFAS, PFOA, manganese and 1-4 dioxane annually. Results of such testing must be provided to DPH and the Department of Consumer Protection (DCP) within nine days due to the public health concerns surrounding unregulated contaminants.

- **Section 88** requires that an environmental laboratory that conducts an analysis of a drinking water sample notify the public water system that requested the analysis not later than twenty four hours after obtaining a test result that shows a contaminant level that is in violation of the federal Environmental Protection Agency national primary drinking water standards. The water company must then report the result to DPH not later than twenty four hours after obtaining notification of said test result.

- **Section 89** requires health care institutions to obtain potable water, as a temporary measure to alleviate a water supply shortage, from a bulk water hauler or water bottler licensed in Connecticut.

Any questions, please contact:
Dan Aubin || Email: *Daniel.aubin@ct.gov*

DWS Circular Letters

DWS Circular Letter #2021-59

Sent on August 10, 2021

LIHWAP Survey for the Community Public Water Systems

DWS Circular Letter #2021-60

Sent on August 10, 2021

Memorandum from the White House on National Security - Cybersecurity

DWS Circular Letter #2021-61

Sent on August 20, 2021

Severe Weather Preparedness Reminder – Tropical Storm Henri

DWS Circular Letters

DWS Circular Letter #2021-63

Sent on August 22, 2021

Severe Weather Reminder – Tropical Storm Henri

DWS Circular Letter #2021-65 (Serving < 1000)

Sent on August 27, 2021

Drought Response and Water Loss Workshop for Small Water Utilities

Registration link | Wed 09/22/2021 at 9 am

DWS Circular Letter #2021-66 (Serving > 1000)

Sent on August 26, 2021

Drought Response and Water Loss Workshop for Medium & Large Water Utilities

Registration link | Thru 09/23/2021 at 9 am

CISA Region I (Connecticut)

Cybersecurity Advisor Program

Richard Berthao
Cybersecurity Advisor, Region I (CT)
Cybersecurity and Infrastructure Security Agency (CISA)

Cybersecurity Advisor Program

TLP:WHITE

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

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

CISA CYBER+INFRASTRUCTURE

Misconceptions Vs. Reality

Common Misconceptions		Reality
You need a big budget!	→	Step-by-step process: Crawl-Walk-Run
Silver Bullet!	→	Get the “101” stuff in order
Why would we be a target?	→	A good asset inventory will show you
There’s too much to do!	→	Research the solutions!
We don’t own the risk!	→	You do own the risk!

Current Cyber Trends and Topics

TLP:WHITE

What are some of the current trends and topics in the Cyber world?

CISA
CYBER+INFRASTRUCTURE

CISA ANALYSIS OF RISK AND VULNERABILITY ASSESSMENTS

TLP:WHITE

RISK AND VULNERABILITY ASSESSMENT (RVA) MAPPED TO THE MITRE ATT&CK® FRAMEWORK

FISCAL YEAR 2020 (FY20)

Risk and Vulnerability Assessment: Upon request, CISA can identify vulnerabilities that adversaries could potentially exploit to compromise security controls. CISA collects data in an onsite assessment and combines it with national threat information to provide customers with a tailored risk analysis report. To schedule an RVA or learn more, contact CISAServiceDesk@cisa.dhs.gov.

+ POTENTIAL ATTACK PATHS

Attack Path 1: Seems "Phishy" to Me

Initial Access - Phishing Link and MSHTA
Execution - PowerShell
Defense Evasion - Process Injection and MSHTA
Discovery - Network Sniffing
Collection - Data from Local System
Command & Control - Remote Access Software

Attack Path 2: Where is the Poison Control?

Initial Access - Valid Accounts
Execution - Windows Management Instrumentation
Credential Access - LLMNR/NBT-NS Poisoning and Relay
Discovery - Permission Groups Discovery
Collection - Data from Network Shared Drives
Command & Control - Standard Application Layer Protocol

Attack Path 3: Discover & Unlock

Initial Access - Trusted Relationship
Execution - Windows Management Instrumentation
Discovery - Permission Groups Discovery
Collection - Data from Local System
Command & Control - Remote Access Software

Attack Path 4: Take Into Account: Good Guy or Bad Guy?

Initial Access - User Execution
Execution - Windows Management Instrumentation
Discovery - Account Discovery
Collection - Data from Local System/
Data from Network Shared Drive
Command & Control - Remote Access Software
Exfiltration - Exfiltration over C2 Channel

Attack Path 5: Credential Convenience Has Its Cost

Initial Access - Valid Accounts
Execution - Windows Management Instrumentation
Credential Access - OS Credential Dumping
Discovery - Account Discovery
Collection - Data from Local System/
Data from Network Shared Drive
Command & Control - Remote Access Software

FY20 RVA RESULTS

MITRE ATT&CK Tactics and Techniques

This page is a breakout of the top three most successful techniques in each tactic. The percent noted for each technique represents the success rate for that technique across all RVAs. For example, a phishing link was used to gain initial access in 49% of the FY20 RVAs.

