American Hospital Association™

Advancing Health in America

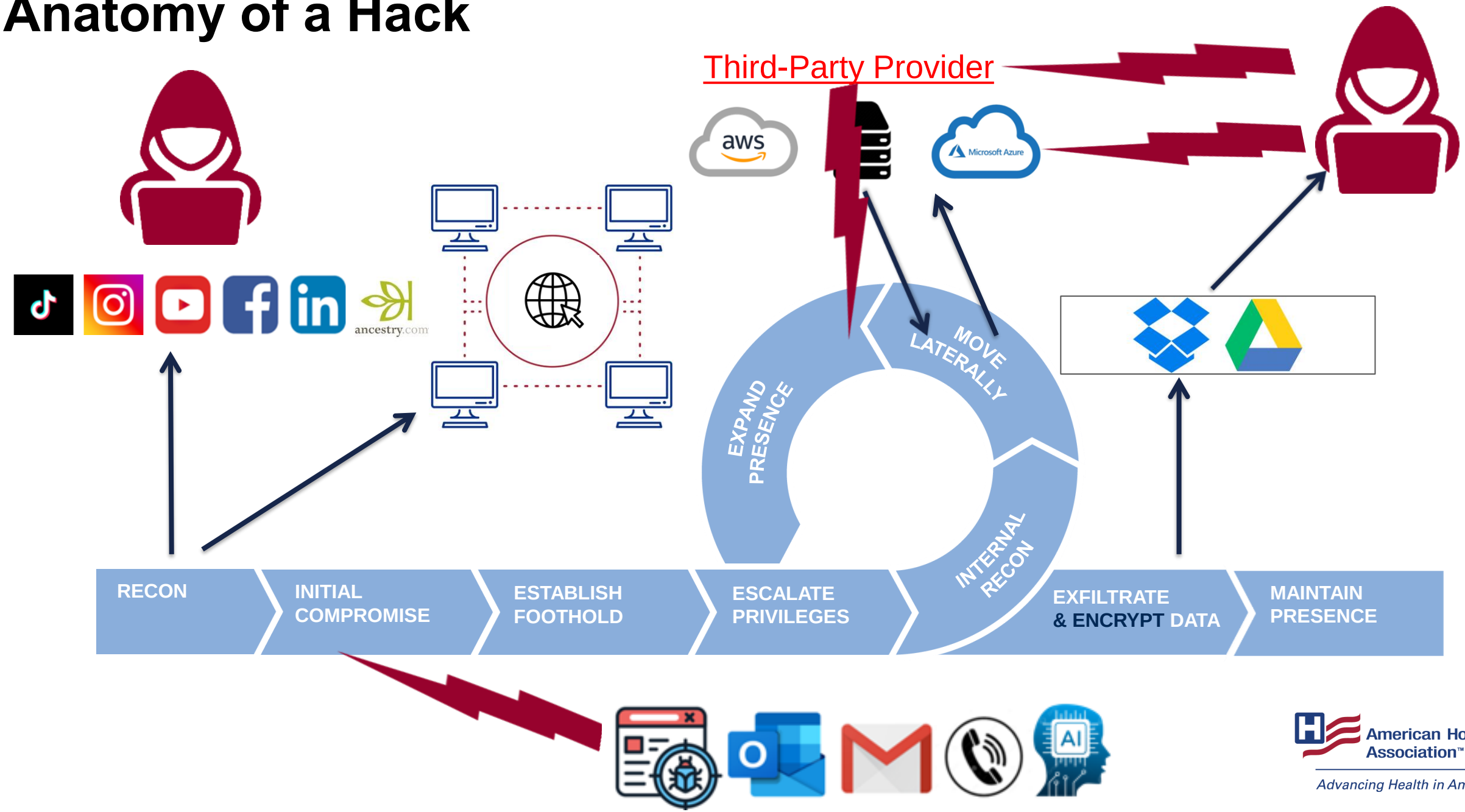
South Dakota Association of Healthcare Organizations

