

## **Cyber Threat Landscape: Risk, Impact and Preparedness**

**Scott Gee, Deputy National Advisor for Cybersecurity and Risk  
American Hospital Association**



# 42nd Annual Oregon Rural Health Conference

October 1 - 3, 2025  
Riverhouse Lodge | Bend, OR



## Cyber Threat Landscape: *Risk, Impact and Preparedness*

Scott Gee, Deputy National Advisor for Cybersecurity and Risk  
American Hospital Association

October 1, 2025

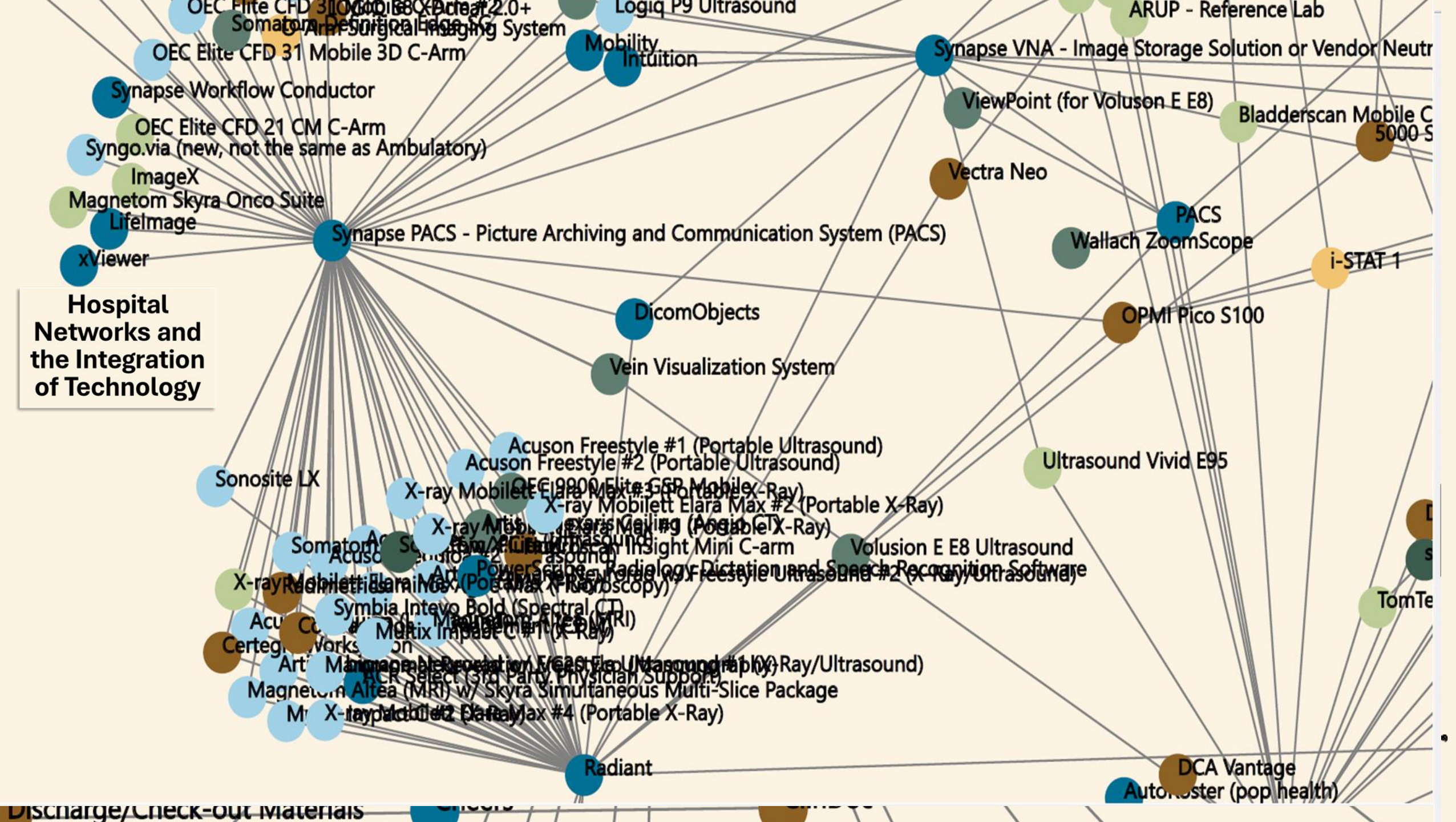




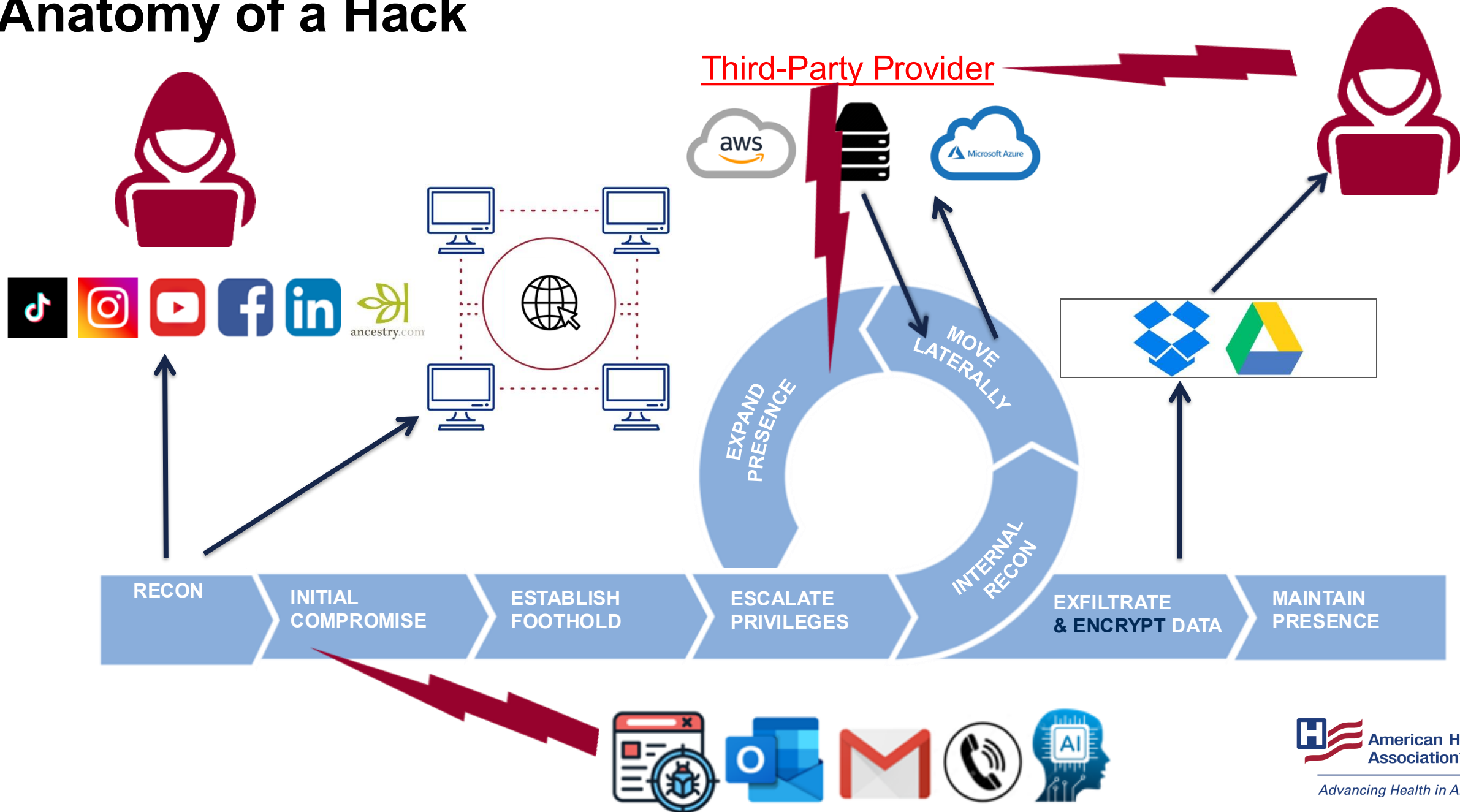






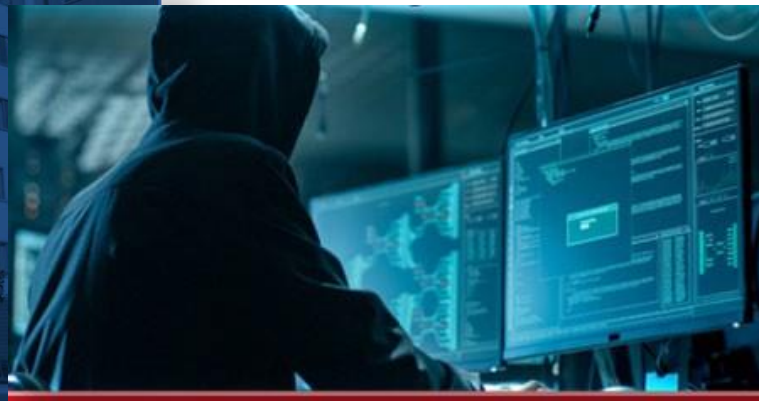


# Anatomy of a Hack



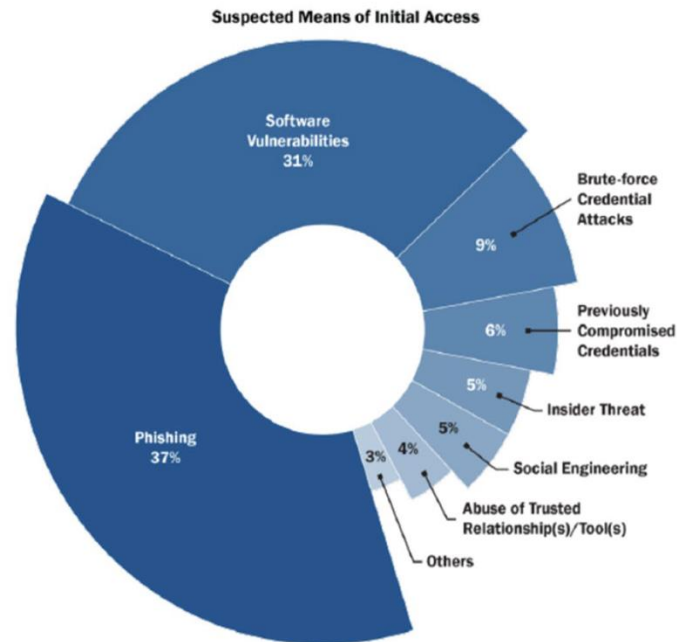


## Hospital Cyber Resiliency Initiative Landscape Analysis



Healthcare & Public Health  
Sector Coordinating Council  
PUBLIC PRIVATE PARTNERSHIP

Unit42 research presented at H-ISAC on the suspects' means of initial access in healthcare



### Social engineering



- This includes email phishing schemes, pretext calls, smishing, vishing, and
  - *With AI enhancements*
  - *Help Desk Manipulation*

### Exploiting technical vulnerabilities

- Unpatched known and exploited vulnerabilities (KEV) – 3<sup>rd</sup> Party software
- **Chained vulnerabilities** exploitations – including cloud services
- Insecure Remote Desktop Protocol (RDP)
- Zero-day vulnerabilities

### Stolen credentials

- This includes threat actors gaining access to employees' credentials via social engineering, email accounts, password spray attacks