37 Total Number of Assessments

Initial Access

Phishing Link	49%
Exploit Public-Facing Application	11.8%
Phishing Attachment	9.8%

Execution

PowerShell	24.4%
Windows Management Instrumentation	13%
Command & Scripting Interpreter	12.2%

Privilege Escalation

Valid Accounts	37.5%
Exploitation for Privilege Escalation	21.9%
Make & Impersonate Token	15.6%

Defense Evasion

Process Hollowing	18.5%
Mshta	12.3%
Valid Accounts	12.3%

Note: see https://www.cisa.gov/publication/rva for *CISA Analysis: FY2020 Risk and Vulnerability Assessments*, which provides a sample attack path that could compromise an organization that has weaknesses that are representative of those in the FY20 RVAs.

Credential Access

OS Credential Dumping	17%
LLMNR/NBT-NS Poisoning & SMB Rekay	17%
Kerberoasting	13.2%

Discovery

Account Discovery	12.1%
Network Service Scanning	10.9%
File & Directory Discovery	8.1%

Lateral Movement

Pass the Hash	29.8%
Remote Desktop Protocol	25%
Exploitation of Remote Services	11.9%

Collection

Data from Local System	32.2%
Data from Network Shared Drive	30.5%
Screen Capture	22%

Command & Control

Web Protocols	42%
Remote Access Software	15.9%
Standard Application Layer Protocol	8.7%

Exfiltration

Exfiltration Over C2 Channel	68.2%
Archive Collected Data	9.1%
Automated Exfiltration	9.1%

