TRC

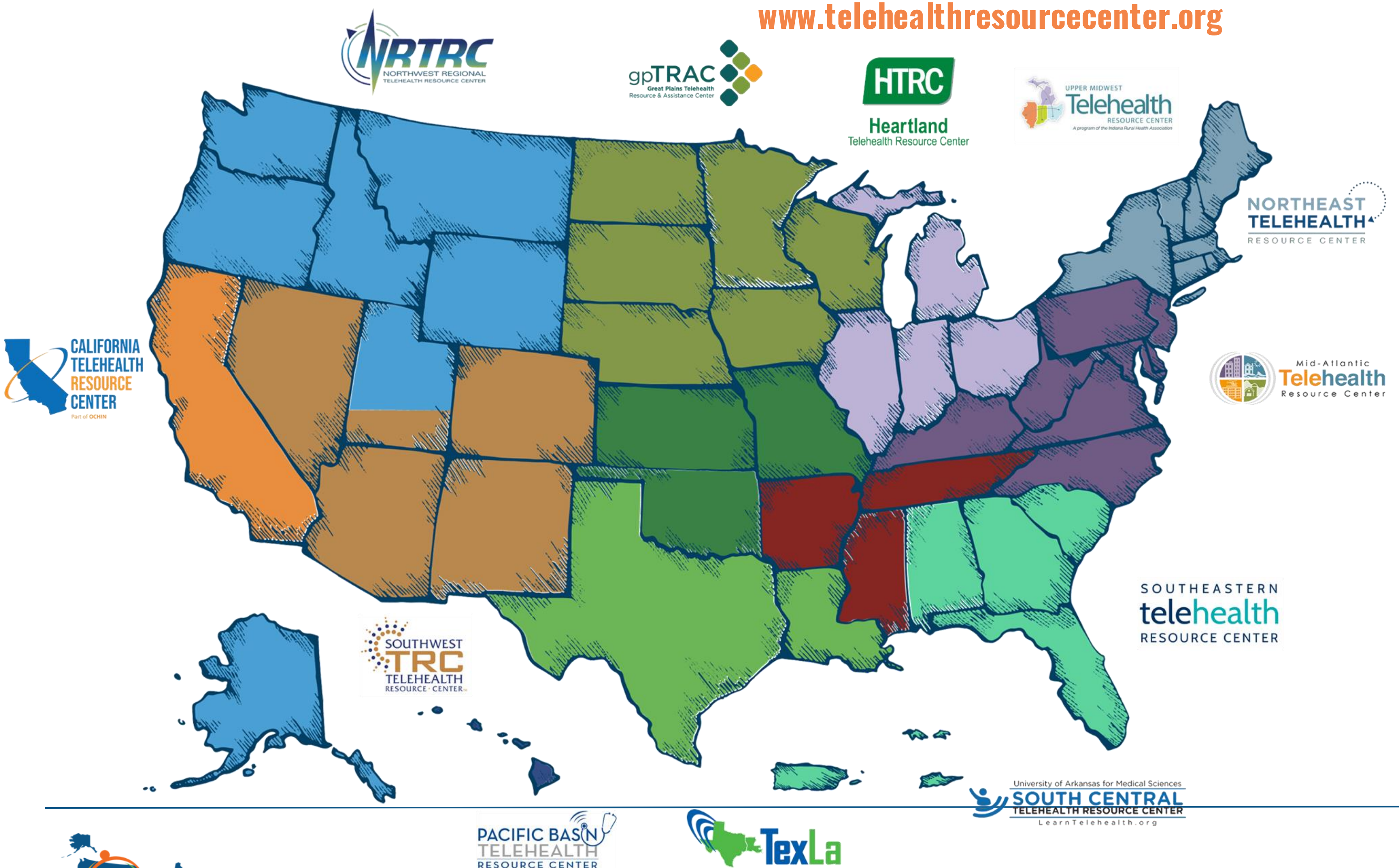
NATIONAL CONSORTIUM OF
TELEHEALTH
RESOURCE CENTERS

CISA Services: Federal Cybersecurity Resources for Telehealth

November 14, 2024

HRSA Funded Telehealth Resource Centers

www.telehealthresourcecenter.org


NRTRC
NORTHWEST REGIONAL TELEHEALTH RESOURCE CENTER
gpTRAC
Great Plains Telehealth Resource & Assistance Center
HTRC
Heartland Telehealth Resource Center
UPPER MIDWEST Telehealth RESOURCE CENTER
A program of the Indiana Rural Health Association
NORTHEAST TELEHEALTH RESOURCE CENTER
Mid-Atlantic Telehealth Resource Center
CALIFORNIA TELEHEALTH RESOURCE CENTER
Part of OCHIN
SOUTHEASTERN telehealth RESOURCE CENTER
SOUTHWEST TRC TELEHEALTH RESOURCE CENTER
University of Arkansas for Medical Sciences
SOUTH CENTRAL TELEHEALTH RESOURCE CENTER
LearnTelehealth.org
PACIFIC BASIN TELEHEALTH RESOURCE CENTER
THE UNIVERSITY OF HAWAI'I AT MĀNOA
TexLa
Telehealth Resource Center

NRTRC	gpTRAC	NETRC
CTRC	HTRC	UMTRC
SWTRC	SCTRC	MATRC
PBTRC	TexLa	SETRC

12 REGIONAL RESOURCE CENTERS

TTAC TelehealthTechnology.org CCHP

2 NATIONAL RESOURCE CENTERS

TRC NATIONAL CONSORTIUM OF TELEHEALTH RESOURCE CENTERS

Webinar Tips and Notes

- Your phone &/or computer microphone has been muted.
- If we do not reach your question, please contact your regional TRC. There may be delays in response time: https://telehealthresourcecenter.org/contact-us/
- Please fill out the post-webinar survey.
- Closed Captioning is available.
- Please submit your questions using the Q&A function.
- The webinar is being **recorded**.
- Recordings will be posted to our YouTube Channel:

  https://www.youtube.com/c/nctrc

CISA/HHS CYBERSECURITY TOOLKIT

Travis Light
CISA Cybersecurity Advisor

Bob Bastani
HHS ASPR Senior Cyber Security Advisor

CISA | CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Today’s Roadmap

- **Intro to CISA & HHS ASPR**
- Threat Environment
- Joint Cybersecurity Toolkit
- HHS Cyber Performance Goals
- Additional Resources

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.

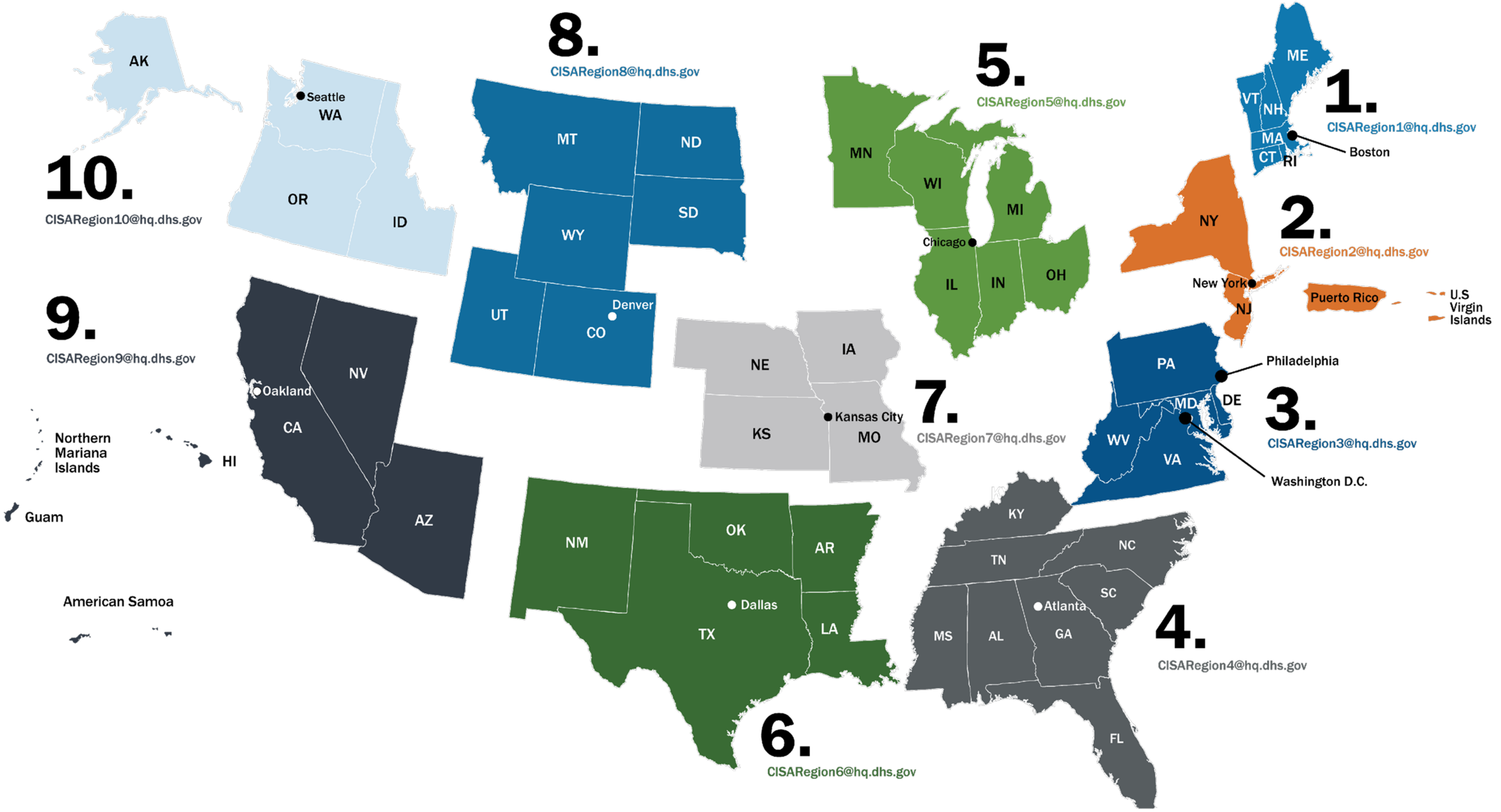
CISA's Core Capabilities

AT A GLANCE

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

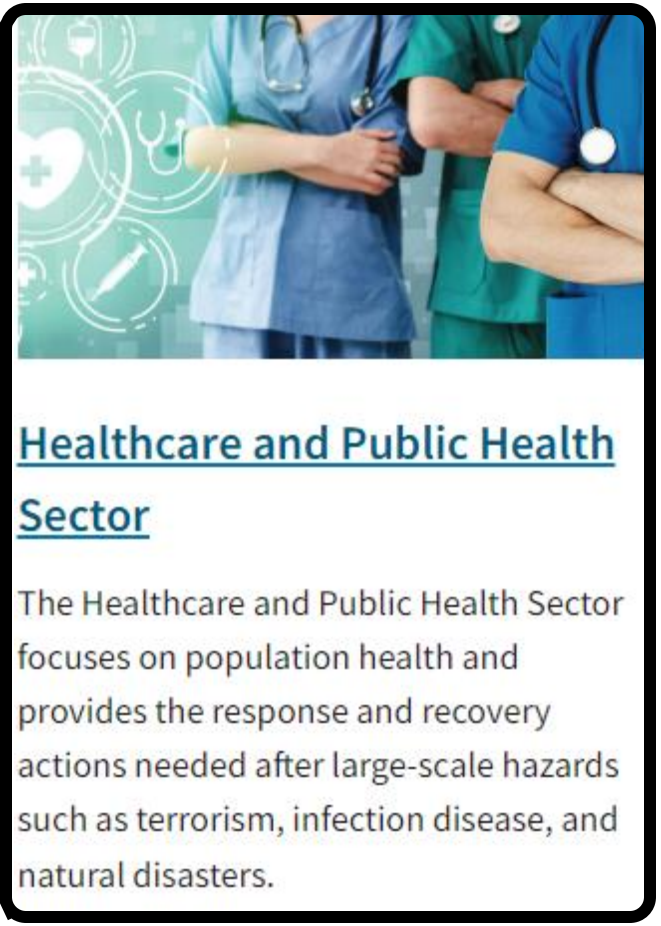
CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