Cyber Threat Landscape:
Risk, Impact and Preparedness

Scott Gee, Deputy National Advisor for Cybersecurity and Risk, AHA

June 25, 2025

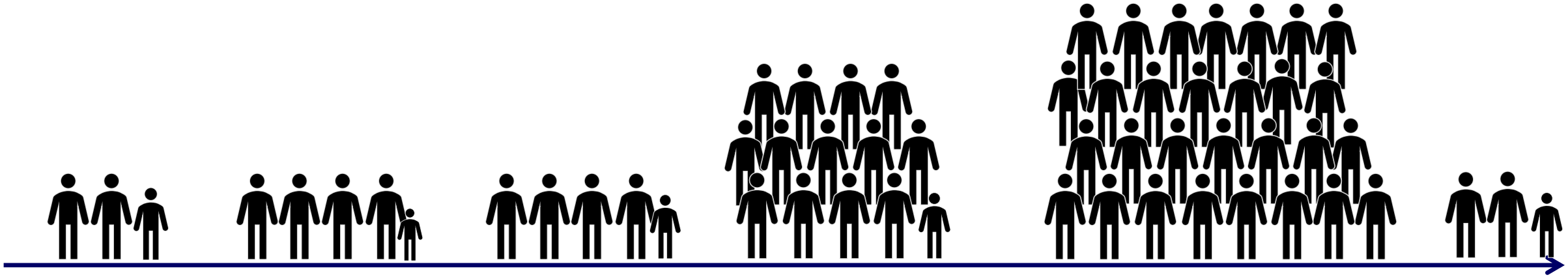
Anatomy of a Hack



American Hospital Association™
Advancing Health in America

Hacking Health Care

By the numbers

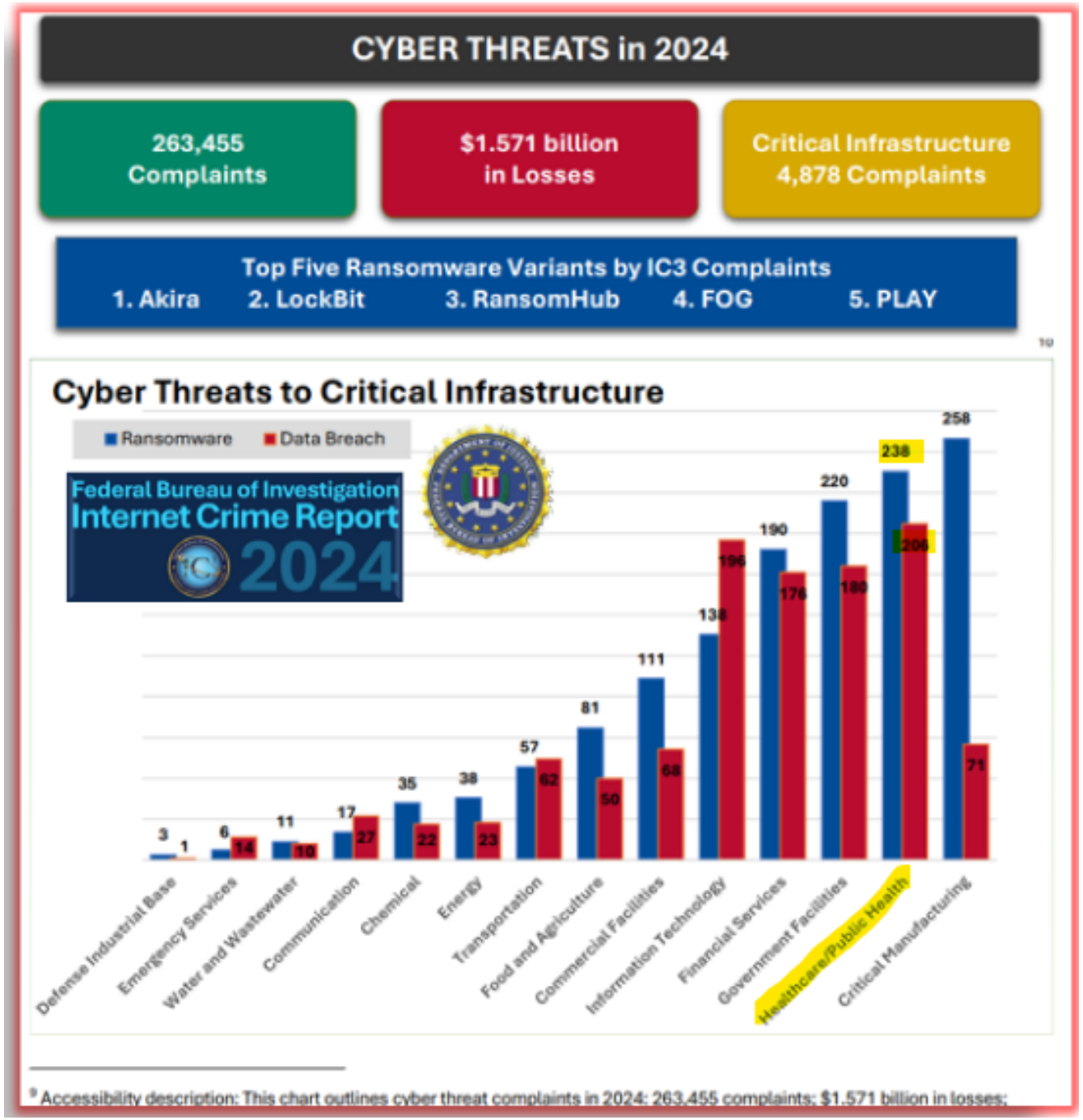


2020	2021	2022	2023	2024	2025
425 incidents 27M people	518 incidents 43M people	556 incidents 44M people	591 incidents 136M people	592 incidents 259M people	222 incidents 27.6M people

= 10 million people

American Hospital Association™

Advancing Health in America



FBI Internet Crime Report 2024
Issued 4/25/2025

FBI Reports for 2024:
Healthcare had 238 Reported Ransomware Attacks plus 206 Data Breaches,
Totaling 444 Reported Cyber Threats – The Most of All Critical Infrastructure Sectors

HHS-OCR 2024 Total:
592 Hacks, 259 Million Individuals Impacted

American Hospital Association™
Advancing Health in America

2025 - Top 25 Reported Healthcare Hacks, as of 06/23/2025

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Yale New Haven Health System	CT	Healthcare Provider	5,556,702	04/11/2025	Hacking/IT Incident	Network Server
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
Southeast Series of Lockton Companies, LLC (Lockton)	GA	Business Associate	1,118,572	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
Medusind Inc.	FL	Business Associate	701,475	01/07/2025	Hacking/IT Incident	Network Server
United Seating and Mobility, LLC d/b/a Numotion	TN	Healthcare Provider	494,326	03/07/2025	Hacking/IT Incident	Email
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
Allegheny Health Network Home Medical Equipment LLC and Allegheny Health	PA	Healthcare Provider	292,773	01/17/2025	Hacking/IT Incident	Network Server
Union Health System, Inc.	IN	Healthcare Provider	262,831	04/21/2025	Hacking/IT Incident	Network Server
The City of Long Beach, CA	CA	Healthcare Provider	258,191	04/14/2025	Hacking/IT Incident	Network Server
Ocuco Inc	FL	Business Associate	240,961	05/30/2025	Hacking/IT Incident	Network Server
Marlboro-Chesterfield Pathology, P.C.	NC	Healthcare Provider	235,911	05/09/2025	Hacking/IT Incident	Network Server
Sunflower Medical Group, P.A.	KS	Healthcare Provider	220,968	03/07/2025	Hacking/IT Incident	Network Server
Legacy Professionals, LLP	IL	Business Associate	216,752	02/28/2025	Hacking/IT Incident	Network Server
Dameron Hospital	CA	Healthcare Provider	210,706	04/02/2025	Hacking/IT Incident	Network Server
Asheville Eye Associates, PLLC	NC	Healthcare Provider	204,984	01/17/2025	Hacking/IT Incident	Network Server
Harbin Clinic, LLC	GA	Healthcare Provider	176,149	05/16/2025	Hacking/IT Incident	Network Server
CDHA Management, LLC and Spark DSO, LLC dba Chord Specialty Dental Par	TN	Healthcare Provider	173,430	03/14/2025	Hacking/IT Incident	Email
Central Texas Pediatric Orthopedics	TX	Healthcare Provider	140,000	04/04/2025	Hacking/IT Incident	Network Server
University Diagnostic Medical Imaging, PC	NY	Healthcare Provider	138,080	01/21/2025	Hacking/IT Incident	Network Server
		222 Incidents reported	**27,604,048**	**Individual Records**		

American Hospital Association™

Advancing Health in America

Key Observations - Cyber Attacks in 2024

1. Change Healthcare breach resulted in the theft of the PHI of ***190 million*** Americans

2. 95%+ of stolen PHI records were NOT stolen from hospitals – business associates, non-hospital providers and health plans…like CMS

3. 90% + were stolen ***OUTSIDE*** of the EMR. Stolen credentials and data mapping.

4. 100% of the hacked data was ***NOT*** encrypted. Stolen credentials, encryption principles

5. 70% of reported hacks were ransomware AND data theft - More of this in 2025?

6. 90%+ of ransomware attacks perpetrated by Russian speaking ransomware gangs…with some help

AHA helped secure funding and regulatory relief for the field.

payments on an individual basis, relax prior authorization requirements for struggling healthcare providers

AHA Executive Vice President for Government Relations and Public Policy Stacey Hughes participated in a Wall Street Journal panel to discuss the fallout from the Change Healthcare cybersecurity breach.

Molly Smith, AHA's group vice president for public policy, and many AHA leaders spoke to numerous national media outlets regarding the impact of the Change Healthcare cyber breach.