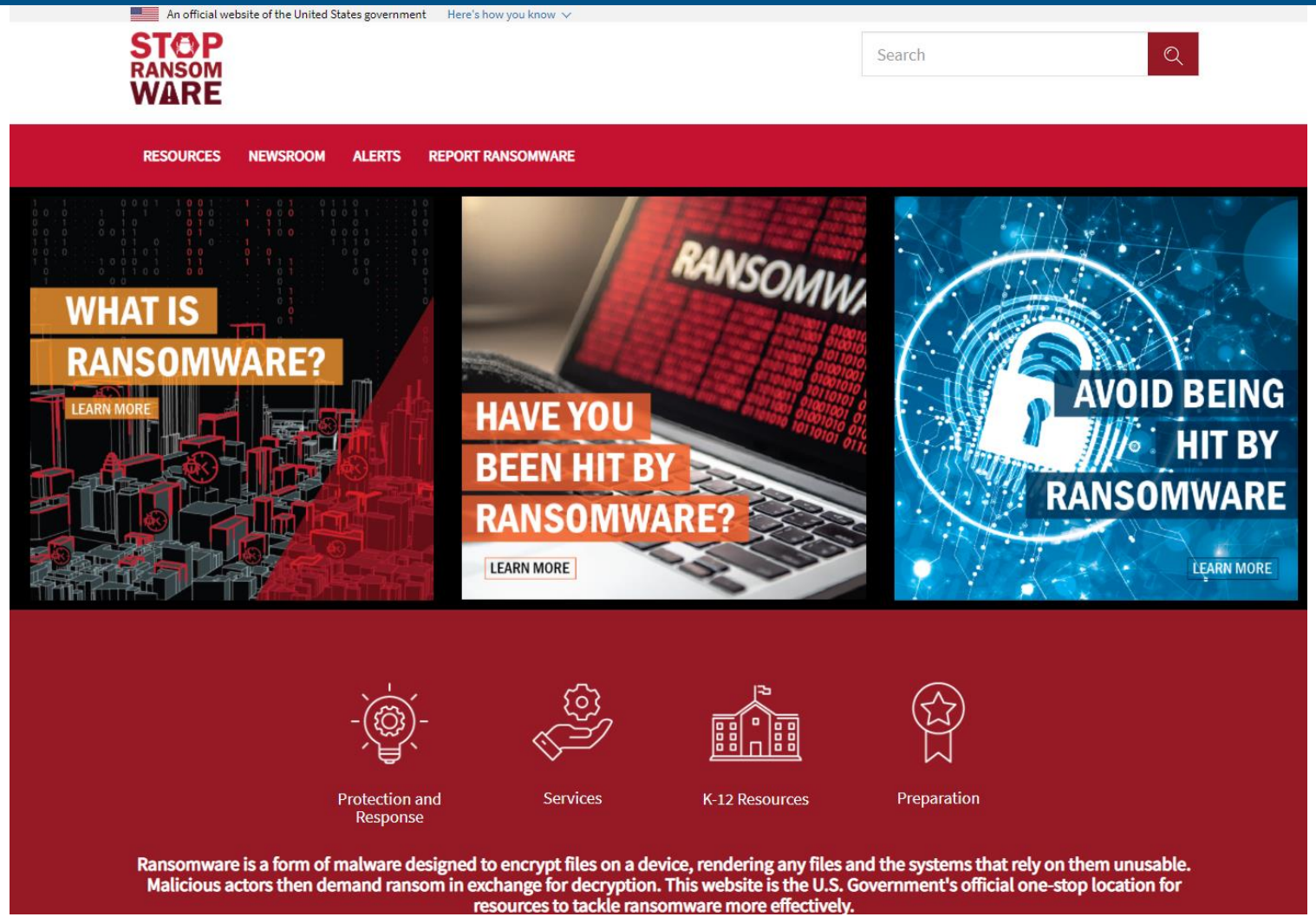
https://www.cisa.gov/publication/rva

*CISA encourages organizations to request the assessment services available on the **CISA Cyber Resource Hub**. The more assessment data CISA can collect, the better the analysis we can share with partners to help them gain visibility into vulnerability trends, adversarial activities and, most importantly, effective mitigations to implement for better protection of their networks.*

This advisory uses the MITRE ATT&CK® v9.0 and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks at https://attack.mitre.org/versions/v9/ for referenced threat actor techniques. For more information about CISA assessment services, please visit https://www.cisa.gov/cyber-resource-hub.

TLP:WHITE

New website: Stopransomware.gov



CISA CYBER+INFRASTRUCTURE

CSET Ransomware Readiness Assessment (RRA)

TLP:WHITE

CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET—applicable to both information technology (IT) and industrial control system (ICS) networks—enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations.

The Ransomware Readiness Assessment (RRA).

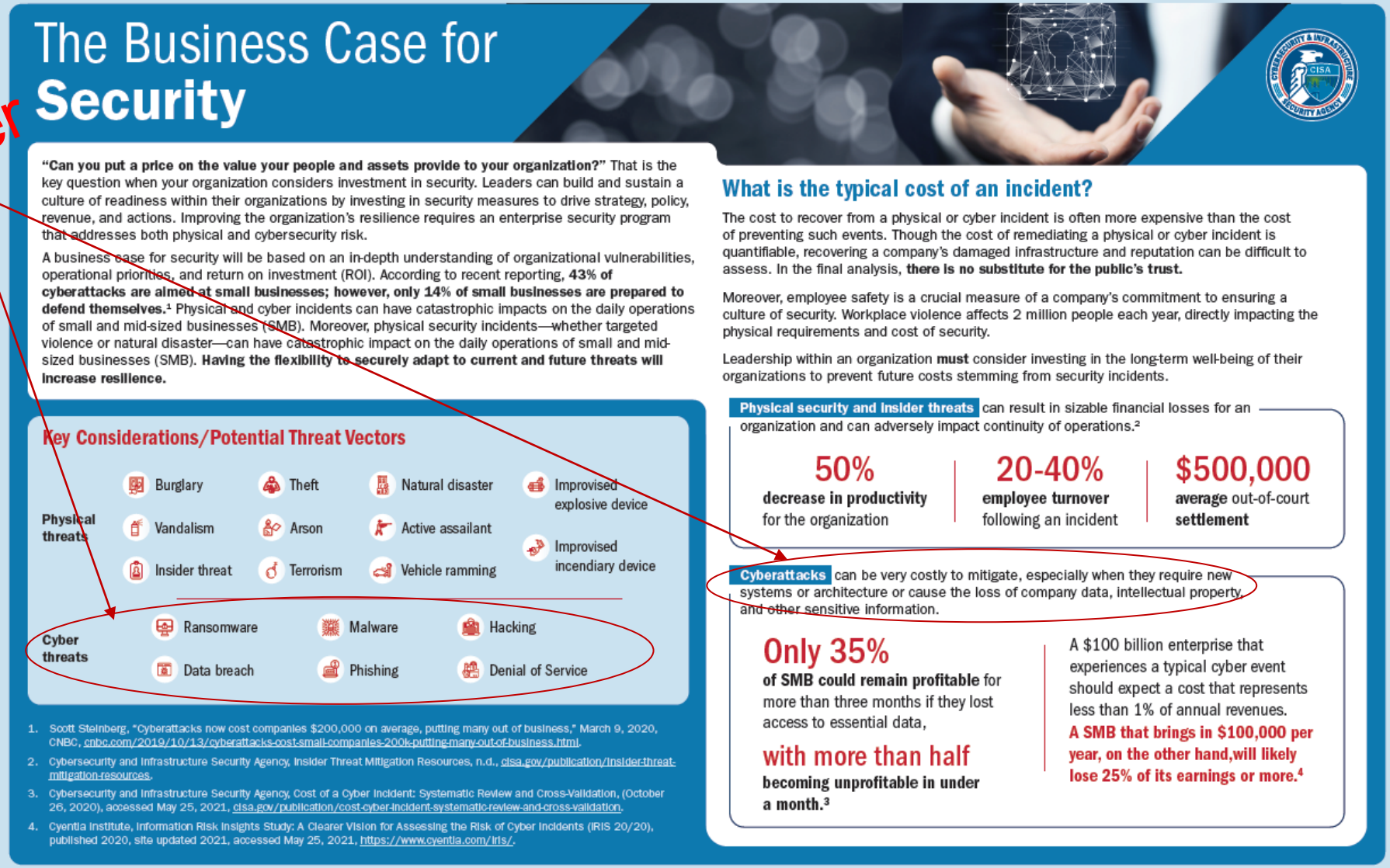
- Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