- **Active Directory compromise**



Advancing Health in America



# Who are the Hackers?



Foreign Cyber Organized Crime Groups -Ransomware as a Service Groups

Nation State Military and Intelligence Services

Sometimes Both - Hybrid Threat

# Why Attack Hospitals and Healthcare ?

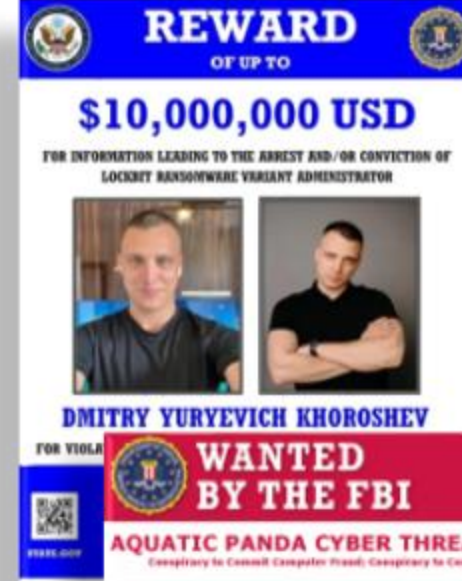


Stolen Data Monetization - PHI, PII, Financial, Medical Research (IP) Enduring Value

Data Extortion

***Impact - Ransomware Creates a “Threat to Life” situation***

Intelligence Value of Information – Strategic and Tactical



# Criminals Use Generative Artificial Intelligence to Facilitate Cyber Attacks

The FBI is (AI) to co schemes. deceive th by a user These too might oth synthetic to facilitat when cont criminals i recognition

## AI-Gener

Criminals social eng investmer fraud sche

- Crim profil
- Crim wider
- Crim gram
- Crim inves
- Crim victim

## AI-Gener



**Public Service Announcement**  
FEDERAL BUREAU OF INVESTIGATION

**Alert Number: I-051525-PSA**  
**May 15, 2025**

**Senior US Officials Impersonated in Malicious Messaging Campaign**

FBI is issuing this announcement to warn and provide mitigation tips to the public about an ongoing malicious text and voice messaging campaign. Since April 2025, malicious actors have impersonated senior US officials to target individuals, many of whom are current or former senior US federal or state government officials and their contacts. If you receive a message claiming to be from a senior US official, do not assume it is authentic.

**SPECIFIC CAMPAIGN DETAILS**

The malicious actors have sent text messages and AI-generated voice messages — techniques known as smishing and vishing, respectively — that claim to come from a senior US official in an effort to establish rapport before gaining access to personal accounts. One way the actors gain such access is by sending targeted individuals a malicious link under the guise of transitioning to a separate messaging platform. Access to personal or official accounts operated by US officials could be used to target other government officials, or their associates and contacts, by using trusted contact information they obtain. Contact information acquired through social engineering schemes could also be used to impersonate contacts to elicit information or funds.

"Smishing" is the malicious targeting of individuals using Short Message Service (SMS) or Multimedia Message Service (MMS) text messaging. "Vishing", which may incorporate AI-generated voices, is the malicious targeting of individuals using voice memos. Both smishing and vishing use tactics similar to spear phishing, which uses email to target specific individuals or groups.