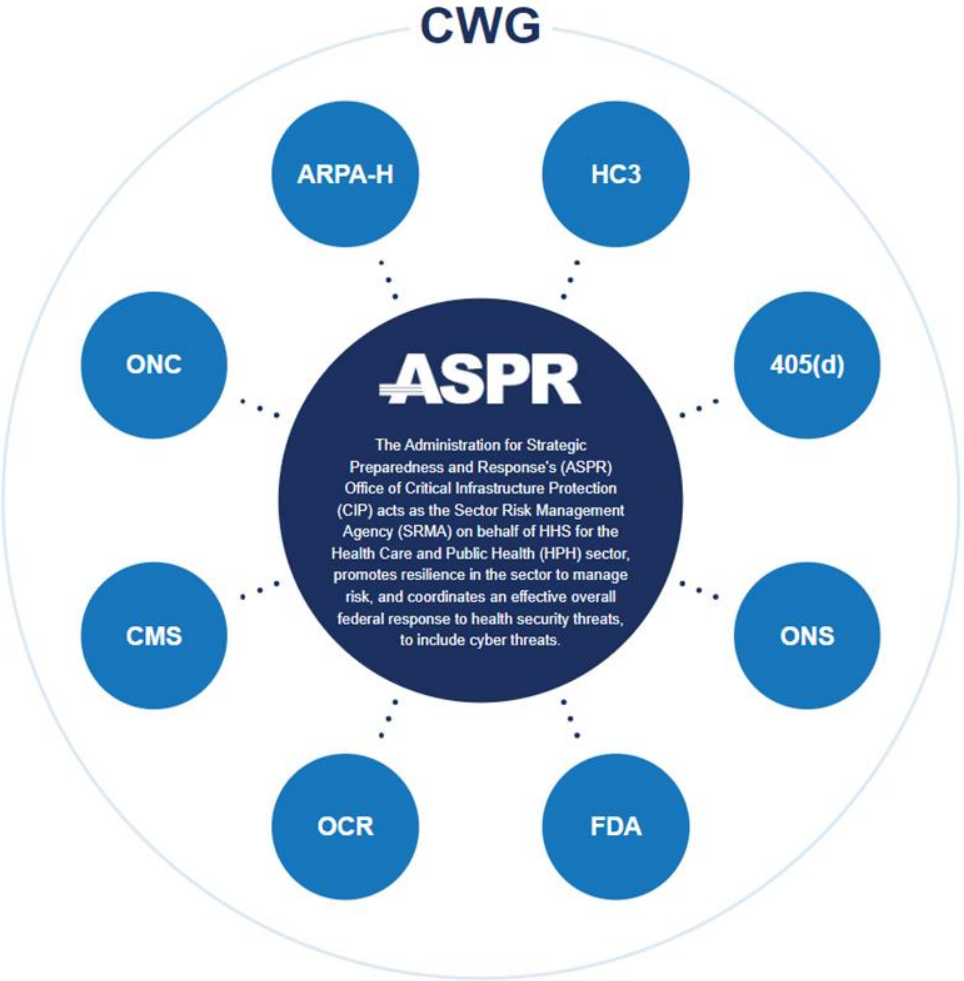
CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	DHS & GSA
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA



Healthcare and Public Health Sector

The Healthcare and Public Health Sector focuses on population health and provides the response and recovery actions needed after large-scale hazards such as terrorism, infection disease, and natural disasters.

ASPR serves as the HHS “One-Stop-Shop” for Healthcare and Public Health cybersecurity



CWG

ARPA-H

HC3

ONC

405(d)

ASPR

The Administration for Strategic Preparedness and Response's (ASPR) Office of Critical Infrastructure Protection (CIP) acts as the Sector Risk Management Agency (SRMA) on behalf of HHS for the Health Care and Public Health (HPH) sector, promotes resilience in the sector to manage risk, and coordinates an effective overall federal response to health security threats, to include cyber threats.

CMS

ONS

OCR

FDA

- Strengthen cyber preparedness
- Improve cyber resilience
- Protect patient information and safety

Health Sector Coordinating Council

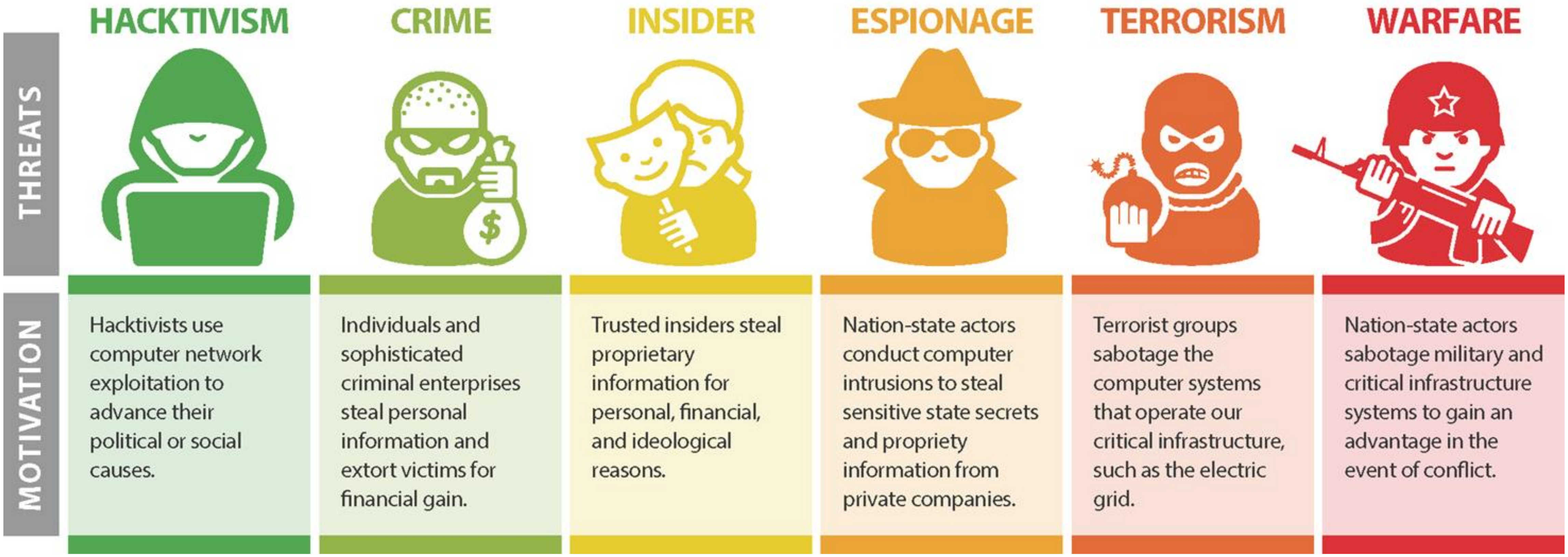
Healthcare Sector
Coordinating Council
Cybersecurity Working Group

- Industry Council of 400+ healthcare providers, pharmaceutical and medtech companies, payers and health IT entities
- Partnered with Federal Government
- HHS 405(d) Program Task Group

Today’s Roadmap

- Intro to CISA & HHS ASPR
- **Threat Environment**
- Joint Cybersecurity Toolkit
- HHS Cyber Performance Goals
- Additional Resources

Threat Actors and Motivation



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Threat Categories

Cyber Threats

Social engineering

Ransomware attacks

Loss or theft of equipment or data

Insider, accidental or malicious data loss

Attacks against network connected medical devices that may affect patient safety

YOUR FILES ARE ENCRYPTED!

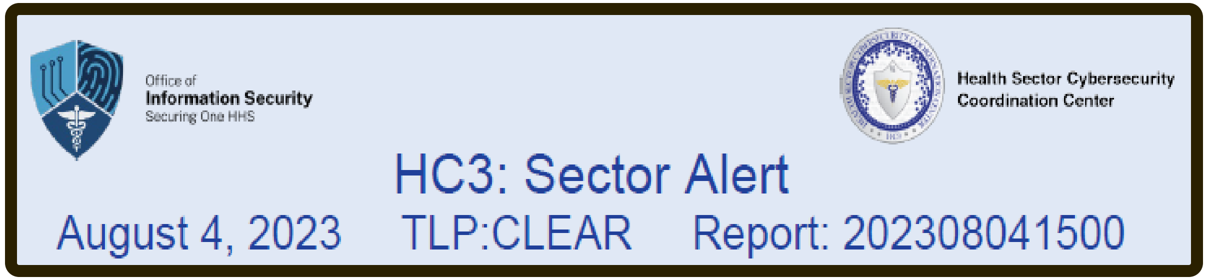
Threat Actors Can Use AI Too

- **Social Engineering:** GPT-crafted phishing emails; deepfaked calls and videos
- **AI-powered Malware**: Lower barriers to entry; autonomous zero-day attacks
- **Supply Chain Attacks**: Compromise the AI services you rely on or use AI to attack those services
- **AI Poisoning:** Deliberate and malicious contamination of the data that trains your AI systems, leading to incorrect or even harmful responses

The Threat is Real – Prospect Holdings

Prospect Medical Holdings

- 16 Hospitals / 160+ Clinics
- Emergency rooms closed
- Ambulances diverted
- Reverted to manual processes for medical records, labs, & radiology
- 500,000 patient records claimed stolen
- **On sale for 50 Bitcoin! ($1.3M)**