86/104

THE VALUE OF AHA MEMBERSHIP

John Riggi, AHA's national advisor for cybersecurity and risk, testified in front of the House Energy and Commerce Subcommittee on Health on the need for hospital support.

American Hospital Association™
Advancing Health in America

Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field

The cyberattack on Change Healthcare in February 2024 disrupted health care operations on an unprecedented national scale, endangering patients' access to care, disrupting critical clinical and eligibility operations and threatening the solvency of the nation's provider network. It demonstrated that the national consequences of cyberattacks targeting mission-critical third-party providers can be even more devastating than when hospitals or health systems are attacked directly.

Incident Overview

Attack target: Change Healthcare, a subsidiary of UnitedHealth Group, is the predominant source of more than 100 critical functions that keep the U.S. health care system operating. It annually processes 15 billion health care transactions — tou… …zation, drug prescriptions, claims

What …Cat encrypted and incapa…

Impa …lers and communities, endan… …in the country felt the impac… …h reserves, vendor redun…

WSJ PRO

UnitedHealth Estimates Change Healthcare Hack Impacted About 190 Million People

Over half of the U.S. had private data stolen in a 2024 cyberattack at the insurance giant—far more than previous estimates

By *James Rundle*

Jan. 24, 2025 8:58 pm ET | WSJ PRO

Share Resize Listen (2 min)

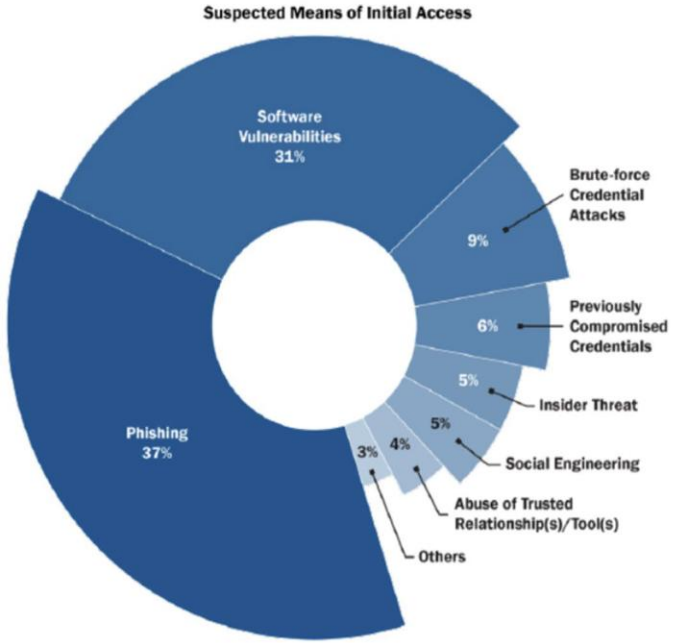
American Hospital Association™
Advancing Health in America

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***

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

- Phishing, pretext calls, smishing, vishing, help desk manipulation
- *Some with AI enhancements*

Exploiting technical vulnerabilities

- Unpatched vulnerabilities – 3P software
- Chain vulnerability exploitations
- Insecure Remote Desktop Protocol(RDP)
- Zero-day vulnerabilities

Stolen credentials

- Includes social engineering, email accounts, password spray attacks
- Active Directory compromise

American Hospital Association™
Advancing Health in America

South Dakota
Association of Healthcare Organizations

Cyber Risk Impact to Healthcare

American Hospital Association™
Advancing Health in America

AP

A cyberattack has disrupted hospitals and health care in several states

BY PAT EATON-ROBB

Updated 8:35 PM EDT, August 4, 2023

HEALTH

A month after cyberattack, Ascension says workers now have access to patient medical records at nsin hospitals, clinics

Volpenhein

ukee Journal Sentinel

n. CT June 11, 2024 | Updated 3:44 p.m. CT June 11, 2024

AP

WORLD U.S. POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK ODDITIES HEALTH VID

Israel-Hamas war U.S. inflation Homeland Security Secretary Alejandro Mayorkas Buffalo Bills' Josh

U.S. NEWS

Cyberattack hits 2 New York hospital forces ambulance diversions

Emergency rooms in at least 3 states diverting patients after ransomware attack

Ardent Health Services, which oversees 30 hospitals across the U.S., said it had shut down a significant number of its computerized services.

Great Plains Regional Medical Center Victim of Ransomware Attack

Data breach at Yale New Haven Health impacts 5.6M people

It's the largest healthcare brea

Published April 24, 2025

Emily Olsen
Reporter

HCAREDIVE Deep Dive

Anna Jacques Hospital Notifies 316K Patients About December 2023 Ransomware Attack

Posted By Steve Alder on Dec 9, 2024

Beth Israel Lahey Health's Anna Jaques Hospital in Newburyport, Massachusetts, has recently notified regulators and patients about a cyberattack and data breach that occurred on Christmas Day in 2023.

I-TEAM

I-Team: How the Change Healthcare cyber attack is impacting Massachusetts

by: Taylor Knight
Posted: Mar 21, 2024 / 02:11 PM EDT
Updated: Mar 21, 2024 / 07:09 PM EDT

Kidney Dialysis Services Provider DaVita Hit by Ransomware

DaVita has not named the ransomware

By Ionut Arghire
April 15, 2025

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

by Caden DeLisa | Aug 2, 2024

Reported Clinical and Business Impact of Ransomware Attacks on Hospitals 2020 – 2025

- **Radiology / Imaging / PACS down - other diagnostic te** … **ncology (RADONC)** treatment may be dependent upon **radiology lost. All could lead to stroke and trauma diver** … internet connected technology.
- **Cath lab down = heart attack diversion** … lay of treatment when diverted to alternate RADONC treatment
- ***Risk to patient safety***. **ED's shutdown** - **Ambulances pla** … **rural distance** delay of emergency treatment. Trauma Cent … **py** and RADONC treatment plans may not be available.
- **Telemetry systems inoperable** – additional staff required fo … **pared for extended clinical downtime procedures for *all*** Home health care telemetry. *Patients at home, greater risk?* … **nd paper EMR charting lasting up to three to four weeks**
- **EHR rendered inaccessible**. Patient history, treatment prot … **ur week *recovery time*** *for mission critical systems, ransom* interactions unknown – delay in rendering care … ***residual impacts lasting 6 months - 2 years***
- **Lab** and **Pathology** disrupted … **rrupted or only 65% restoration from uncorrupted**
- Elective **surgeries** cancelled … **TO and RPO not fully understood.**
- **ADT** forms and instructions unavailable … **ems unrecoverable**
- **Drug cabinet**/ **pharmacy** systems down … **erruption and revenue loss** due to incomplete charts. **Need 60 n hand – no income for 60 days.**
- **Loss of VoIP phones and email systems** … **timekeeping and payroll systems disrupted**
- **Ransomware "blast radius" – effect on other providers v** … **and physical security technology impact**, access control ED, EMR, labs, imaging, cancer treatment and other third p … **s** requesting independent certification before reconnection
- **Regional impact** and stress based upon **capacity** of surrou … **surance** premiums or loss of coverage
- Simultaneous loss of all network and internet connected info … for publicly released PHI or negative outcome operational technology – ***Downtime computers lost or lin***
- ***ED wait times significantly increased.*** … **deral regulatory liability + Reputational Har**

American Hospital Association™
Advancing Health in America

United Nations | UN News
Global perspective Human stories

UN Photo/Manuel Elías | Eduardo Conrad, President of Ascension, briefs the Security Council on impacts of ransomware attacks on hospitals run by the organization.