**SMISHING, VISHING, AND SPEAR PHISHING ARE COMMON CRIMINAL TACTICS**

- Advanced and Rapid Identification of Network and Software Vulnerabilities
- Advanced and Rapid
- AI-Generated Text
- AI-Generated Images
- AI-Generated Audio, aka Vocal Cloning
- AI-Generated Videos

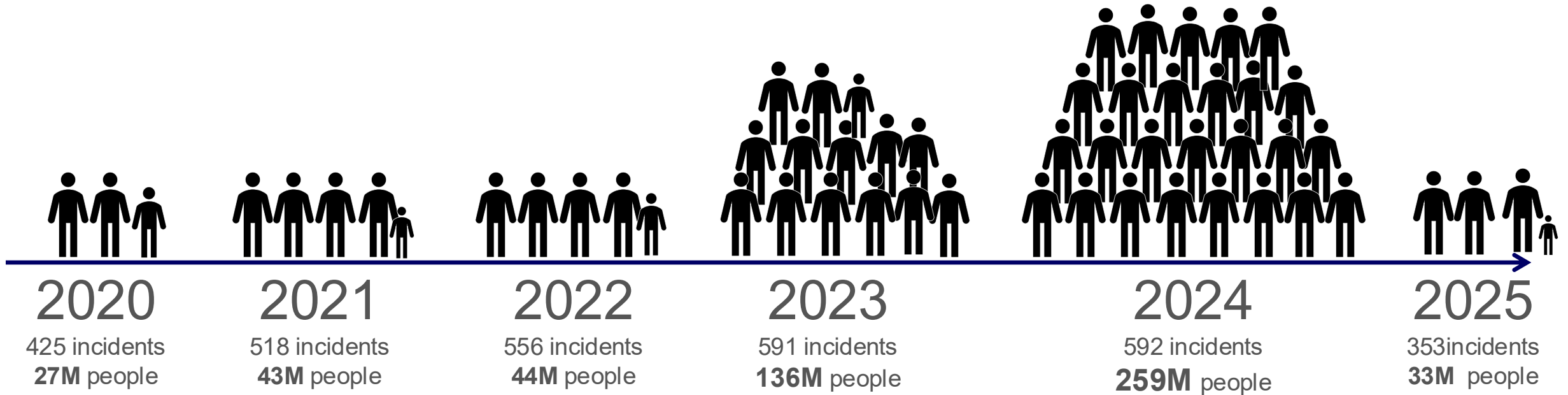





# Recent Cyber Headlines

# Hacking and Attacking Health Care

By the numbers



 = 10 million people



# 2025 - Top 25 Reported Healthcare Hacks, as of 09/29/2025

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Episource, LLC	CA	Business Associate	5,418,866	06/06/2025	Hacking/IT Incident	Network Server
Blue Shield of California	CA	Business Associate	4,700,000	04/09/2025	Hacking/IT Incident	Network Server
DaVita Inc.	CO	Healthcare Provider	2,689,826	08/01/2025	Hacking/IT Incident	Network Server
Anne Arundel Dermatology	MD	Healthcare Provider	1,905,000	07/11/2025	Hacking/IT Incident	Network Server
Radiology Associates of Richmond, Inc.	VA	Healthcare Provider	1,419,091	07/01/2025	Hacking/IT Incident	Network Server
Southeast Series of Lockton Companies, LLC (Lockton)	GA	Business Associate	1,124,727	02/28/2025	Hacking/IT Incident	Network Server
Community Health Center, Inc.	CT	Healthcare Provider	1,060,936	01/30/2025	Hacking/IT Incident	EMR, Network Server
Frederick Health	MD	Healthcare Provider	934,326	03/28/2025	Hacking/IT Incident	Network Server
McLaren Health Care	MI	Healthcare Provider	743,131	06/24/2025	Hacking/IT Incident	Network Server
Medusind Inc.	FL	Business Associate	701,475	01/07/2025	Hacking/IT Incident	Network Server
Kelly & Associates Insurance Group, Inc.	MD	Business Associate	553,332	04/00/2025	Hacking/IT Incident	Network Server
Goshen Medical Center	NC	Healthcare Provider	456,385	09/17/2025	Hacking/IT Incident	Network Server
Ascension Health	MO	Healthcare Provider	437,329	04/28/2025	Hacking/IT Incident	Network Server
Onsite Mammography	MA	Business Associate	357,265	04/21/2025	Hacking/IT Incident	Email
St Clair Orthopaedics & Sports Medicine	MI	Healthcare Provider	340,000	01/30/2025	Hacking/IT Incident	Network Server
New Era Life Insurance Companies	TX	Health Plan	335,506	02/11/2025	Hacking/IT Incident	Network Server
Compumedics USA, Inc.	NC	Business Associate	318,150	06/27/2025	Hacking/IT Incident	Network Server
Allegheny Health Network Home Medical Equipment LLC and Allegheny	PA	Healthcare Provider	292,773	01/17/2025	Hacking/IT Incident	Network Server
Zumpano Patricios, P.A.	FL	Business Associate	279,275	07/03/2025	Hacking/IT Incident	Network Server
Union Health System, Inc.	IN	Healthcare Provider	262,831	04/21/2025	Hacking/IT Incident	Network Server
		<b>364 Incidents</b>	<b>33,289,884</b>	<b>Individuals impacted</b>		