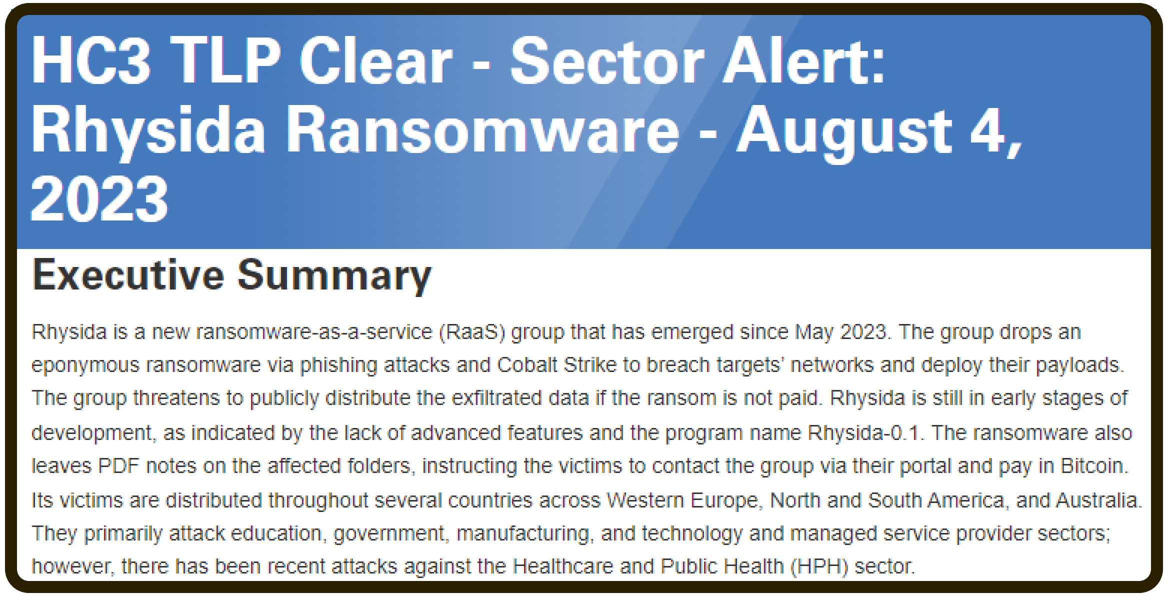


Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500



HC3 TLP Clear - Sector Alert: Rhysida Ransomware - August 4, 2023

Executive Summary

Rhysida is a new ransomware-as-a-service (RaaS) group that has emerged since May 2023. The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads. The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin. Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia. They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector.

The Threat is Real – Change Health

Change Healthcare

- UnitedHealth Group
- Processes ~14B claims each year
- Relief programs established by UnitedHealth and HHS
- Potential ransom of $22M
- “Significant portion” of US citizens’ data compromised

NEWS | April 11, 2024

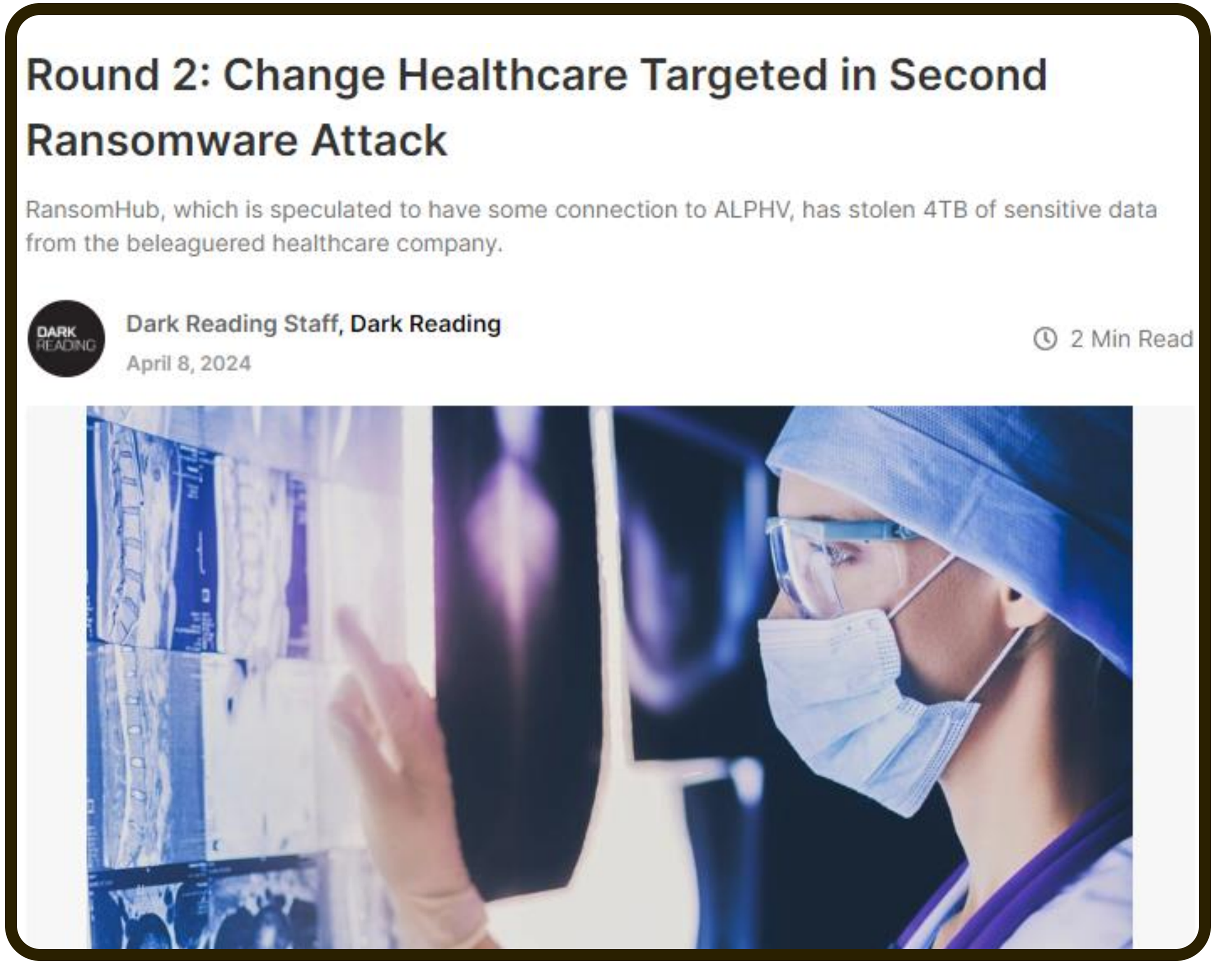
Military Pharmacies Restored to Full Operations After Change Healthcare Cyberattack

By TRICARE Communications

The Threat is Real – Supply Chain

Change Healthcare - Round 2

- 4TB of data exfiltrated
- **Different threat actor**
  - 1st was ALPHV/Blackcat
  - 2nd was RansomHub



Round 2: Change Healthcare Targeted in Second Ransomware Attack

RansomHub, which is speculated to have some connection to ALPHV, has stolen 4TB of sensitive data from the beleaguered healthcare company.

Dark Reading Staff, Dark Reading

April 8, 2024

2 Min Read

CISA/HHS Cybersecurity Roundtable

"Given that healthcare organizations have a combination of personally identifiable information, financial information, health records, and countless medical devices, they are essentially a one-stop shop for an adversary."

- CISA Deputy Director Nitin Natarajan

CISA/HHS Cybersecurity Roundtable

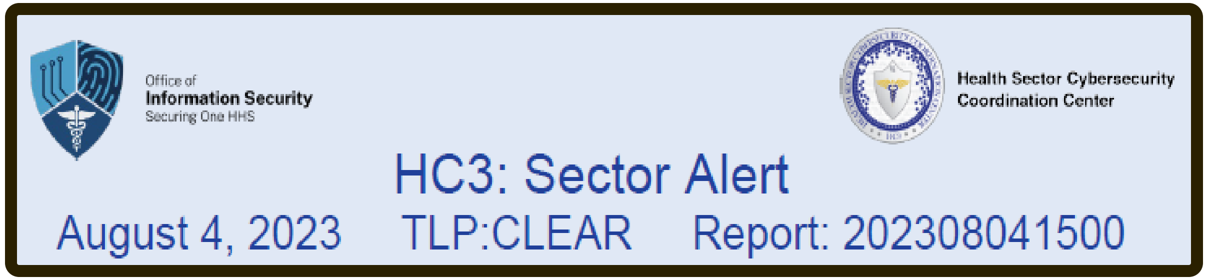
"We have seen a significant rise in the number and severity of cyber attacks against hospitals and health systems in the last few years. ***These attacks expose vulnerabilities in our healthcare system****,* ***degrade patient trust, and ultimately endanger patient safety****.*

- HHS Deputy Secretary Andrea Palm

The Threat is Real – Prospect Holdings

Prospect Medical Holdings

- 16 Hospitals / 160+ Clinics
- Emergency rooms closed
- Ambulances diverted
- Reverted to manual processes for medical records, labs, & radiology
- 500,000 patient records claimed stolen
- **On sale for 50 Bitcoin! ($1.3M)**