Real world turmoil

Eduardo Conrado, President of Ascension Healthcare, a US-based non-profit healthcare provider, shared firsthand insights into the harsh realities of ransomware attacks.

He detailed the May 2024 cyberattack on Ascension, which severely disrupted operations across its 120 hospitals.

The attack encrypted thousands of computer systems, rendering electronic health records inaccessible and affecting key diagnostic services, including magnetic resonance imaging (MRIs) and computed tomography (CT) scans.

Mr. Conrado illustrated the practical challenges that arose: "**nurses were unable to look up patient records from their computer stations** and were forced to comb through paper back-ups…imaging teams were unable to quickly send the latest scans up to surgeons waiting in the operating rooms, and **we had to rely on runners to deliver printed copies of the scans to the hands of our surgery teams.**"

These disruptions not only delayed care but increased patient risk and placed an extraordinary burden on medical staff already contending with high-stress conditions, he said.

Restoring operations took 37 days, during which the backlog of paper records grew to a towering mile-high equivalent, he said, adding that financially, Ascension spent about $130 million on its response to the attack and lost approximately $0.9 billion in operating revenue as of the

- Russian ransomware group attack May 2024
- Disruption to 120 hospitals, care sites across 19 states
- Diversions to nearby hospitals – Regional impact
- Over ***$1 Billion*** in costs to Ascension and counting…
  - $130 Million in initial response costs
  - $900 Million lost operating revenue
  - 30-day recovery for core systems
- This is a global threat and a national security threat

"…nurses were unable to look up patient records from their computer stations and were forced to comb through paper back-ups…imaging teams were unable to quickly send the latest scans up to surgeons waiting in the operating rooms, and we had to rely on runners to deliver printed copies of the scans to the hands of our surgery teams."

Eduardo Conrado, President of Ascension, testimony before the UN Security Council - 11/08/2024

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 cyber-attacks on hospitals specifically, are really threats to life."

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

American Hospital Association™

Advancing Health in America

South Dakota
Association of Healthcare Organizations

Recent Cyber Threats and Risk

American Hospital Association™
Advancing Health in America

Dialysis firm DaVita hit
attack, says patient care

By **Reuters**

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

The outdoor sign seen at the DaVita Dialysis clinic in Denver February 16, 2016. RE
Rights

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

American Hospital Association™

Advancing Health in America

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

Image: Kettering Health

IMAGE: KETTERINGHEAL

Jonathan Greig

June 6th, 2025

Cybercrime

"Cybercrime group Interlock has begun publishing some of the 941-gbytes of data the gang claims to have stolen in a disruptive May attack on Kettering Health. The Ohio-based healthcare organization is making IT system restoration progress and cyber enhancements, but is still recovering."

American Hospital Association™

Advancing Health in America

Cybersecurity Experts Slam Oracle's Handling of Big Breach

Technology Giant Accused of Using 'Wordplay' to Previously Deny Breach Report

Mathew J. Schwartz (euroinfosec) · April 3, 2025

Share Tweet Share Credit Eligible

Image: Shutterstock

Cybersecurity experts slammed Oracle's handling of a customer data breach that appears to stem from infrastructure the technology giant failed to update and keep secure.

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

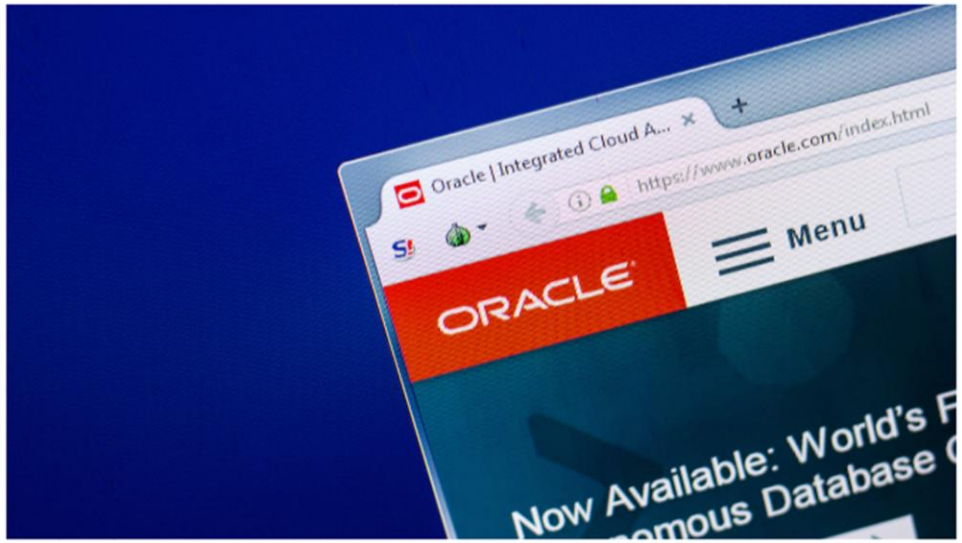
Malware & Threats · Security Operations · Security Architecture · Risk Management · CISO Strategy · ICS/OT · Funding/M&A

CLOUD SECURITY

Oracle Confirms Cloud Hack

Oracle has confirmed suffering a data breach but the tech giant is apparently trying to downplay the impact of the incident.