# Third-party cyber risk exposure

- Data theft
- Network access by Third-party
- Supply chain attacks
- *Loss of service availability > Cascading effects*
- *Third Party Risk Management Program*
  - *Life, mission and business criticality*
  - *Storage or access to sensitive data*
  - *Privileged persistent network access*
  - *Requirements Must be in BAA*
  - *AVOID exclusivity clauses – Need to prepare contingency plans and contracts prior to attack*





U.S. NEWS

# A massive telecom threat was stopped right as world leaders gathered at UN headquarters in New York



The U.S. Secret Service has dismantled a massive hidden telecom network in New York. Investigators say the system could have crippled cell towers and jammed 911 calls. (AP Video: David R. Martin)



This photo provided by the U.S. Secret Service, in New York, Monday, Sept. 22, 2025, shows SIM card packaging that was seized by the agency. (U.S. Secret Service via AP)



PASSENGERS CAST SHADOWS AT LONDON'S HEATHROW AIRPORT IN 2018. IMAGE: YOLANDA SUEN VIA UNSPLASH

Daryna Antoniuk

September 24th, 2025

Cybercrime

News

Industry

## UK authorities announce arrest in cyberattack that disrupted European airports

Britain's National Crime Agency (NCA) said it has arrested a man as part of an investigation into a cyberattack that **disrupted flights** at Heathrow and several other European airports over the weekend.



*Advancing Health in America*



# Cloudflare Joins List of Salesloft Drift Breach Victims

Full Breach Scope Remains Unclear; Hundreds of Organizations Reported Affected

Mathew J. Schwartz (@euroinfosec) • September 3, 2025

Share Tweet



Image: Shutterstock

A rash of data breaches caused by hackers' theft of access service software provider Salesloft's Drift artificial intelligence Cloudflare, alongside what investigators say are many hundreds of other data.

**Data Breach**  
Prevention. Response. Notification. TODAY

CyberEd.io Cybersecurity Awareness Coming Soon  
BE THE FIRST TO KNOW

Topics ▾ News ▾ Training ▾ Resources ▾ Events ▾ Jobs ▾

TRENDING: Adversarial Exposure Validation (AEV) - The Missing Link in Your CTEM Program • Adaptive Risk Management

## Workday Breached as Ransomware Group Seeks Salesforce Data

CRM Breach May Be Tied to Ongoing Scattered Spider and ShinyHunters Campaign

Mathew J. Schwartz (@euroinfosec) • August 18, 2025

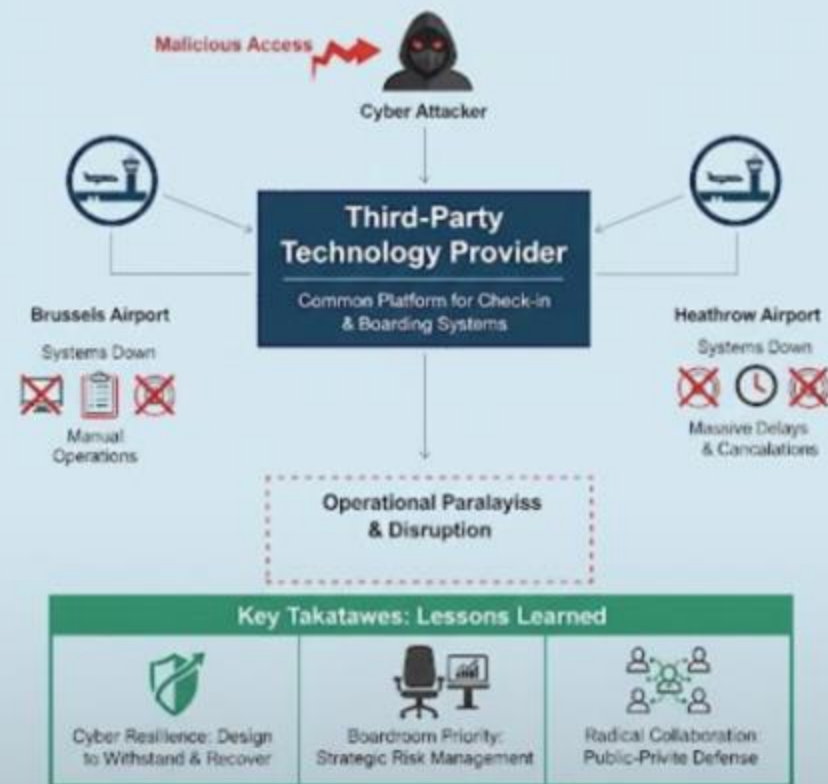
Share Tweet in Share Credit Eligible Get Permission



Image: Shutterstock

## European Airport Cyberattack: Critical Infrastructure Domino Effect

Single Point of Failure Triggers Systemic Crisis



 American Hospital Association™

Advancing Health in America

TLP AMBER: Limited Disclosure. This information may be shared within your organization.