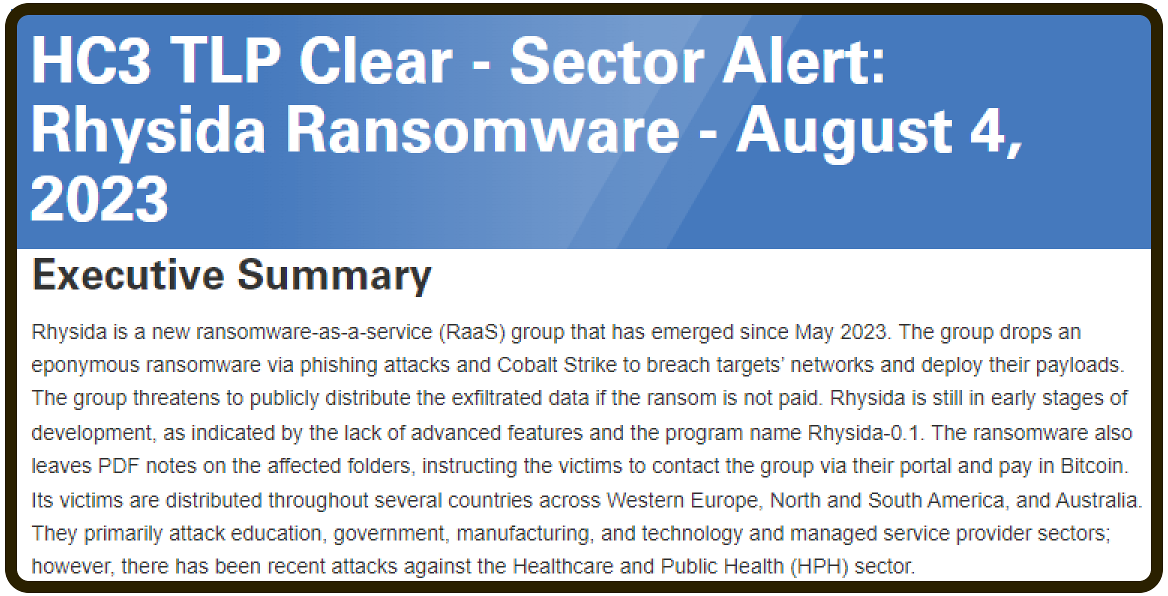


Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500



HC3 TLP Clear - Sector Alert: Rhysida Ransomware - August 4, 2023

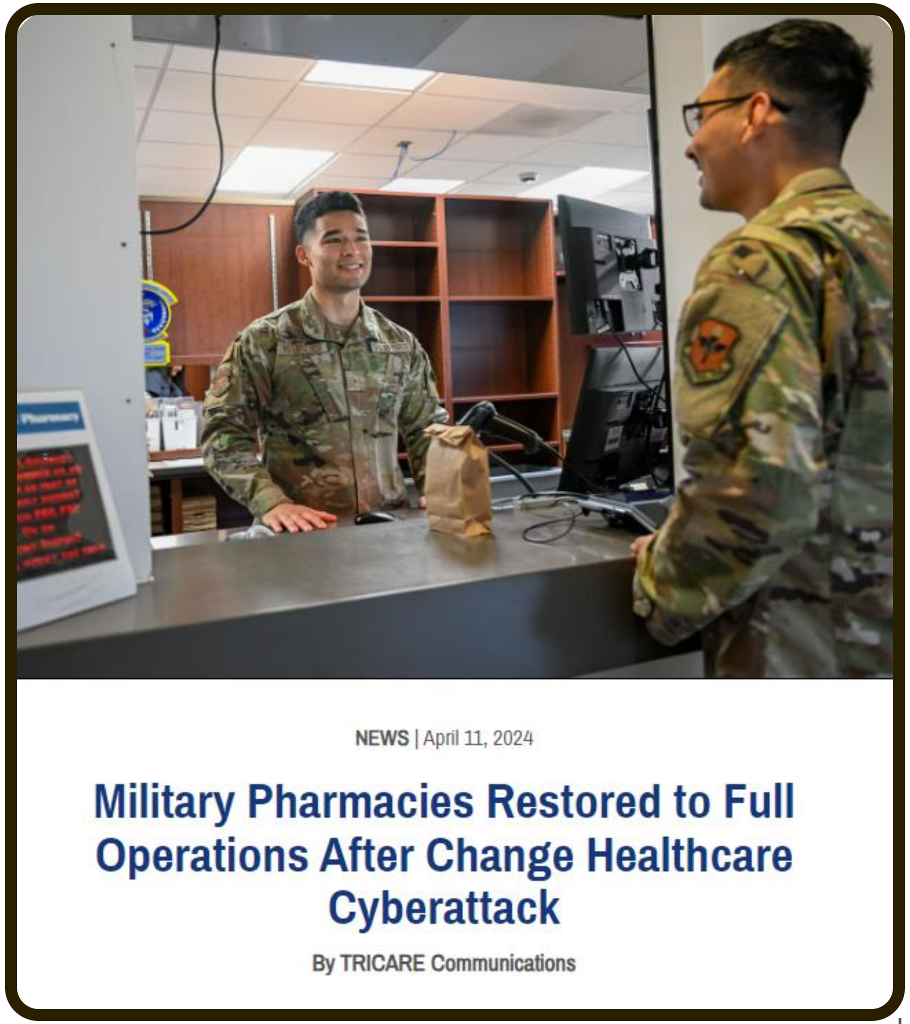
Executive Summary

Rhysida is a new ransomware-as-a-service (RaaS) group that has emerged since May 2023. The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads. The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin. Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia. They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector.

The Threat is Real – Change Health

Change Healthcare

- UnitedHealth Group
- Processes ~14B claims each year
- Relief programs established by UnitedHealth and HHS
- Potential ransom of $22M
- “Significant portion” of US citizens’ data compromised



NEWS | April 11, 2024

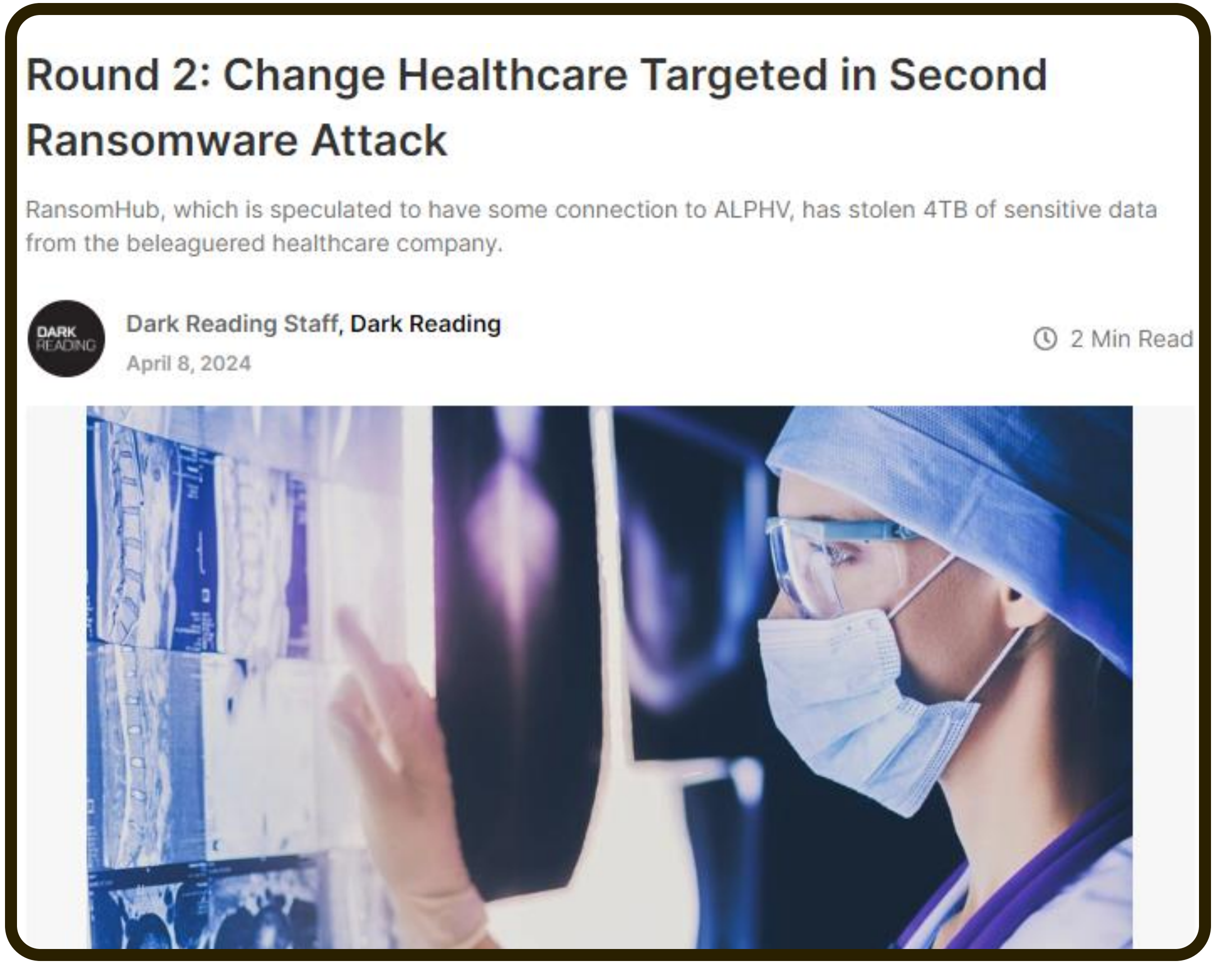
Military Pharmacies Restored to Full Operations After Change Healthcare Cyberattack

By TRICARE Communications

The Threat is Real – Supply Chain

Change Healthcare - Round 2

- 4TB of data exfiltrated
- **Different threat actor**
  - 1st was ALPHV/Blackcat
  - 2nd was RansomHub



Round 2: Change Healthcare Targeted in Second Ransomware Attack

RansomHub, which is speculated to have some connection to ALPHV, has stolen 4TB of sensitive data from the beleaguered healthcare company.

Dark Reading Staff, **Dark Reading**
April 8, 2024

2 Min Read

Today’s Roadmap

- Intro to CISA & HHS ASPR
- Threat Environment
- **Joint Cybersecurity Toolkit**
- HHS Cyber Performance Goals
- Additional Resources

CISA/HHS Cybersecurity Toolkit

Consolidates CISA and HHS resources such as:

- Cyber Performance Goals for Healthcare
- CISA's Free Cybersecurity Services & Tools
- Alerts & Advisories
- Training & Exercises
- Incident Response Guides

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEPARTMENT OF HEALTH & HUMAN SERVICES·USA
Healthcare and Public Health Cybersecurity