CISA CYBER+INFRASTRUCTURE

https://github.com/cisagov/cset/releases/tag/v10.3.0.0

Business Case for Security

Cyber



The Business Case for **Security**

"Can you put a price on the value your people and assets provide to your organization?" That is the key question when your organization considers investment in security. Leaders can build and sustain a culture of readiness within their organizations by investing in security measures to drive strategy, policy, revenue, and actions. Improving the organization's resilience requires an enterprise security program that addresses both physical and cybersecurity risk.

A business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment (ROI). According to recent reporting, **43% of cyberattacks are aimed at small businesses; however, only 14% of small businesses are prepared to defend themselves.**[1] Physical and cyber incidents can have catastrophic impacts on the daily operations of small and mid-sized businesses (SMB). Moreover, physical security incidents—whether targeted violence or natural disaster—can have catastrophic impact on the daily operations of small and mid-sized businesses (SMB). **Having the flexibility to securely adapt to current and future threats will increase resilience.**

Key Considerations/Potential Threat Vectors

Physical threats

- Burglary
- Theft
- Natural disaster
- Improvised explosive device
- Vandalism
- Arson
- Active assailant
- Improvised incendiary device
- Insider threat
- Terrorism
- Vehicle ramming

Cyber threats

- Ransomware
- Malware
- Hacking
- Data breach
- Phishing
- Denial of Service

What is the typical cost of an incident?

The cost to recover from a physical or cyber incident is often more expensive than the cost of preventing such events. Though the cost of remediating a physical or cyber incident is quantifiable, recovering a company's damaged infrastructure and reputation can be difficult to assess. In the final analysis, **there is no substitute for the public's trust.**

Moreover, employee safety is a crucial measure of a company's commitment to ensuring a culture of security. Workplace violence affects 2 million people each year, directly impacting the physical requirements and cost of security.

Leadership within an organization **must** consider investing in the long-term well-being of their organizations to prevent future costs stemming from security incidents.

Physical security and insider threats can result in sizable financial losses for an organization and can adversely impact continuity of operations.[2]

- **50%** **decrease in productivity** for the organization
- **20-40%** **employee turnover** following an incident
- **$500,000** **average** out-of-court **settlement**

Cyberattacks can be very costly to mitigate, especially when they require new systems or architecture or cause the loss of company data, intellectual property, and other sensitive information.

- **Only 35%** **of SMB could remain profitable** for more than three months if they lost access to essential data,
- **with more than half** **becoming unprofitable in under a month.**[3]

A $100 billion enterprise that experiences a typical cyber event should expect a cost that represents less than 1% of annual revenues. **A SMB that brings in $100,000 per year, on the other hand,will likely lose 25% of its earnings or more.**[4]

1. Scott Steinberg, "Cyberattacks now cost companies $200,000 on average, putting many out of business," March 9, 2020, CNBC, cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.
2. Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Resources, n.d., cisa.gov/publication/insider-threat-mitigation-resources.
3. Cybersecurity and Infrastructure Security Agency, Cost of a Cyber Incident: Systematic Review and Cross-Validation, (October 26, 2020), accessed May 25, 2021, cisa.gov/publication/cost-cyber-incident-systematic-review-and-cross-validation.
4. Cyentia Institute, Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents (IRIS 20/20), published 2020, site updated 2021, accessed May 25, 2021, https://www.cyentia.com/iris/.