September 8, 2025

## Joint Bulletin: Proliferation of the .med Top-level Domain and Associated Risks to the Health Sector

### EXECUTIVE SUMMARY

Health-ISAC and the American Hospital Association (AHA) collaborated to develop a joint bulletin, raising awareness about the new .med Top-Level Domain (TLD) and potential cybersecurity risks to health sector organizations. When originally developed approximately 10 years ago, the .med TLD was intended for use by the health sector to help end users identify reliable medical websites. However, on Sept. 2, 2025, the domains in the .med TLD were made available for purchase by the general public, on a first-come, first-served basis, **with no health care affiliation verification requirements or verification that the registrant is authorized to make a .med TLD registration on behalf of a known health care organization.**

The potential for unverified .med TLD proliferation also introduces significant risks, particularly the potential for exploitation by threat actors. It appears that the current validation process to register .med TLD is insufficient to warrant implied trust in the .med TLD, raising concerns about potential malicious use by threat actors. This bulletin outlines how .med domains can be leveraged for nefarious purposes, such as lookalike domains, and provides actionable recommendations to mitigate these risks.

"The AHA proactively worked with the field to identify this potential strategic and systemic cyber risk before it materialized. The guidance in this advisory will help members mitigate the risk associated with the appalling and irresponsible lack of controls in the registration process for .med domains," said John Riggi, AHA national advisor for cybersecurity and risk. "This advisory should be shared broadly with hospital and health system leadership in all functions."

### ANALYSIS

The .med TLD, despite its intended purpose of establishing a trusted medical community, is susceptible to the same types of abuse as other TLDs. In fact, its very nature as a domain designed for medical professionals and entities makes it a prime target for threat actors looking to exploit its inherent credibility.



## Dialysis firm DaVita hit by ransomware attack, says patient care continues

By Reuters

April 14, 2025 10:41 AM EDT • Updated 7 hours ago



## Interlock Begins Leaking Kettering Health's Stolen Data

Ohio-Based Organization Says It's Making Progress Restoring IT, Beefing Up Security

Marianne Kolbasuk McGee (@HealthInfoSec) • June 5, 2025

Share Tweet Share Credit Eligible Get Permission



ST. JOSEPH HOSPITAL IN NASHUA, NEW HAMPSHIRE. CREDIT: ST. JOSEPH VIA LINKEDIN

Jonathan Greig

May 30th, 2025

News Cybercrime

## Hospitals in Maine, New Hampshire limit services after cyberattack on Catholic health org

## Ransomware attack on OneBlood disrupts Florida blood supply, sparks urgent donation call

by Caden DeLisa | Aug 2, 2024



American Hospital Association™

Advancing Health in America



# FBI Director Wray talks cyberattacks, workplace violence

🕒 Apr 25, 2023 - 03:49 PM



*More than 1,000 executive leaders from the nation's top hospitals and health systems convened at the 2023 AHA Annual Membership Meeting, April 23-25 in Washington, D.C.*

**“What it comes down to is that cyber risk is business risk, and cyberattacks on hospitals specifically, are really threats to life.”**

FBI Director Wray at the AHA Annual Conference - 4/25/2023



# Geopolitical Risk = Cyber Risk

# Salt Typhoon: A Wake-Up Call For Strengthening Telecom Cybersecurity

By [Milind Gunjan](#) , Forbes Councils Member.

for [Forbes Technology Council](#), [COUNCIL POST](#) | Membership (fee-based)

Mar 05, 2025, 06:15am EST

**CYBERSECURITY** INFRASTRUCTURE SECURITY

## Volt Typhoon: The Cybersecurity Industry Effect on Critical Infrastructure

## Flax Typhoon using legitimate software to quietly access Taiwanese organizations

By [Microsoft Threat Intelligence](#)

## Microsoft: Chinese Hackers “Silk Typhoon” Now Target the IT Supply Chain





## Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

### Executive summary

People's Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally, including, but not limited to, telecommunications, government, transportation, lodging, and military infrastructure networks. While these actors focus on large backbone routers of major telecommunications providers, as well as provider edge (PE) and customer edge (CE) routers, they also leverage compromised devices and trusted connections to pivot into other networks. These actors often modify routers to maintain persistent, long-term access to networks.

This activity partially overlaps with cyber threat actor reporting by the cybersecurity industry—commonly referred to as Salt Typhoon, OPERATOR PANDA, RedMike, UNC5807, and GhostEmperor, among others. The authoring agencies are not adopting a particular commercial naming convention and hereafter refer to those responsible for

This report is marked TLP: CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules.