Link to CISA/HHS Toolkit

CISA/HHS: Resiliency Landscape Analysis

Healthcare & Public Health Sector Coordinating Council

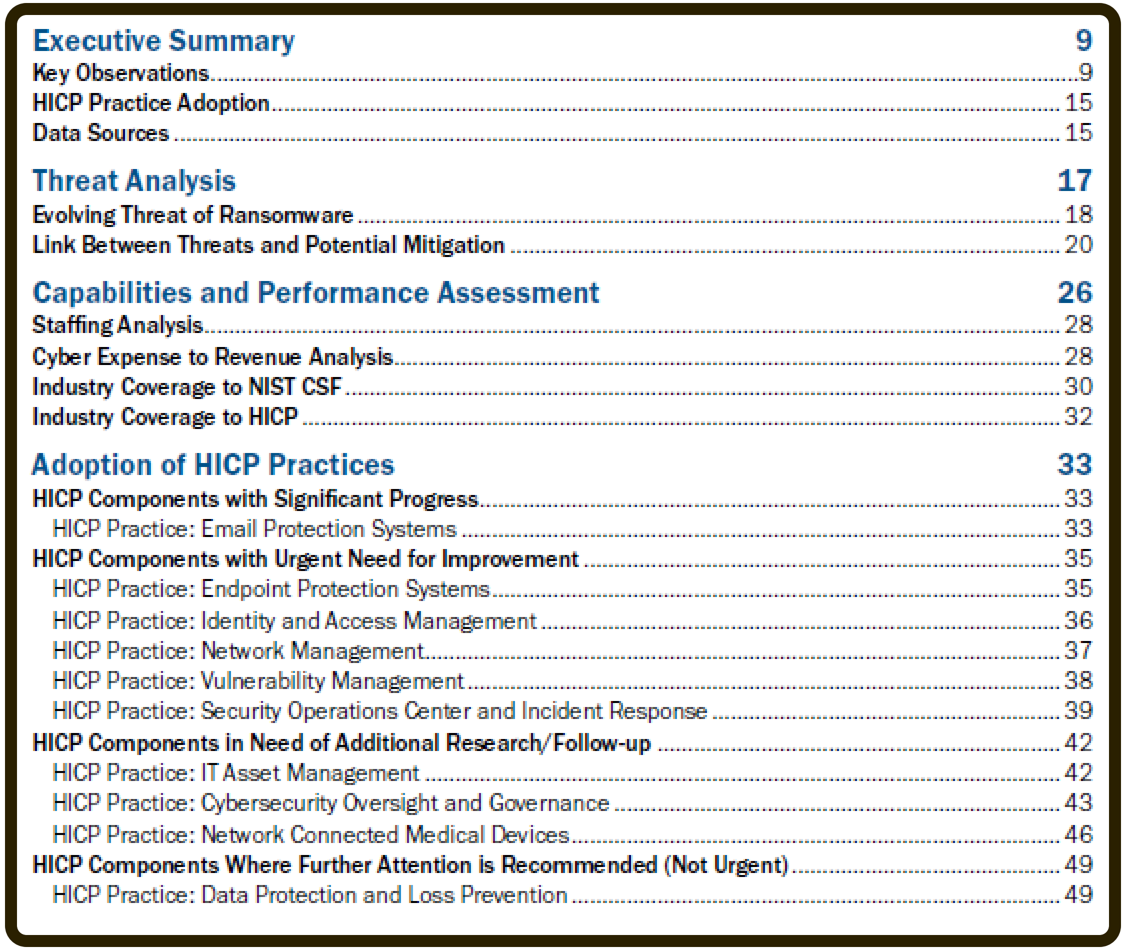
PUBLIC PRIVATE PARTNERSHIP

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES

HHS 405(d) Aligning Health Care Industry Security Approaches

Hospital Cyber Resiliency Initiative

Landscape Analysis

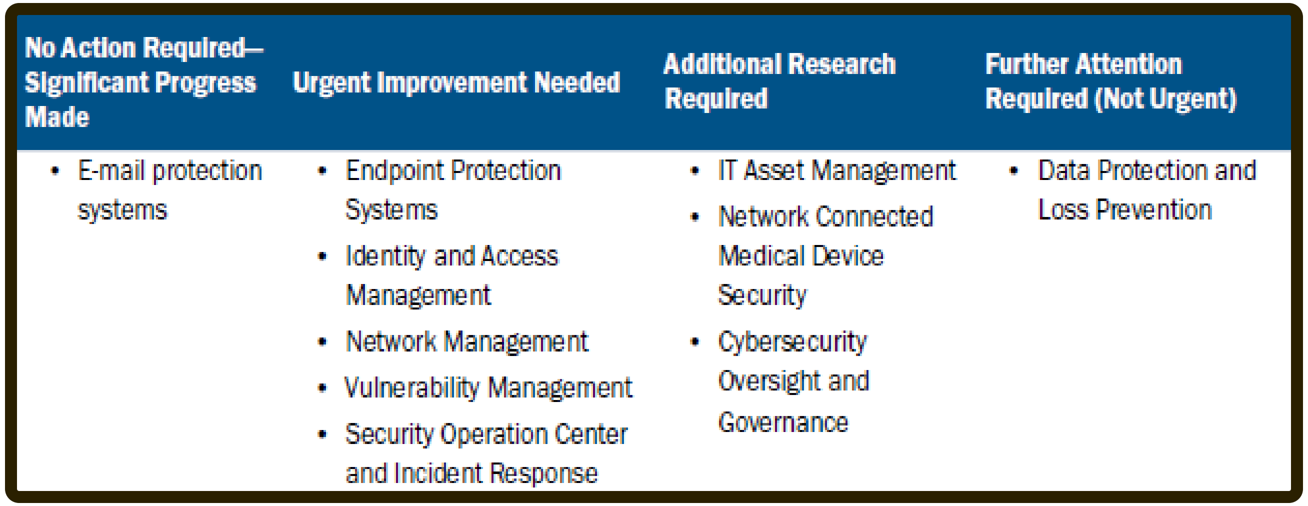


Link to CISA/HHS Toolkit

CISA/HHS: Resiliency Landscape Analysis

Key Findings

1) Growing threat of ransomware
2) Variable adoption of critical security features
    1) MFA
    2) Vulnerability Assessments
    3) Training & Outreach
    4) Hospital-at-Home
3) ✓ Email protections are way up!
4) Supply chain risk is pervasive
5) Medical devices generally aren’t targeted



No Action Required—Significant Progress Made	Urgent Improvement Needed	Additional Research Required	Further Attention Required (Not Urgent)
• E-mail protection systems	• Endpoint Protection Systems • Identity and Access Management • Network Management • Vulnerability Management • Security Operation Center and Incident Response	• IT Asset Management • Network Connected Medical Device Security • Cybersecurity Oversight and Governance	• Data Protection and Loss Prevention

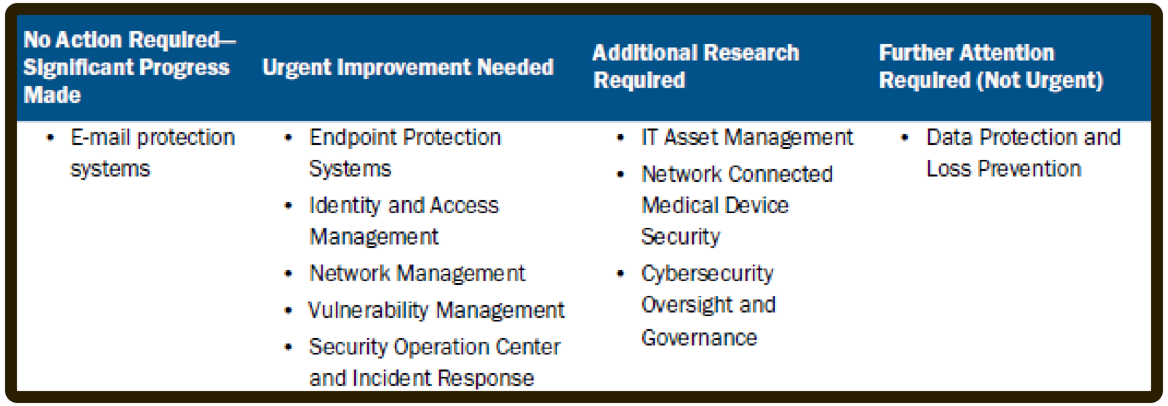
Link to CISA/HHS Toolkit

CISA/HHS: Resiliency Landscape Analysis

Key Findings

6) Inconsistency across health orgs
7) Use of antiquated hardware, software, and systems
8) Insurance premiums continue to rise
9) Recruiting and retaining cyber talent is a challenge

✓10) **Adopting Health Industry Cybersecurity Practices works!**



No Action Required—Significant Progress Made	Urgent Improvement Needed	Additional Research Required	Further Attention Required (Not Urgent)
• E-mail protection systems	• Endpoint Protection Systems • Identity and Access Management • Network Management • Vulnerability Management • Security Operation Center and Incident Response	• IT Asset Management • Network Connected Medical Device Security • Cybersecurity Oversight and Governance	• Data Protection and Loss Prevention

Link to CISA/HHS Toolkit

Today’s Roadmap

- Intro to CISA & HHS ASPR
- Threat Environment
- Joint Cybersecurity Toolkit
- **HHS Cyber Performance Goals**
- Additional Resources

Cyber Performance Goals - Healthcare

Cyber Performance Goals (CPGs) Assessment:

- Voluntary guidelines tailored to Healthcare organizations

10 <u>Essential</u> Goals establish a floor of safeguards that will better protect from cyber attacks, improve response when events occur, and minimize residual risk

10 <u>Enhanced</u> Goals provide a path to reach the next level of defense needed to protect against additional attack vectors

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

HEALTHCARE AND PUBLIC HEALTH SECTOR-SPECIFIC

CYBERSECURITY PERFORMANCE GOALS

Link to HHS CPGs

Why Cybersecurity Performance Goals (CPGs) now?

Based on industry-specific analysis, the CPGs set a floor for cybersecurity expectations for all healthcare and public health organizations, no matter their size or cyber maturity. The CPGs map directly to existing cybersecurity frameworks, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Healthcare Industry Cybersecurity Practices (HICP), and the National Cybersecurity Strategy.

Increasing attacks

Between 2018-2022, the HPH Sector saw a **93% increase in large, reported breaches** and a **278% increase** in large **breaches involving ransomware.**

Chronic underfunding

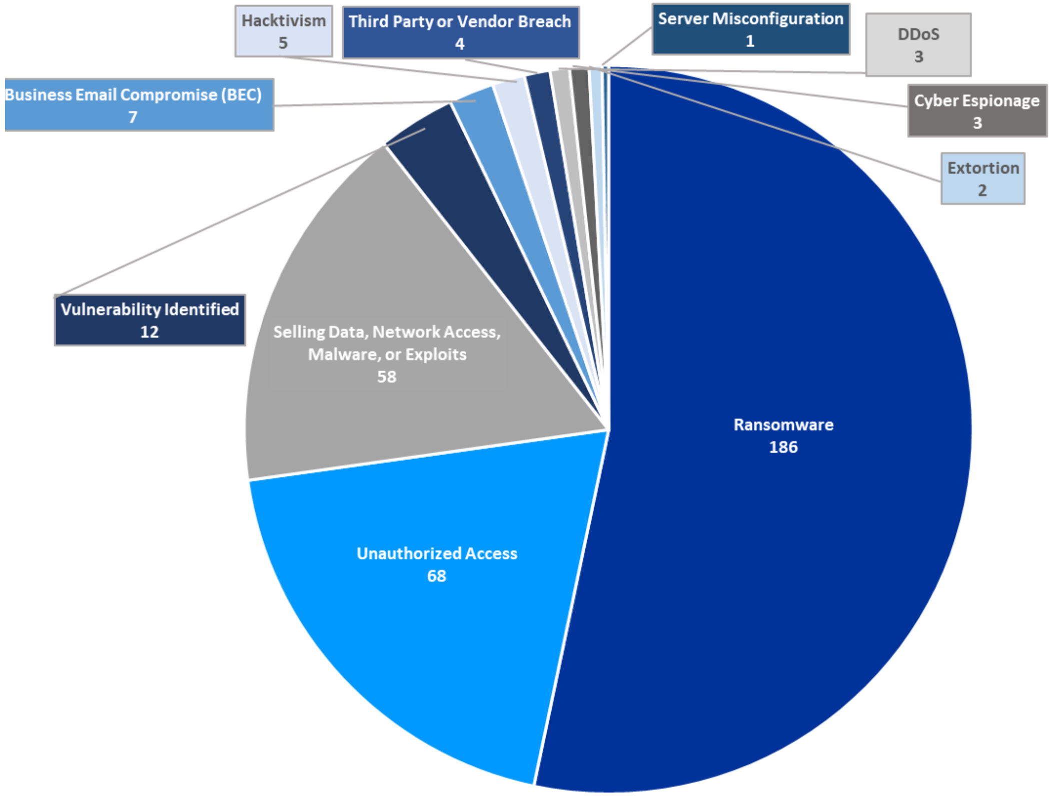
Cybersecurity planning efforts are chronically underfunded, leaving the Sector vulnerable and unable to address, or mitigate, cybersecurity risks.

Evolving threat landscape

The type, size, frequency, and scale of impact of cybersecurity attacks is continuously evolving and, due to a myriad factors, the HPH Sector cannot keep up.

Requests for clear guidance

The HPH Sector has asked for help prioritizing most impactful practices to enhance cybersecurity tailored to their needs.



# of cyberattacks on the HPH Sector, by type: Q3, 2023

What are the Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (CPGs)?

The HPH CPGs were developed and adapted from the 2023 DHS/CISA-led Cross-Sector CPGs and provide HPH Sector-specific cybersecurity guidance to healthcare and public health organizations at all levels of technical competency and resource-availability.