https://www.cisa.gov/publication/business-case-security

Cybersecurity Workforce Training Guide

https://www.cisa.gov/publication/cybersecurity-workforce-training-guide

3 Items to Take Away

1. Ransomware, Information Stealers, and Banking Trojans are still the most likely threat to organizations typically originating as Phishing activity. ***Cyber Awareness Training is where this defense starts!***

2. Continue to focus your efforts around building a Cyber Hygiene organizational culture first then ***build detection and response capacity to identify and contain known malicious activity quickly.***

3. ***Public and Private partnerships absolutely make a difference in this case.*** We have come a long way when it comes to threat information sharing across the cybersecurity community and it is absolutely making a difference in our ability to respond and deter the threat actor. CISA values this partnership and is counting on this community approach to better protect and safeguard the homeland.

CISA Cybersecurity Offerings

TLP:WHITE

LOCAL

CSA Provided Offerings

- **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 Infrastructure Surveys (**C-IST**)
  - Cyber Resilience Reviews (**CRR**)
  - External Dependency Management (**EDM**)
  - Cyber Security Evaluation Tool (**CSET**)

Cybersecurity Advisors (CSA)

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

Protective Security Advisors (PSA)

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

CISA HQ Response Assistance

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

Delivered by CISA Vulnerability Management 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)

* Need (**CRR**) first

CISA CYBER+INFRASTRUCTURE

Report Incidents, Phishing, Malware, or Vulnerabilities

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To submit a report, please select the appropriate method from below:

Incident Reporting Form: report incidents as defined by NIST Special Publication 800-61 Rev 2, to include

- Attempts to gain unauthorized access to a system or its data,
- Unwanted disruption or denial of service, or
- Abuse or misuse of a system or data in violation of policy.

Federal incident notification guidelines, including definitions and reporting timeframes can be found at http://www.us-cert.gov/incident-notification-guidelines.

Share indicators and defensive measures: submit cyber threat indicators and defensive measures with DHS and the Federal Government (includes sharing under the Cybersecurity Information Sharing Act of 2015).

Report phishing: an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques, typically via emails containing links to fraudulent websites.

Report malware: malicious code (e.g., viruses, worms, bots) that disrupts service, steals sensitive information, gains access to private computer systems, etc.

Report software vulnerabilities or ICS vulnerabilities: defects that allow an attacker to violate an explicit (or implicit) security policy to achieve some impact (or consequence). In particular, defects that allow intruders to gain increased levels of access or interfere with the normal operation of systems are vulnerabilities. Insecure configurations, design choices, and changing environmental conditions can also cause vulnerabilities.

Report vulnerabilities in U.S. Government websites: defects that may allow an attacker to violate a security policy to cause some impact or consequence, particularly those vulnerabilities that allow increased levels of access or the ability to interfere with the normal operation of the server or site.

Need CISA's help but don't know where to start? Contact CISA Central

https://us-cert.cisa.gov/report

CISA CYBER+INFRASTRUCTURE

Questions?

Any Questions?

Contact Information

TLP:WHITE

Cybersecurity Advisor
richard.berthao@cisa.dhs.gov
202-839-1429

Protective Security Advisor
bryan.gran@cisa.dhs.gov
202-809-8408

CISA
CYBER+INFRASTRUCTURE

Cyber Security Contacts

Bryan H. Gran
Protective Security Advisor
Connecticut District
Cybersecurity and Infrastructure Security Agency

Email: ***bryan.gran@cisa.dhs.gov***

Phone# 202-809-8408

Richard Berthao
Cybersecurity Advisor for Connecticut
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Email: ***richard.berthao@cisa.dhs.gov***

Mobile# (202) 839-1429

Ron Ford
Cybersecurity Advisor | Region 1 - New England (CT, ME, MA, NH, VT) |
Cybersecurity and Infrastructure Security Agency |U.S. Department of Homeland Security
Email: ***Ron.Ford@cisa.dhs.gov | Phone# (978) 778-8390***

Report a Cyber Issue: https://us-cert.cisa.gov/report or **(888) 282-0870**
CISA Cyber: https://www.cisa.gov/cybersecurity
CISA Resources Hub: https://www.cisa.gov/cyber-essentials

DRINKING WATER SECTION

Webinar # 2021- 14
WEBINAR SERIES

Water Utilities

Certified Water Operators

Environmental Laboratories

09/02/2021

EPA'S INTRODUCTION TO CYBERSECURITY

(VIRTUAL WORKSHOPS)

EPA is offering three different opportunities to participate in this workshop (the same content is repeated). Workshop participation is open to water and wastewater systems, government officials, and others involved in water sector cybersecurity. Continuing education credits have been applied for in all 50 states. Participants must attend both days in full to receive the credits. Workshop dates and registration links are listed below.