UOO198904-25 | PP-25-3703 | August 2025 Ver. 1.0

TLP: CLEAR

# UK warning: Russia's 'aggressive' cyber warfare is threat to NATO

Russian state-aligned groups have stepped up their cyberattacks against NATO countries in the past year, according to a senior British minister.

SHARE

## JOINT CYBERSECURITY ADVISORY

Authored by:



## Russian Military Cyber Global Critical Infrastru

### Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive [WhisperGate](#) malware against multiple Ukrainian victim organizations as early as January 13, 2022. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455.

To mitigate this malicious cyber activity, organizations should take the following actions today:

- Prioritize routine system updates and remediate known exploited vulnerabilities.
- Segment networks to prevent the spread of malicious activity.
- Enable phishing-resistant multifactor authentication (MFA) for all externally facing account services, especially for webmail, virtual private networks (VPNs), and accounts that access critical systems.

This Cybersecurity Advisory provides tactics, techniques, and procedures (TTPs) associated with Unit 29155 cyber actors—both during and succeeding their deployment of WhisperGate against Ukraine—as

## Software company providing services to US and UK grocery stores says it was hit by ransomware attack

By Sean Lyngaas, CNN  
2 minute read · Published 3:41 PM EST, Sun November 24, 2024

1 comment





# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-082025-PSA  
August 20, 2025

## Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure

The Federal Bureau of Investigation (FBI) is warning the public, private sector, and international community of the threat posed to computer networks and critical infrastructure by cyber actors attributed to the Russian Federal Security Service's (FSB) Center 16. The FBI detected Russian FSB cyber actors exploiting Simple Network Management Protocol (SNMP) and end-of-life networking devices running an unpatched vulnerability (CVE-2018-0171) in Cisco Smart Install (SMI) to broadly target entities in the United States and globally.

the top ten ransomware groups HC3 has seen targeting the healthcare sector.

### Report

This chart shows the top 10 most active ransomware groups HC3 has seen targeting the U.S. HPH:



## Chinese ship 'detained' after Baltic Sea cables were severed

The cargo ship, which had docked in Russian ports, has been stopped in the Danish Kattegat strait, with a navy patrol boat guarding it



Graphic by The Times and Sunday Times. Source: Marinetraxx



# DHS Warns of 'Heightened Threat' After US Strikes on Iran

Published Jun 22, 2025 at 2:46 PM EDT

Updated Jun 22, 2025 at 6:19 PM EDT

The U.S. [Department of Homeland Security](#) (DHS) warned of a heightened threat environment in the United States in its [Advisory System Bulletin](#).

The post comes hours after Washington struck three key nuclear



## Cybersecurity Advisory

June 23, 2025

### DHS Advises of Heightened Cyber, Physical Threat Environment Due to Activity in Iran

*No specific, credible threat to U.S. homeland or health care organizations*

## Israel-Iran War: Hacktivist Groups' Claimed Activity Surges

While Exceptions Apply, Such Efforts Often Only Amount to Psychological Operations

Mathew J. Schwartz (@euroinfosec) · June 20, 2025

Share Tweet Share Credit Eligible Get Permission





# JOINT CYBERSECURITY ADVISORY

Co-Authoring by:



TLP:CLEAR

Product ID: AAD4-242A

August 29, 2024

## #StopRansomware: RansomHub Ransomware

### Summary

*Note: This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit [stopransomware.gov](https://stopransomware.gov) to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

#### Actions to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Department of Health and Human Services (HHS) (hereafter referred to as the authoring organizations) are releasing this joint advisory to disseminate known RansomHub ransomware IOCs and TTPs. These have been identified through FBI threat response activities and third-party reporting as recently as August 2024. RansomHub is a ransomware-as-a-service variant—formerly known as Cyclops and Knight—that has established itself as an efficient and successful service model (recently attracting high-profile affiliates from other prominent variants such as LockBit and ALPHV).

Since its inception in February 2024, RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at [Report@cisa.gov](mailto:Report@cisa.gov) or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or [SOC@cisecurity.org](mailto:SOC@cisecurity.org)).

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see <http://www.cisa.gov/ttp>.

TLP:CLEAR



## Cybersecurity Advisory

August 29, 2024

### Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations

The FBI, Cybersecurity and Infrastructure Agency and the Department of Defense Cyber Crime Center today [issued](#) a joint advisory to warn of Iranian-based cyber actors leveraging unauthorized network access to U.S. organizations, including health care organizations, to facilitate, execute and profit from future ransomware attacks by apparently Russian-affiliated ransomware gangs. The Iranian group, which is associated with the Government of Iran, has conducted a high volume of cyberattack attempts on U.S. organizations since 2017 and as recently as August 2024. Based on an FBI assessment, the cyber actors obtain network access for espionage reasons then collaborate with ransomware groups, including the notorious Russian-linked ransomware groups [RansomHub](#) and APLHV aka [BlackCat](#), to execute ransomware attacks against the espionage target. BlackCat was responsible for the 2024 Change Healthcare ransomware attack, the largest and most consequential cyberattack in U.S. history. The advisory does not indicate if the Iranian actors had any role in the Change Healthcare attack but does state that the Iranian group's ransomware activities are not likely sanctioned by the Government of Iran.