Overview

A **baseline set of recommended cybersecurity controls and best practices** with known risk-reduction values

Developed by HHS, DHS/CISA, and the private sector community for information technology (IT) and operational technology (OT) owners and operators to improve the state of cybersecurity within HPH entities

HHS CPGs **work to simplify the confusion** of multiple frameworks and recommendations, and **support compliance** with other regulatory requirements

Benefits

Strengthen cyber preparedness

Improve cyber resilience

Protect patient information and safety

How can your organization take immediate action?

The HPH CPGs help provide layered protection at different points of potential exploitation in healthcare digital systems. Layered protection at key points along the cybersecurity attack chain are crucial to mitigating the impacts of cybersecurity attacks when they occur. The HPH CPGs are divided into two categories supporting this layered approach:

Essential Goals

Essential Goals **set a floor of safeguards** to help healthcare organizations **address common vulnerabilities**, improve response when events occur, and minimize residual risk.

Examples of Essential Goals

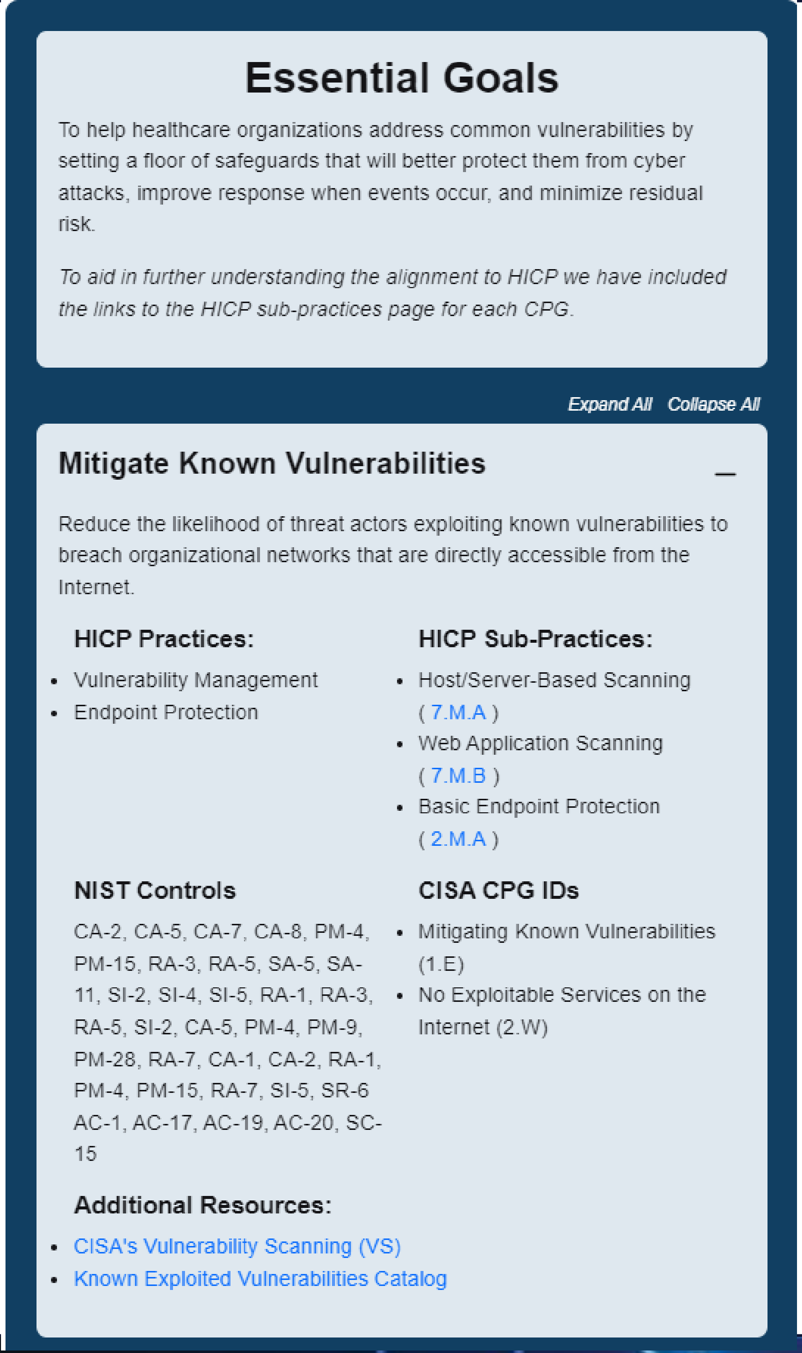
- Mitigate known vulnerabilities
- Enhance email security
- Implement multifactor authentication
- Promote strong encryption
- Use unique credentials
- Separate user and privileged accounts
- Establish both vendor and supplier cybersecurity requirements

Enhanced Goals

Enhanced Goals **enable organizations to mature their cybersecurity capabilities** and enhance the defenses needed to protect against less common, but potentially more impactful, attack vectors.

Examples of Enhanced Goals

- Develop and oversee an asset inventory
- Implement third party vulnerability disclosures
- Establish cybersecurity testing procedures and norms
- Segment networks, especially mission critical assets
- Centralize log collection
- Centralize incident planning and preparedness
- Manage device and systems settings in a consistent manner



Essential Goals

To help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyber attacks, improve response when events occur, and minimize residual risk.

To aid in further understanding the alignment to HICP we have included the links to the HICP sub-practices page for each CPG.

Mitigate Known Vulnerabilities

Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.

HICP Practices:

- Vulnerability Management
- Endpoint Protection

HICP Sub-Practices:

- Host/Server-Based Scanning (7.M.A)
- Web Application Scanning (7.M.B)
- Basic Endpoint Protection (2.M.A)

NIST Controls

CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, RA-1, RA-3, RA-5, SI-2, CA-5, PM-4, PM-9, PM-28, RA-7, CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15

CISA CPG IDs

- Mitigating Known Vulnerabilities (1.E)
- No Exploitable Services on the Internet (2.W)

Additional Resources:

- CISA's Vulnerability Scanning (VS)
- Known Exploited Vulnerabilities Catalog

Essential Goals

The Essential Goals are as follows:

- **Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.
- **Email Security:** Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud.
- **Multifactor Authentication:** Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet**.**
- **Basic Cybersecurity Training:** Ensure organizational users learn and perform more secure behaviors.
- **Strong Encryption:** Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion.
- **Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers:** Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly.
- **Basic Incident Planning and Preparedness:** Ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents.
- **Unique Credentials:** Use unique credentials inside organizations' networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks.
- **Separate User and Privileged Accounts:** Establish secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised.
- **Vendor/Supplier Cybersecurity Requirements:** Identify, assess, and mitigate risks associated with third party products and services.

405(d) Outreach & Program Resources

HHS/405(d) Awareness Materials

Knowledge on Demand

405(d) Outreach

Official Task Group Products

CYBER DILIGENCE & HEALTH CRISES

During a health crisis, keeping patients safe is the #1 priority so remember, Cyber Safety is Patient Safety.

Be cautious of the 5 most pre[illegible] cyberse[illegible] during a [illegible]

1. Ransomw[illegible]
2. Email Phi[illegible]
3. Network [illegible]
4. Loss or T[illegible] or Data
5. Medical D[illegible]

To protect your patients and organization, keep in mind these cyber safety tips:

1. Don't click it, check it
2. Prevent it, See it, Report it
3. Secure your home office

405(d) Program Presents:

A Case Study of "Cancer Care in the Wake of a Cyber Attack"

Aligning Health Care Industry Security Approaches

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Log4j
HHS 405(d) Program SBAR Brief
December 17, 2021

The 405(d) Situation, Background, Assessment, Recommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the Cybersecurity Act of 2015 with the goal of aligning industry security approaches, the 405(d) SBARs, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: A potentially catastrophic vulnerability has recently been identified that applies to a common application called Log4j. This vulnerability is found in products that have Java based software installed. The software was created by The Apache Software Foundation and is widely used in applications, inclusive of Linux and Windows operating systems. The exploitation allows the execution of any code which could result in compromise of the server, download of malicious binaries, or propagation of further attacks such as ransomware or a zero-day attack. Healthcare and Public Health (HPH) organizations are being urged to review the recently released Apache security patch with their security team and take immediate action to secure their organization and protect their patients. The link to the patch can be found here: Apache Log4j Vulnerability Guidance | CISA. Also, continue to check for the latest updates as there are still many unknown implications of this vulnerability. The patch may not supply a fix for all organizations because of legacy systems that may be present in their network.[1] There are other security precautions that can be put in place to secure your organization. Continue reading for additional tools and resources.

Pertinent and brief information related to the situation

BACKGROUND: This tool is used universally between developers and vendor solutions for enabling logging features in their applications. Log4j is an open source tool, which means that it is easily available and free to use. It is often downloaded by any size organization to assist with user error log information, such as how many times an employee incorrectly enters their password when logging into their computer.

This is a commonly used vendor product and IT solution. It can be susceptible to hackers who can use this access to perpetrate further attacks against the organization, such as deploying malware, downloading more attack tools, and pivoting into the broader network.

Analysis and considerations of options—what we found and think

ASSESSMENT: The popularity and accessibility of the Log4j software makes it a potential risk to all healthcare organizations regardless of size. This vulnerability is becoming more widespread every day. At this time, the true impact of this vulnerability is unknown because the various ways of exploitation are still being identified. It is estimated that this vulnerability could potentially affect hundreds of millions of devices, networks, and/or software platforms.

Healthcare organizations are dependent on readily available devices and software that are vendor supplied and connected to an external network to operate. These complex and interconnected devices affect patient safety and privacy. They represent potential attack vectors across an organization like medical equipment such as bedside monitors that monitor vital signs during an inpatient stay. Or, they may be more complicated, like infusion pumps that deliver specialized therapies and require continual drug library updates. If an attacker gained access to the network through a vulnerability such as Log4j, they would be able to gain control of the software and could potentially disconnect devices from the network, therefore, causing a disruption to daily procedures and putting patient safety at risk.

Many mainstream and well-known organizations, including cloud services, are already utilizing the Log4j software and may be vulnerable. This includes cloud applications that medical organizations utilize for Electronic Health Records (EHR) services and outsourced security services such as Software as a Service (SaaS). For an updated list of vendors/products that are affected, please visit: https://github.com/cisagov/log4j-affected-db

Staying Cyber Safe in the Healthcare and Public Health Sector
Tips for individuals and organizations

Why is healthcare targeted?