Workshop Dates, Times, and Registration Links:

- **September 15th (1:00-4:30 pm EST) & September 16th (1:00-5:00 pm EST)**
  Registration Link: https://us02web.zoom.us/meeting/register/tZYlceGoqzMrG9cnIe7rS-dGWrCCY7hwa1rA

- **October 13th (1:00-4:30 pm EST) & October 14th (1:00-5:00 pm EST)**
  Registration Link: https://us02web.zoom.us/meeting/register/tZIuf-isrj0iHNwVAmh_ovAPmR6aXnMul4Tp

- **November 3rd (1:00-4:30 pm EST) & November 4th (1:00-5:00 pm EST)**
  Registration Link: https://us02web.zoom.us/meeting/register/tZctcu2srTwpE90p1Fexz7JZmZF-vJO5jX4F

Contaminants and Drinking Water Quality

PFAS

State Budget allocations

Federal infrastructure bill includes money to address emerging contaminants in drinking water with an emphasis on PFAS

Any questions, please contact:
Pat Bisacky || Email: *patricia.bisacky@ct.gov*

Operator Certification Program

Operator Certification Program – dph.opcert@ct.gov

Bill Sullivan	Kevin Veilleux
Phone# 860-936-1266	*Phone# 860-937-7735*

Certification Examinations:

- CT DPH Operator Certification Examination, Applications and Reference Material List
- **Circular letter 2021-14**: Computer Based Exams at Test Centers

COVID-19 Suspension of Certification Renewal:

- Operators, whose renewal requirement has been suspended, should prepare to renew their certification
- Operators who are ready to renew, may request their renewal application
  – send email to dph.opcert@ct.gov
- While the period for renewal may have been extended your next period will be shortened by an equivalent amount,
- www.elicense.ct.gov (without password, click "**Online Services**" click "**Lookup a License**")

Approved Water Operator Training:

- Distance Education (Correspondence, Online, Live Internet Instructor Lead Courses)

Reported Water Treatment Chemical Shortage: Draft Circular Letter, Instructions for Reporting

Environmental Labs Certification Program

Drinking Water Technical Assistance Documents

40 CFR Part 141: Electronic Code of Federal Regulations (eCFR)

Code of Federal Regulations pertaining to the National Primary Drinking Water Regulations

EPA drinking water website:

Certification of Laboratories that Analyze Drinking Water Samples to Ensure Compliance with Regulations | US EPA

- ***Manual for the Certification of Laboratories Analyzing Drinking Water fifth addition.*** **Technical information for laboratories analyzing drinking water compliance samples.**
- **Approved drinking analytical methods-Pdfs of the approved methods along with links to the published method and links to technical notes.**