The joint advisory provides tactics, techniques, procedures, and indicators of compromise obtained from FBI investigations and third-party reporting. The federal agencies urge organizations to apply the recommendations in the mitigations section of the advisory to reduce the likelihood of compromise from these Iranian-based cyber actors and other ransomware attacks.

"This alert demonstrates the close 'international cooperation' between hackers to exploit cyber espionage campaigns for criminal profit," said John Riggi, AHA national advisor for cybersecurity and risk. "This alert also demonstrates the nation-state level sophistication and expertise of the ransomware groups that target U.S. health care. No health care organization, regardless of their cybersecurity preparedness, can be expected to fully defend against a group of nation-state-trained hackers collaborating with sophisticated ransomware gangs. Clearly, the initial access leading to a subsequent ransomware attack, sanctioned or not, is state-sponsored. We strongly encourage the U.S. government to treat these attacks as national security threats, by policy and action, and impose significant risk and consequences on our cyber adversaries. Offense is the best defense."

Although there is no specific threat information at this time, the field is reminded to remain especially vigilant over the holiday weekend, as we have historically seen increased targeting of health care around the holidays.

pital

rica

# US Storms 29 Laptop Farms in Crackdown on North Korean IT Worker Schemes

The US has made 29 searches of known or suspected laptop farms supporting North Korean individuals posing as US IT workers.



By Ionut Arghire | July 1, 2025 (4:33 AM ET)



- Hundreds of US companies duped into hiring North Korean IT workers
- Americans aiding the scheme by running laptop farms in the US to disguise their location
- The FBI conducted 21 searches across 14 states
- These schemes are estimated to have netted more than \$88 million over six years.



Threats that the  
Administration Must  
Manage



## Putin and Kim Jong Un will meet in North Korea, supporter of Russia's war in Ukraine

UPDATED JUNE 18, 2024 · 2:30 PM ET

By Se Eun Gong





# Legislation and Policy



# Regulatory and Legislative Update

## 1 Cybersecurity bill (H.R. 7898) PL 116-321 with AHA-supported provisions signed into law Jan. 05, 2021

- Directs HHS to provide regulatory relief for HIPAA covered victims of cyber attacks
- Recognized cybersecurity practices in place previous 12 months
- Reduced fines
- Early, favorable termination of audits
- Mitigation of other penalties
- No increased penalties for not having recognized cybersecurity practices in place

***“The law provides the right balance of incentivizing voluntary, enhanced cybersecurity protocols in exchange for regulatory relief and recognition that breached organizations are victims, not the perpetrators.”***

## 2 Cybersecurity Act of 2015 – (High probability of renewal in 2025 to extend until 2035)

- Civil and Regulatory Protection for Sharing Cyber Threat Information and Defensive Measures with CISA and other Federal Agencies

## 3 HIPAA rewrite?



## View Rule

[View EO 12866 Meetings](#)

[Printer-Friendly Version](#)

[Download RIN Data in XML](#)

HHS/OCR

RIN: 0945-AA22

Publication ID: Spring 2025

**Title:** HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

**Abstract:**

This rule will modify the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). These modifications will improve cybersecurity in the health care sector by strengthening requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats.

**Agency:** Department of Health and Human Services(HHS)

**Priority:** Economically Significant

**RIN Status:** Previously published in the Unified Agenda

**Agenda Stage of Rulemaking:** Final Rule Stage

**Major:** Yes

**Unfunded Mandates:** Undetermined

**EO 14192 Designation:** Regulatory

**CFR Citation:** [45 CFR 160](#) [45 CFR 164](#)

**Legal Authority:** [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\), sec. 262 \(42 U.S.C. 1320d-2\)](#) [Health Information Technology for Economic and Clinical Health \(HITECH\) Act, sec. 13401 \(42 U.S.C. 17931\)](#)

**Legal Deadline:** None

**Timetable:**

Action	Date	FR Cite
NPRM	01/06/2025	<a href="#">90 FR 898</a>
Final Action	05/00/2026	

**Regulatory Flexibility Analysis Required:** Undetermined

**Government Levels Affected:** Undetermined

**Small Entities Affected:** Businesses, Governmental Jurisdictions, Organizations

**Federalism:** Undetermined

**Included in the Regulatory Plan:** Yes

**International Impacts:** This regulatory action will be likely to have international trade and investment effects, or otherwise be of international interest.

**RIN Data Printed in the FR:** No

**Agency Contact:**

Conner O'Brien

Senior Advisor

Department of Health and Human Services

Office for Civil Rights

200 Independence Ave, SW,

Washington, DC 20201

Phone: 800 537-7697

Email: [ocrprivacy@hhs.gov](mailto:ocrprivacy@hhs.gov)





## Discussion and Questions

**Scott Gee**  
**[sgee@aha.org](mailto:sgee@aha.org)**