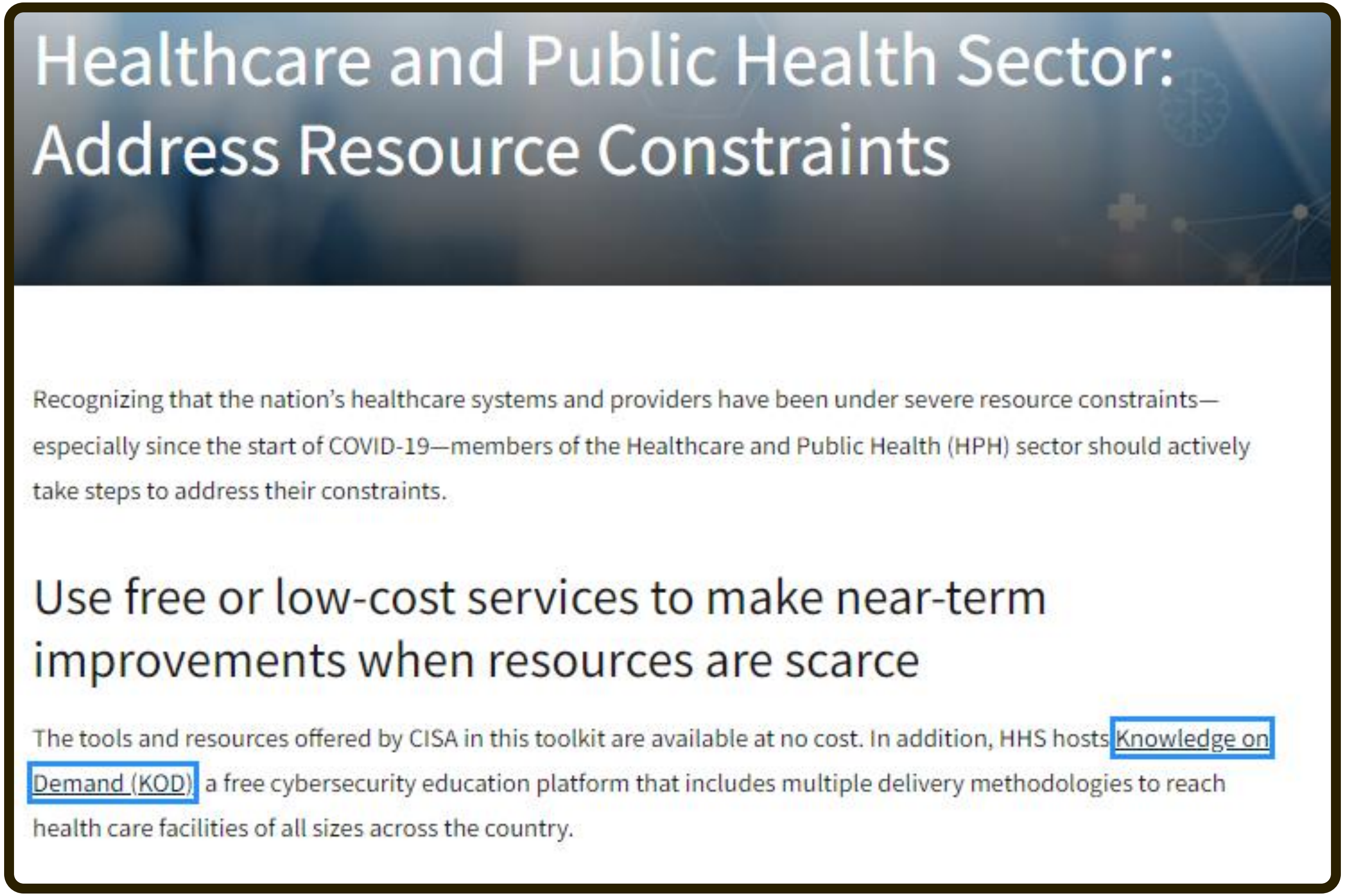
Where do these attacks come from?

Cyber Hygiene Tips:

Today’s Roadmap

- Intro to CISA & HHS ASPR
- Threat Environment
- Joint Cybersecurity Toolkit
- HHS Cyber Performance Goals
- **Additional Resources**

CISA/HHS Toolkit: Address Resource Constraints



Healthcare and Public Health Sector: Address Resource Constraints

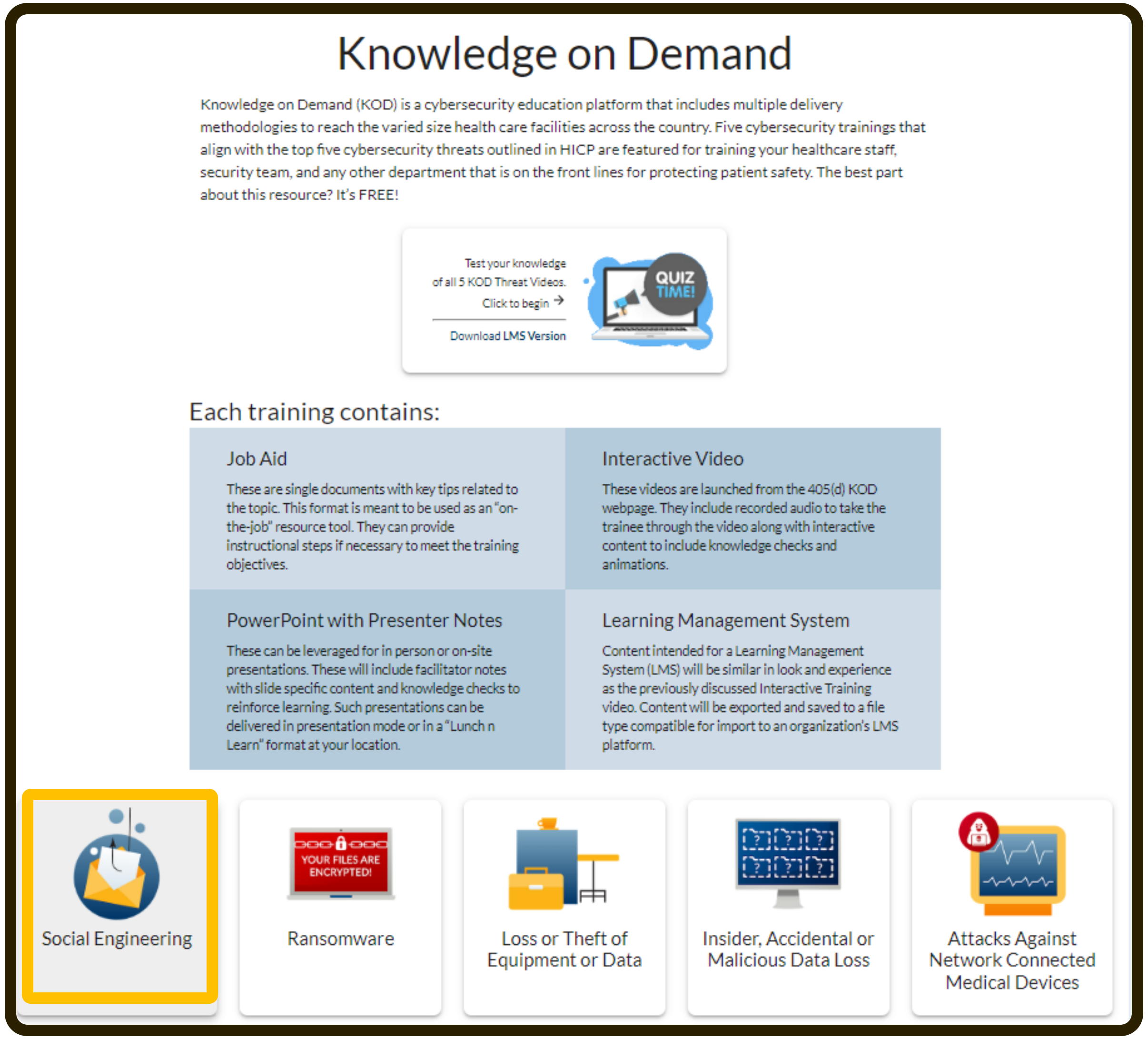
Recognizing that the nation's healthcare systems and providers have been under severe resource constraints—especially since the start of COVID-19—members of the Healthcare and Public Health (HPH) sector should actively take steps to address their constraints.

Use free or low-cost services to make near-term improvements when resources are scarce

The tools and resources offered by CISA in this toolkit are available at no cost. In addition, HHS hosts Knowledge on Demand (KOD), a free cybersecurity education platform that includes multiple delivery methodologies to reach health care facilities of all sizes across the country.

Link to CISA/HHS Toolkit

CISA/HHS Toolkit: Knowledge On Demand



Knowledge on Demand

Knowledge on Demand (KOD) is a cybersecurity education platform that includes multiple delivery methodologies to reach the varied size health care facilities across the country. Five cybersecurity trainings that align with the top five cybersecurity threats outlined in HICP are featured for training your healthcare staff, security team, and any other department that is on the front lines for protecting patient safety. The best part about this resource? It's FREE!

Test your knowledge of all 5 KOD Threat Videos. Click to begin →

Download LMS Version

Each training contains:

Job Aid

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

Interactive Video

These videos are launched from the 405(d) KOD webpage. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

PowerPoint with Presenter Notes

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

Learning Management System

Content intended for a Learning Management System (LMS) will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