Dawn Shaban
Email: *Dawn.Shaban@ct.gov*
Phone 860-488-0652

Shinu Zachariah
Email: *Shinu.zachariah@ct.gov*
Phone 860-936-1678

Tracking per State Drought Plan

DRINKING WATER SECTION

Webinar # 2021- 14
WEBINAR SERIES

Water Utilities

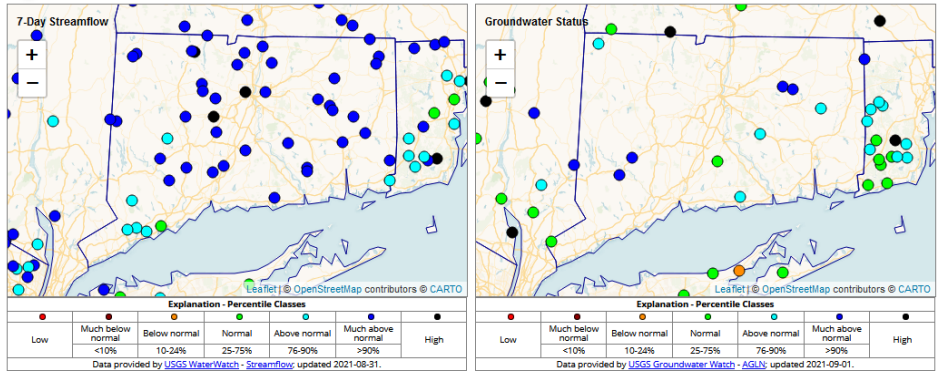
Certified Water Operators

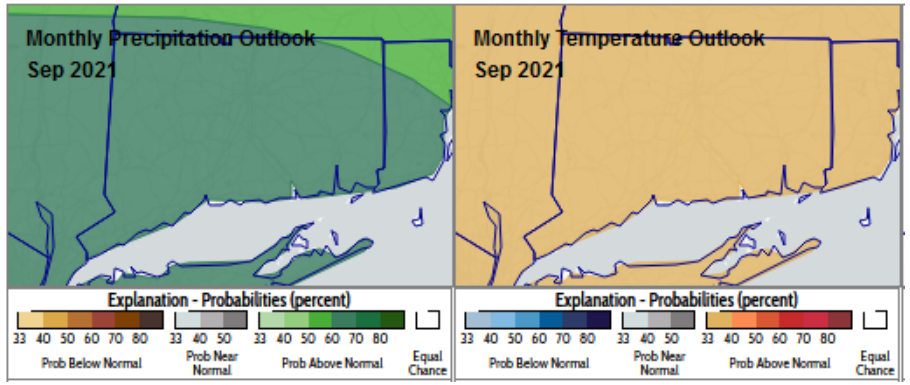
Environmental Laboratories

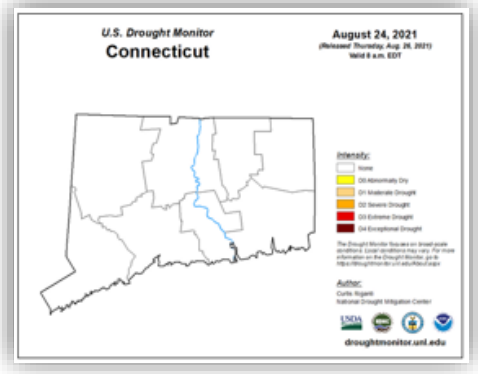
09/02/2021

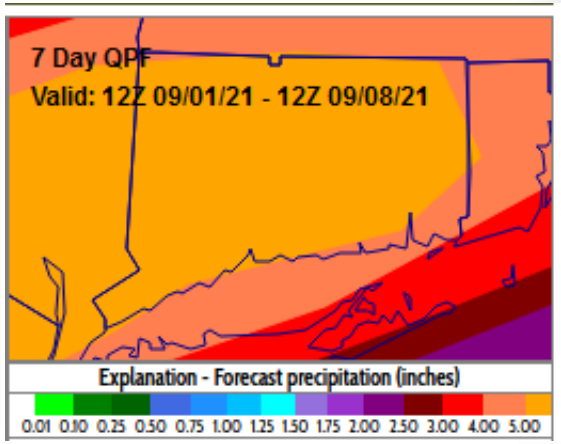
❖ Statewide:

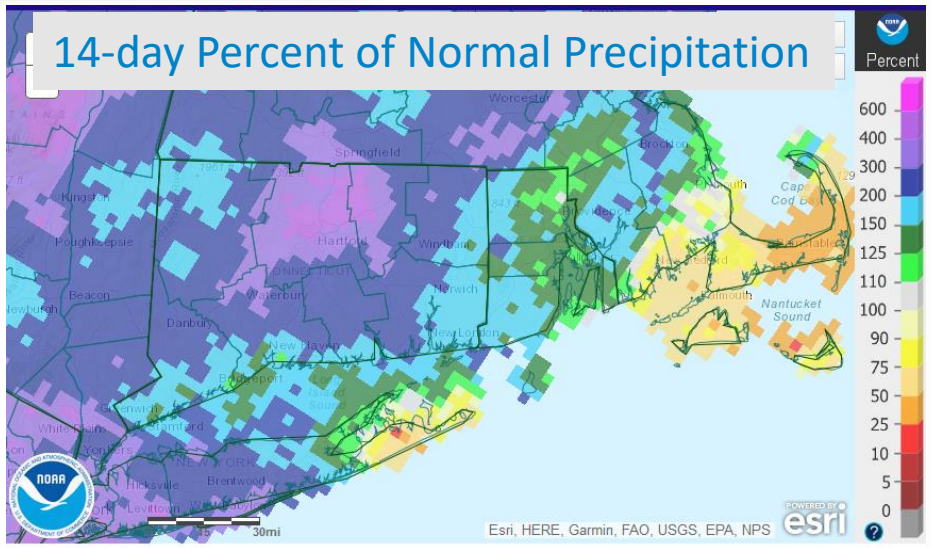
>= 100% of Normal n=34	State Average	Average Percent of Normal
34	93.0% ⬇	109.9% ⬇
Change since last week: --	Last week: 93.7%	Last week: 110.7%