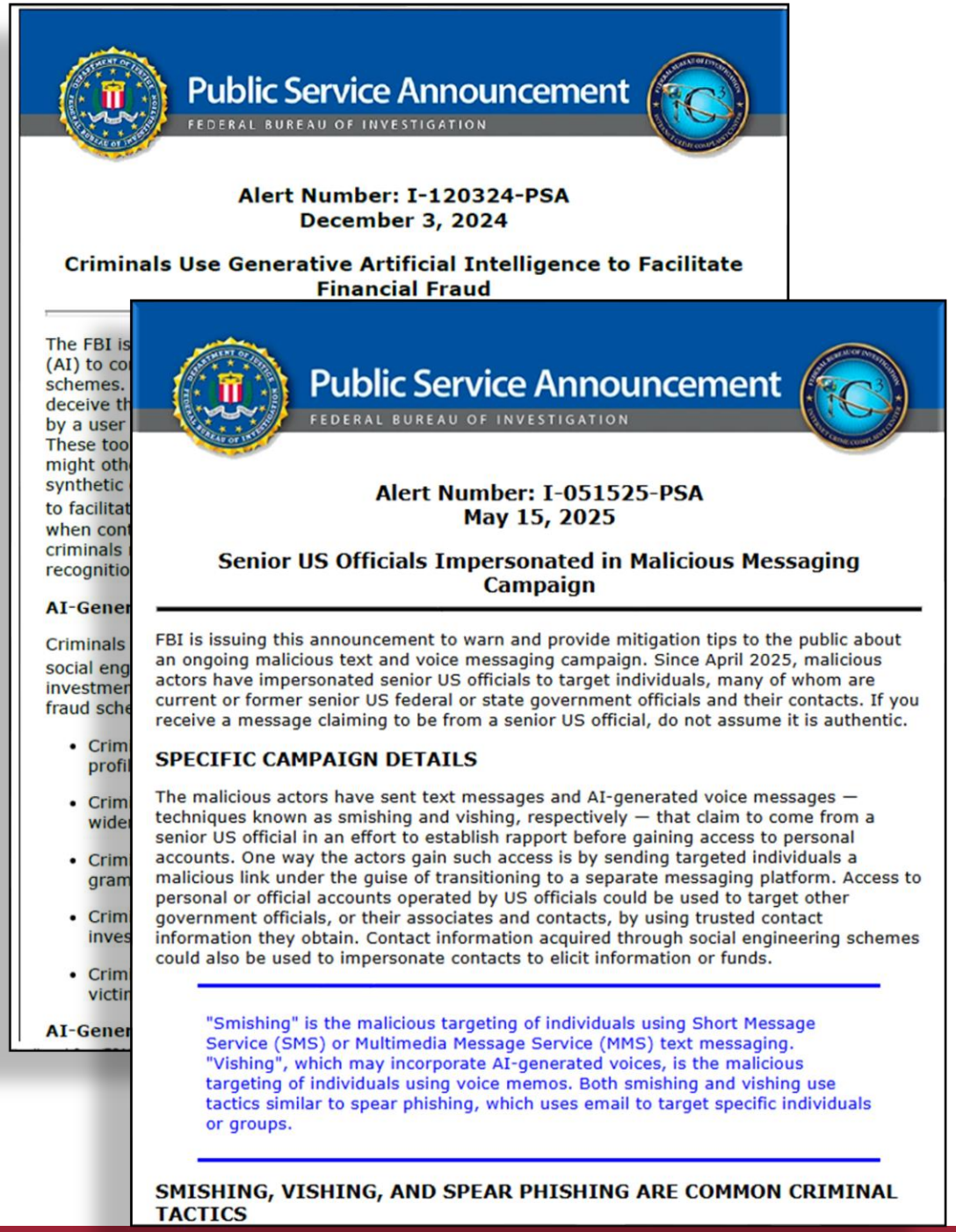
By Eduard Kovacs
April 4, 2025



Oracle is privately confirming to customers that some of its cloud systems have been breached, and is apparently trying to downplay the impact of the incident.

TRENDING

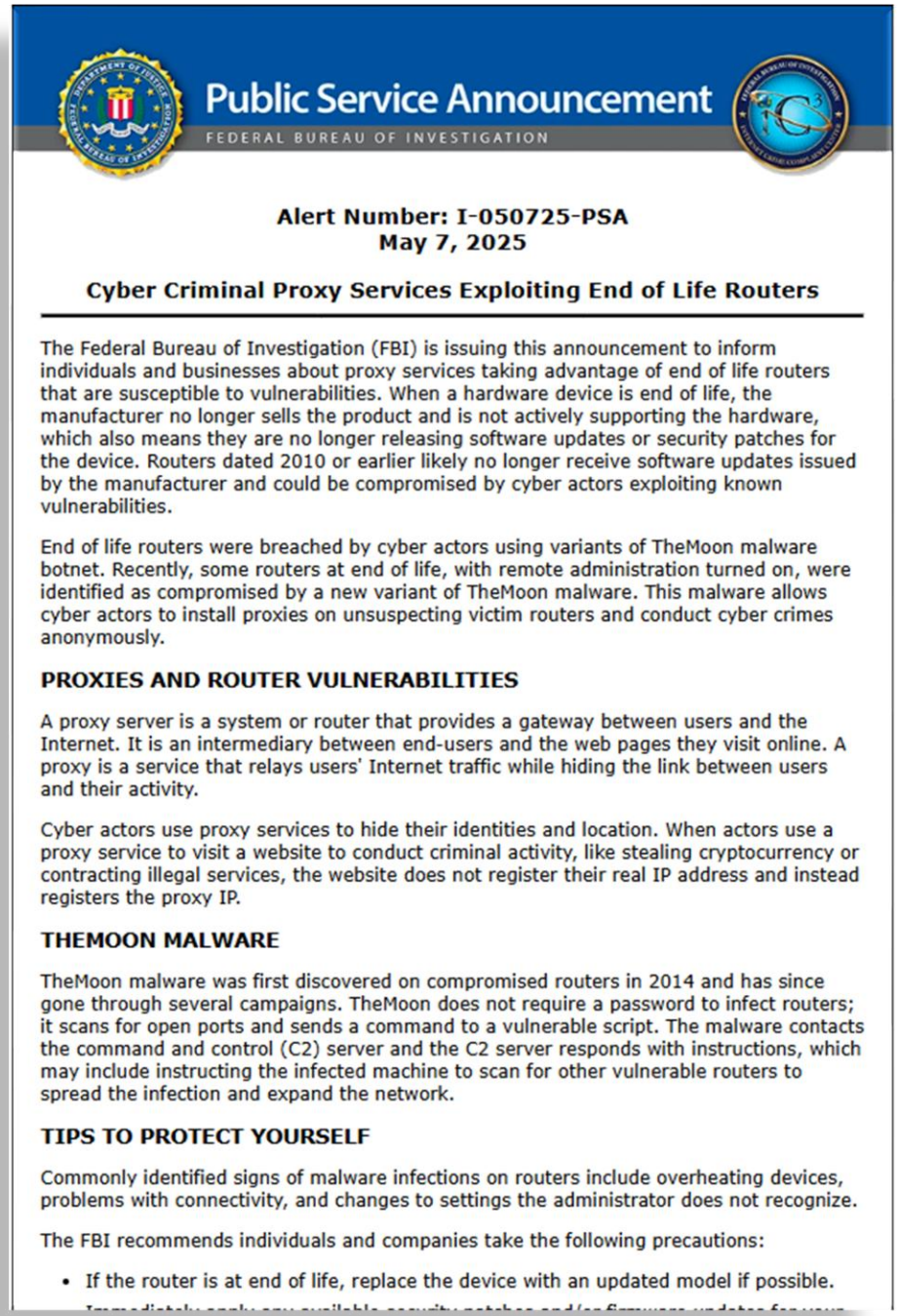
1. Oracle Confirms Cloud Hack
2. Call Records of Millions Exposed by Verizon App Vulnerability
3. Two CVEs, One Critical Flaw: Inside the CrushFTP Vulnerability Controversy
4. Critical Apache Parquet Vulnerability Leads to Remote Code Execution
5. State Bar of Texas Says Personal Information Stolen in Ransomware Attack
6. Chinese APT Pounces on Misdiagnosed RCE in Ivanti VPN Appliances
7. Halo ITSM Vulnerability Exposed Organizations to Remote Hacking



Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud

- AI-Generated Text
- AI-Generated Images
- AI-Generated Audio, aka Vocal Cloning
- AI-Generated Videos

American Hospital Association™
Advancing Health in America



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-050725-PSA
May 7, 2025

Cyber Criminal Proxy Services Exploiting End of Life Routers

The Federal Bureau of Investigation (FBI) is issuing this announcement to inform individuals and businesses about proxy services taking advantage of end of life routers that are susceptible to vulnerabilities. When a hardware device is end of life, the manufacturer no longer sells the product and is not actively supporting the hardware, which also means they are no longer releasing software updates or security patches for the device. Routers dated 2010 or earlier likely no longer receive software updates issued by the manufacturer and could be compromised by cyber actors exploiting known vulnerabilities.

End of life routers were breached by cyber actors using variants of TheMoon malware botnet. Recently, some routers at end of life, with remote administration turned on, were identified as compromised by a new variant of TheMoon malware. This malware allows cyber actors to install proxies on unsuspecting victim routers and conduct cyber crimes anonymously.

PROXIES AND ROUTER VULNERABILITIES

A proxy server is a system or router that provides a gateway between users and the Internet. It is an intermediary between end-users and the web pages they visit online. A proxy is a service that relays users' Internet traffic while hiding the link between users and their activity.

Cyber actors use proxy services to hide their identities and location. When actors use a proxy service to visit a website to conduct criminal activity, like stealing cryptocurrency or contracting illegal services, the website does not register their real IP address and instead registers the proxy IP.

THEMOON MALWARE

TheMoon malware was first discovered on compromised routers in 2014 and has since gone through several campaigns. TheMoon does not require a password to infect routers; it scans for open ports and sends a command to a vulnerable script. The malware contacts the command and control (C2) server and the C2 server responds with instructions, which may include instructing the infected machine to scan for other vulnerable routers to spread the infection and expand the network.

TIPS TO PROTECT YOURSELF

Commonly identified signs of malware infections on routers include overheating devices, problems with connectivity, and changes to settings the administrator does not recognize.

The FBI recommends individuals and companies take the following precautions:

- If the router is at end of life, replace the device with an updated model if possible.

Threat actors exploiting EOL home routers

Access to:

- Networks
- Corporate Data
- PHI?

Do you have remote staff?

What controls are in place?

American Hospital Association™

Advancing Health in America

South Dakota
Association of Healthcare Organizations

Geopolitical Risk = Cyber Risk

American Hospital Association™
Advancing Health in America

News | Breaking News | Iran | Donald Trump | Cyberattacks | Terrorism | Israel | Dhs | War

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

Publishe

T h

Adviso

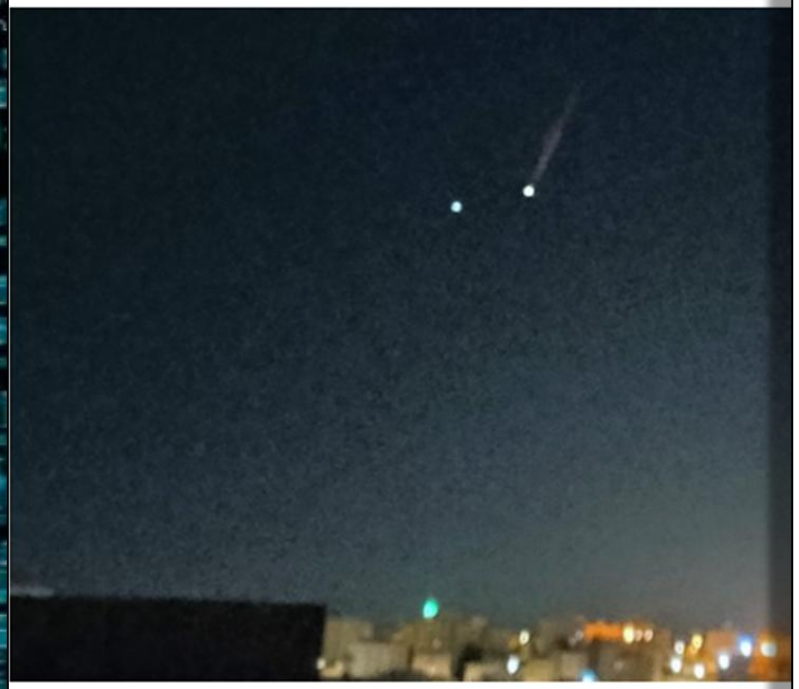
The po

Israel-Iran War: Hacktivist Groups' Claimed Activity Surges

While Exceptions Apply, Such Efforts Often Only Amount to Psychologi

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

Share | Tweet | Share



Two missiles visible in the sky over western Amman, Jordan, descending toward targets [illegible] 16, 2025. (Image:Malkawi99/CC BY-SA 4.0)

he "ongoing Iran conflict is

American Hospital Association™

Advancing Health in America

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

JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA24-242A

August 29, 2024

Co-Authored by:

MS-ISAC® Multi-State Information Sharing & Analysis Center®

#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 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 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).

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/tlp.

TLP:CLEAR

American Hospital Association® Advancing Health in America

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.

keystrike

Blog / The Unseen Storm: How China's Typhoon APT Groups Are Setting the Stage for Cyberwarfare

The Unseen Storm: How China's Typhoon APT Groups Are Setting the Stage for Cyberwarfare

April 17, 2025

American Hospital Association™

Advancing Health in America

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

American Hospital Association™

Advancing Health in America

CNN Politics SCOTUS

Chinese hac
worrying na

By Sean Lyngaas and
3 minute read · Up

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-042425-2-PSA
April 24, 2025

FBI Seeking Tips about PRC-Targeting of US Telecommunications

FBI is issuing this announcement to ask the public to report information about PRC-affiliated activity publicly tracked as "Salt Typhoon" and the compromise of multiple US telecommunications companies, especially information about specific individuals behind the campaign. Investigation into these actors and their activity revealed a broad and significant cyber campaign to leverage access into these networks to target victims on a global scale. This activity resulted in the theft of call data logs, a limited number of private communications involving identified victims, and the copying of select information subject to court-ordered US law enforcement requests.

FBI and US Government partners have previously released public statements on Salt Typhoon activity on 25 October 2024 and 13 November 2024, and published the guide, "Enhanced Visibility and Hardening Guidance for Communications Infrastructure," on 3 December 2024.

FBI maintains its commitment to protecting the US telecommunications sector and the individuals and organizations targeted by Salt Typhoon by identifying, mitigating, and disrupting Salt Typhoon's malicious cyber activity. If you have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you.