Social Engineering

Ransomware

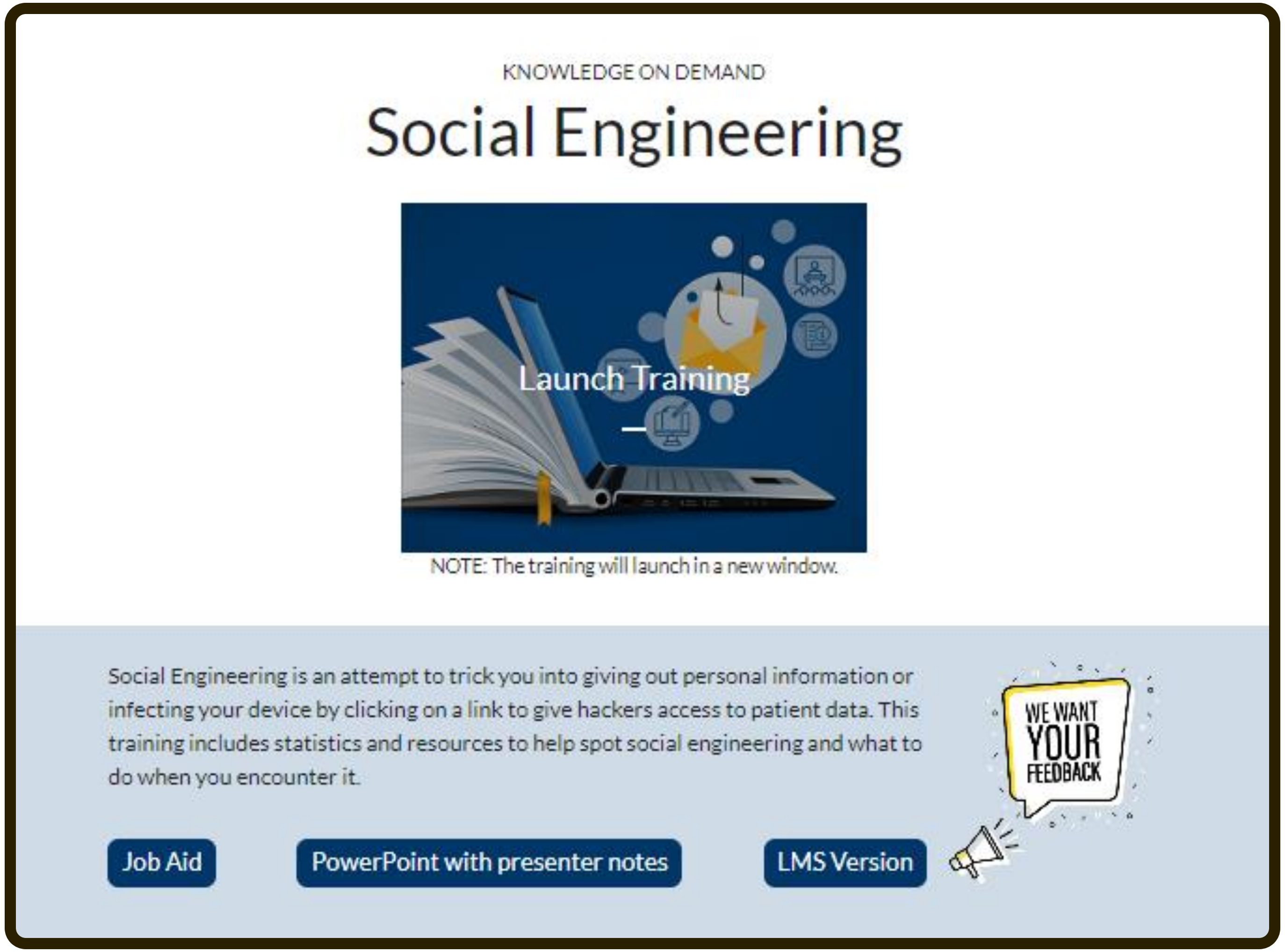
Loss or Theft of Equipment or Data

Insider, Accidental or Malicious Data Loss

Attacks Against Network Connected Medical Devices

Link to CISA/HHS Toolkit

CISA/HHS Toolkit: Knowledge On Demand



KNOWLEDGE ON DEMAND

Social Engineering

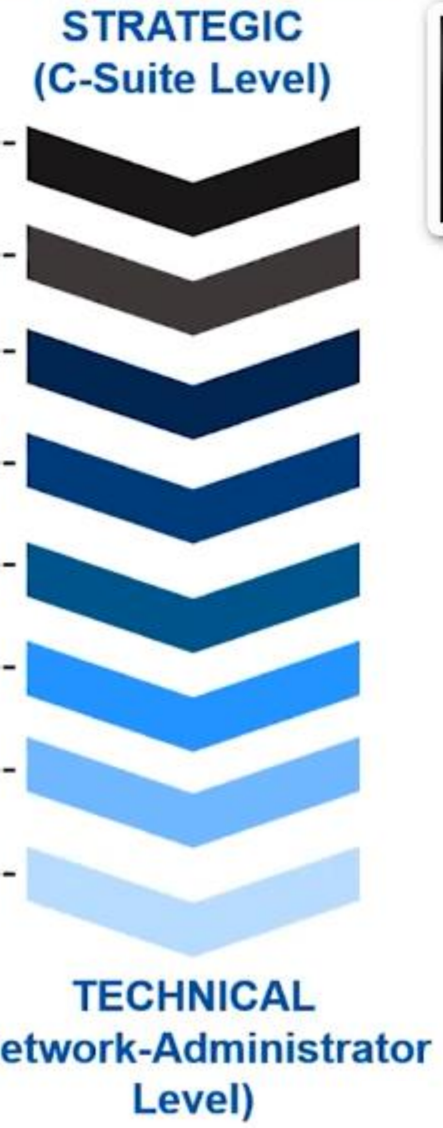
NOTE: The training will launch in a new window.

Social Engineering is an attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data. This training includes statistics and resources to help spot social engineering and what to do when you encounter it.

Link to CISA/HHS Toolkit

Cybersecurity Assessments

- Cyber Resilience Review (Strategic) --------------------------
- External Dependencies Management (Strategic)-----------
- Cyber Infrastructure Survey (Strategic)-----------------------
- Cybersecurity Evaluations Tool (Strategic/Technical)-----
- Phishing Campaign Assessment (Technical)----------------
- Vulnerability Scanning / Hygiene (Technical)----------------
- Validated Architecture Design Review (Technical)--------
- Risk and Vulnerability Assessment (Technical)-------------



Protected Critical Infrastructure Information Program

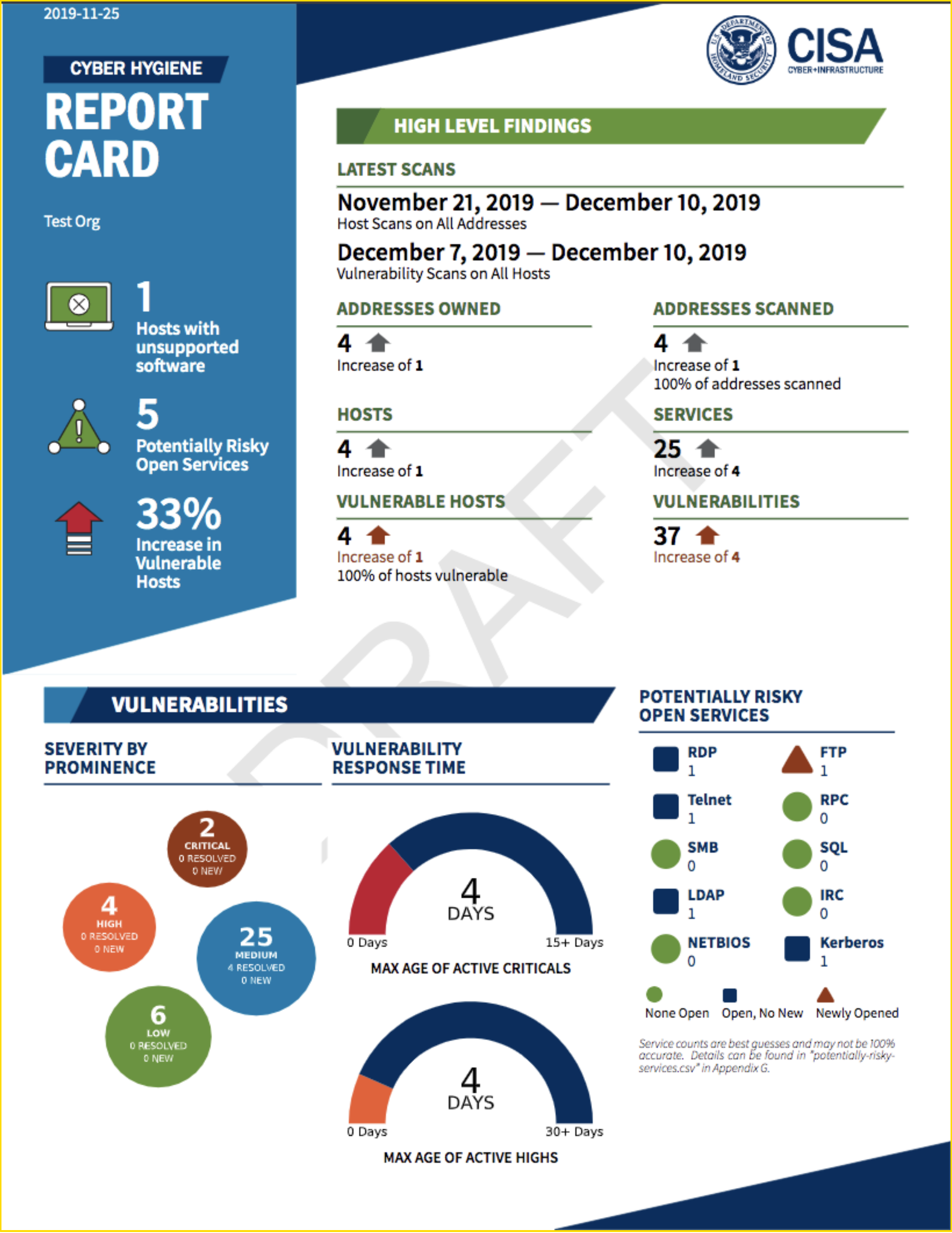
Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- 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.
  - To learn more, visit www.dhs.gov/pcii

Vulnerability Scanning

- Automated scanning of **External-facing, Internet accessible** systems (Top 1000 Ports, can include cloud sites)
- **Weekly report** card that includes current scan results, historic trends, Known Exploited Vulnerabilities, and comparisons to the national average
- Helps you understand your unique exposure
- **Know what the Internet already knows about your environment!**

Sign up by emailing
vulnerability@cisa.dhs.gov
with subject line
“Requesting Cyber Hygiene Services”



2019-11-25

CYBER HYGIENE
REPORT CARD

Test Org

1 Hosts with unsupported software

5 Potentially Risky Open Services

33% Increase in Vulnerable Hosts

CISA
CYBER+INFRASTRUCTURE

HIGH LEVEL FINDINGS

LATEST SCANS

November 21, 2019 — December 10, 2019
Host Scans on All Addresses

December 7, 2019 — December 10, 2019
Vulnerability Scans on All Hosts

ADDRESSES OWNED	ADDRESSES SCANNED
4 ⬆ Increase of **1**	**4** ⬆ Increase of **1** 100% of addresses scanned

HOSTS	SERVICES
4 ⬆ Increase of **1**	**25** ⬆ Increase of **4**

VULNERABLE HOSTS	VULNERABILITIES
4 ⬆ Increase of **1** 100% of hosts vulnerable	**37** ⬆ Increase of **4**

VULNERABILITIES

SEVERITY BY PROMINENCE

2 CRITICAL 0 RESOLVED 0 NEW
4 HIGH 0 RESOLVED 0 NEW
25 MEDIUM 4 RESOLVED 0 NEW
6 LOW 0 RESOLVED 0 NEW

VULNERABILITY RESPONSE TIME

4 DAYS
0 Days 15+ Days
MAX AGE OF ACTIVE CRITICALS

4 DAYS
0 Days 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

■	**RDP** 1	▲	**FTP** 1
■	**Telnet** 1	●	**RPC** 0
●	**SMB** 0	●	**SQL** 0
■	**LDAP** 1	●	**IRC** 0
●	**NETBIOS** 0	■	**Kerberos** 1

● None Open ■ Open, No New ▲ Newly Opened

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

#StopRansomware

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Cyber Tabletop Exercises (CTTX)

- National Cyber Exercise Program
- Premade CISA Tabletop Exercise Packages (CTEP) to help develop your own:
  - Healthcare & Public Health Sector Cyber CTEP Situation Manual
  - Ransomware CTEP Situation Manual
  - Ransomware Third Party Vendor CTEP Situation Manual
  - Vendor Phishing CTEP Situation Manual

Link to CISA CTEPs

Protective Security Advisor (PSA)

- **INFRASTRUCTURE SURVEY TOOL** - Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;

- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.

- **Infrastructure Visualization Platform (IVP) –** brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.

- **SAFE Tool** The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats

CISA Protective Security Advisors

QUESTIONS?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

For more information, visit **CISA.gov** or contact **central@cisa.dhs.gov**

Our Next Webinar

The NCTRC Webinar Series

Occurs 3rd Thursday of every month.

Hosting TRC: Mid-Atlantic Telehealth Resource Center (MATRC)
Telehealth Topic: Breaking Down Barriers to Telehealth: How the Digital Health Readiness Screener Can Drive Equity and Access
Date: January 16, 2025
Times: 11 AM – 12 PM (PT)

Please Complete Our Survey

Your opinion of this webinar is valuable to us.

Please participate in this brief perception survey (will also open after webinar):

https://www.surveymonkey.com/r/XK7R72F