Any questions, please contact: **Steven Harkey || Email: Steven.Harkey@ct.gov**

DRINKING WATER SECTION

Webinar # 2021- 14
WEBINAR SERIES

Water Utilities

Certified Water Operators

Environmental Laboratories

09/02/2021

Free 2 Day Virtual Drought Workshop

For more info and registration see:
Circular Letters
2021-65 & 2021-66

DROUGHT RESPONSE AND WATER LOSS WORKSHOP FOR WATER UTILITIES

Attention:
SMALL WATER UTILITIES

3-Hour Webinar • Wednesday, September 22, 2021

This workshop will include:

- Overview of **US Drought Monitor Map** and how it relates to water systems
- Introduction to EPA's **Drought Response and Recovery**: A Basic Guide for Water Utilities
- Introduction for **creating a drought response plan**
- Introduction to **water loss control resources**

0.30 CEUs will be available for participation

Attention:
MEDIUM & LARGE WATER UTILITIES

3.5-Hour Webinar • Thursday, September 23, 2021

This workshop will include:

- Overview of **US Drought Monitor Map** and how it relates to water systems
- Introduction to the **CT State Water Plan**
- Examples of **conservation strategies** utilities are using
- **Lessons learned** illustrating drought response strategies implemented by CT water Utilities
- Water loss, **water loss management** and water audit basics

0.35 CEUs will be available for participation

Registration info can be found at:
https://www.drought.gov/states/connecticut

Any questions, please contact: **Steven Harkey || Email: Steven.Harkey@ct.gov**

DWSRF Update

- **Public hearing on DWSRF Draft Intended Use Plan (IUP) for SFY 2022 was held on August 18 and DPH is currently preparing the Hearing Report**
- **The Infrastructure Investment and Jobs Act (IIJA) passed through the Senate and is currently with the House of Representatives for a vote no later than September 27, 2021. Current national DWSRF provisions include:**
  - $11.7 billion over the next 5 years for any eligible project
  - $15 billion for lead service line replacements
  - $4 billion for emerging contaminants with a focus of PFAS/PFOA
  - Reauthorization annual appropriations for the DWSRF at levels between $2.4 - $3.25 billion annually from 2022 – 2025 (4 years)

Key Provisions (IIJA)

- Funding is intended to be “in addition to” annual appropriations.
- Funding is available “until expended.”
- No state match is required for supplemental appropriations.
- The bill requires 100% of the capitalization grant for emerging contaminants be used for additional subsidy.
- The bill requires “not less than 50%” of the annual capitalization grant for any eligible project and lead service line replacement be used for additional subsidy. Up to 100% of the capitalization grant may be used for additional subsidy.

Drinking Water Needs Survey and Assessment (DWINSA)

- **The DWINSA determines:**
  - 20-year capital need for drinking water infrastructure investment (nationally & for CT)
  - Results determine Connecticut's DWSRF funding amount
  - More documented need = more $$$ in the DWSRF – which would increase funding for loans, subsidy, funding that support staff providing technical assistance to pws' & certified operators, contracts for technical assistance providers etc.
- **23 PWS' are included in the current DWINSA**
- **Coming to a close December 10, 2021**
- **Thank you for your continued support and participation!**

WUCC Implementation

Water Utility Coordinating Committee Implementation Meeting

September 15, 2021, 1:00-3:00

Location: Virtual via Microsoft Teams
Join on your computer or mobile app

Click here to join the meeting

or email **dph.wucc@ct.gov** for assistance

- Discussion Topics:
  - Development Check List for Municipalities and WUCC Pathway
  - Conservation / Drought
  - Facilitating Water Main Extensions to Serve Developments
  - Small Water System/Non-Community Standards
  - Interconnections

- All are welcome to join the discussion!

UPDATES

- PURA
- CTWC
- Aquarion
- RWA
- MDC
- Others (Torrington, Bristol, etc..)

Requesting to raise your hand from GotoWebinar Control Panel

Suggestions

- **Next webinar is on Thursday October 7, 2021 at 1 pm.**

September
October 7, 2021 **1 PM – 2 PM**

- **Email questions/notifications about water quality testing and monitoring to dwdcompliance@ct.gov**

- **Emergency notifications, may call 860-692-2333 and email to dwdcompliance@ct.gov**

Public Water System, Certified Water Operators and Environmental Laboratories

Thank You

DRINKING WATER SECTION
Webinar 2021-14

Keeping Connecticut Healthy
DPH
Connecticut Department of Public Health

CONNECTICUT DEPARTMENT *of* PUBLIC HEALTH

Accredited Health Department
PHAB
Advancing public health performance
Public Health Accreditation Board