In addition, the U.S. Department of State's Rewards for Justice (RFJ) program is offering a reward of up to $10 million (USD) for information about foreign government-linked individuals participating in certain malicious cyber activities against US critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA).

If you have any information on Salt Typhoon, contact your local FBI field office, file a report on the FBI's Internet Crime Complaint Center at www.ic3.gov, or submit your tip to RFJ on Signal at +1-202-702-7843 or via the RFJ Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required).

American Hospital Association™

Advancing Health in America

Understanding the China Cyber Threat: An Urgent and Direct Threat to U.S. Health Care and National Security

February 13, 2025

1:00 – 2:00 pm Eastern

Register to Attend

"The goal i
that may c
governmer
out compr

POLITICO

COP29 War in Ukraine US elections | Newsletters Podcasts Poll of Polls Policy news Events

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

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

POLITICO

EUROPE

test news Commissioner hearings COP29 War in Ukraine US elections | Newsletters Podcasts Poll of Polls Policy news Events

Europe is under attack from Russia. Why isn't it fighting back?

THE TIMES

Chinese ship 'detained' after Baltic Sea cables were severed

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

Graphic by The Times and Sunday Times. Source: Marinetraffic

JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-249A

September 5, 2024

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure

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

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

April 5, 2024 TLP:CLEAR Report: 202404051700

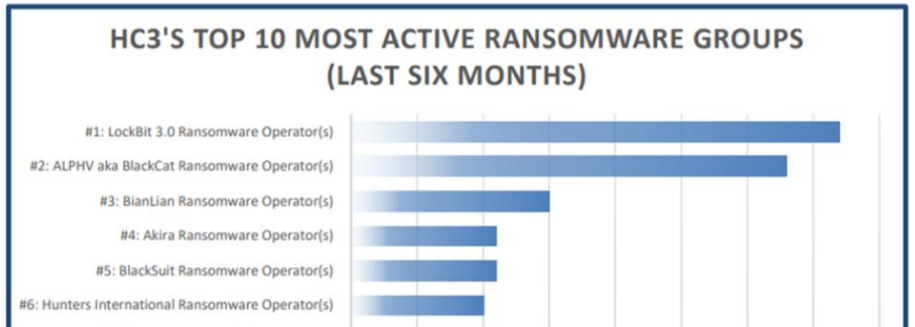
HC3's Top 10 Most Active Ransomware Groups

Executive Summary

HC3 monitors and tracks healthcare incidents across multiple platforms, including proprietary and open-source intelligence. As of mid-March 2024, in the last six months HC3 has tracked 730 attacks against the Healthcare and Public Health (HPH) sector worldwide. Of these attacks, more than 530 affected the U.S. HPH, and of those attacks, nearly half were ransomware related. This report provides high-level insight into the top ten ransomware groups HC3 has seen targeting the healthcare sector.

Report

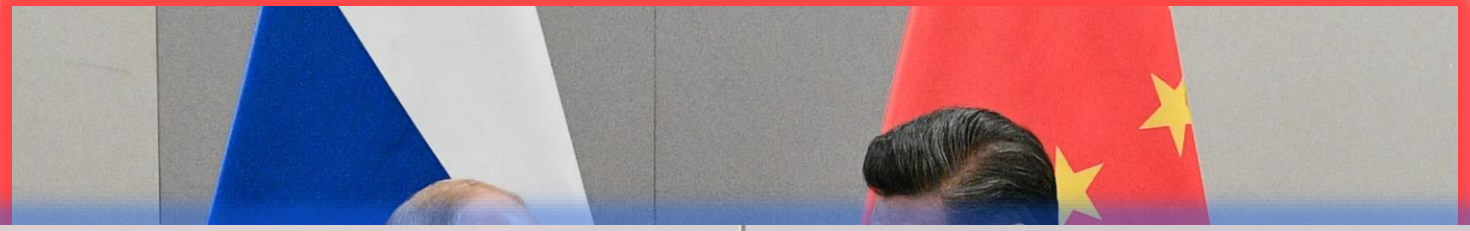
This chart shows the top 10 most active ransomware groups HC3 has seen targeting the U.S. HPH:

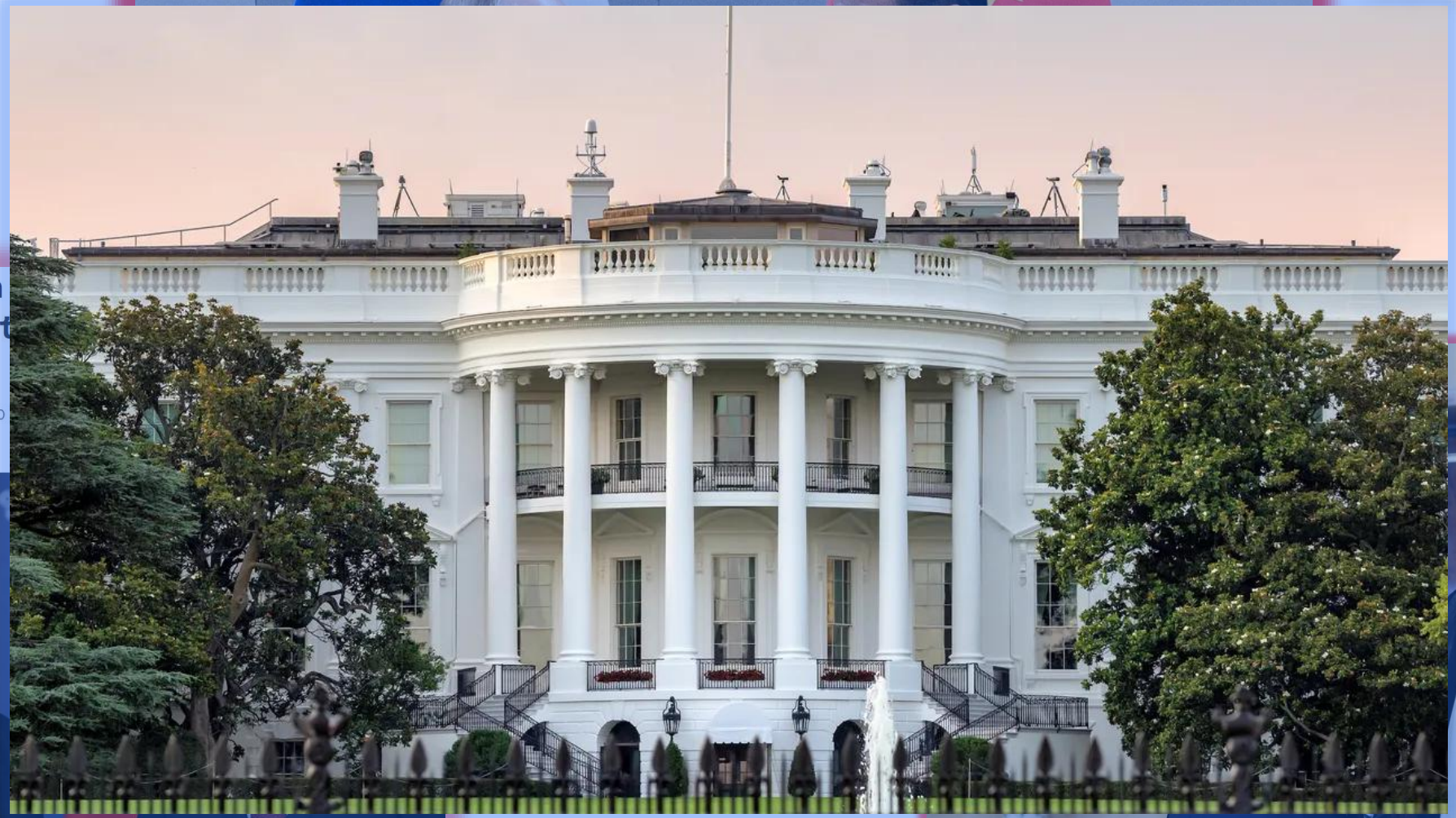


American Hospital Association™

Advancing Health in America

Threats that the Administration Must Manage





Putin and Kim
Korea, support
Ukraine

UPDATED JUNE 18, 2024 · 2:30

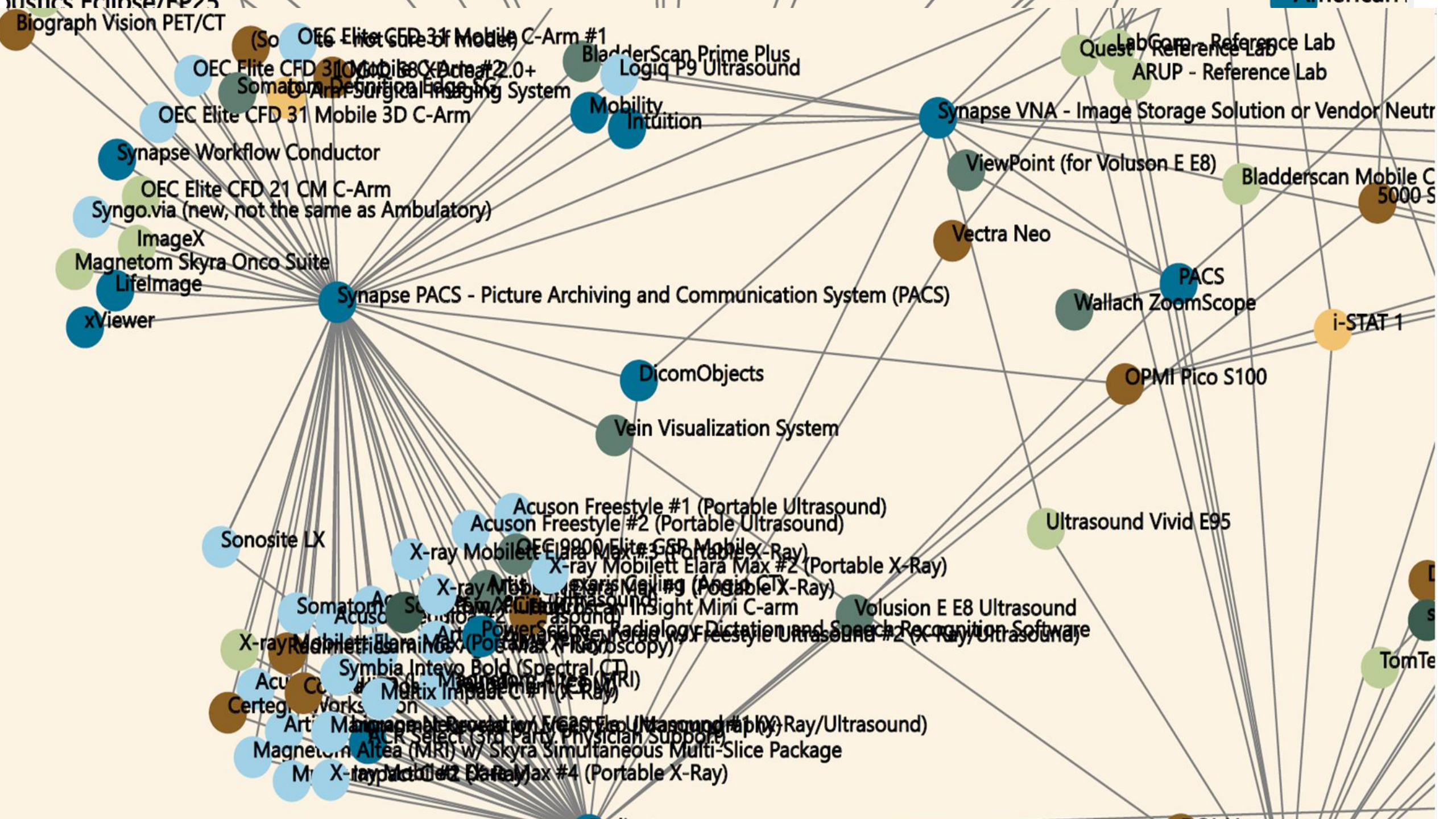
By Se Eun Gong

Cyber Attack Preparedness - The 5 R's

Regional Readiness, Response, Resiliency and Recovery

American Hospital Association™

Advancing Health in America


Biograph Vision PET/CT
OEC Elite CFD 31 Mobile C-Arm #1
BladderScan Prime Plus
Logiq P9 Ultrasound
Quest - Reference Lab
LabCorp - Reference Lab
ARUP - Reference Lab
Somatom Definition Edge SC
C-Arm Surgical Imaging System
Mobility
Intuition
OEC Elite CFD 31 Mobile 3D C-Arm
Synapse VNA - Image Storage Solution or Vendor Neutr
Synapse Workflow Conductor
ViewPoint (for Voluson E E8)
Bladderscan Mobile C
5000 S
OEC Elite CFD 21 CM C-Arm
Syngo.via (new, not the same as Ambulatory)
Vectra Neo
ImageX
Magnetom Skyra Onco Suite
LifeImage
PACS
Synapse PACS - Picture Archiving and Communication System (PACS)
Wallach ZoomScope
xViewer
i-STAT 1
DicomObjects
OPMI Pico S100
Vein Visualization System
Acuson Freestyle #1 (Portable Ultrasound)
Acuson Freestyle #2 (Portable Ultrasound)
Ultrasound Vivid E95
Sonosite LX
X-ray Mobilett Elara Max #3 (Portable X-Ray)
X-ray Mobilett Elara Max #2 (Portable X-Ray)
Insight Mini C-arm
Volusion E8 Ultrasound
Symbia Intevo Bold (Spectral CT)
Magnetom Altea (MRI) w/ Skyra Simultaneous Multi-Slice Package
X-ray Mobilett Elara Max #4 (Portable X-Ray)

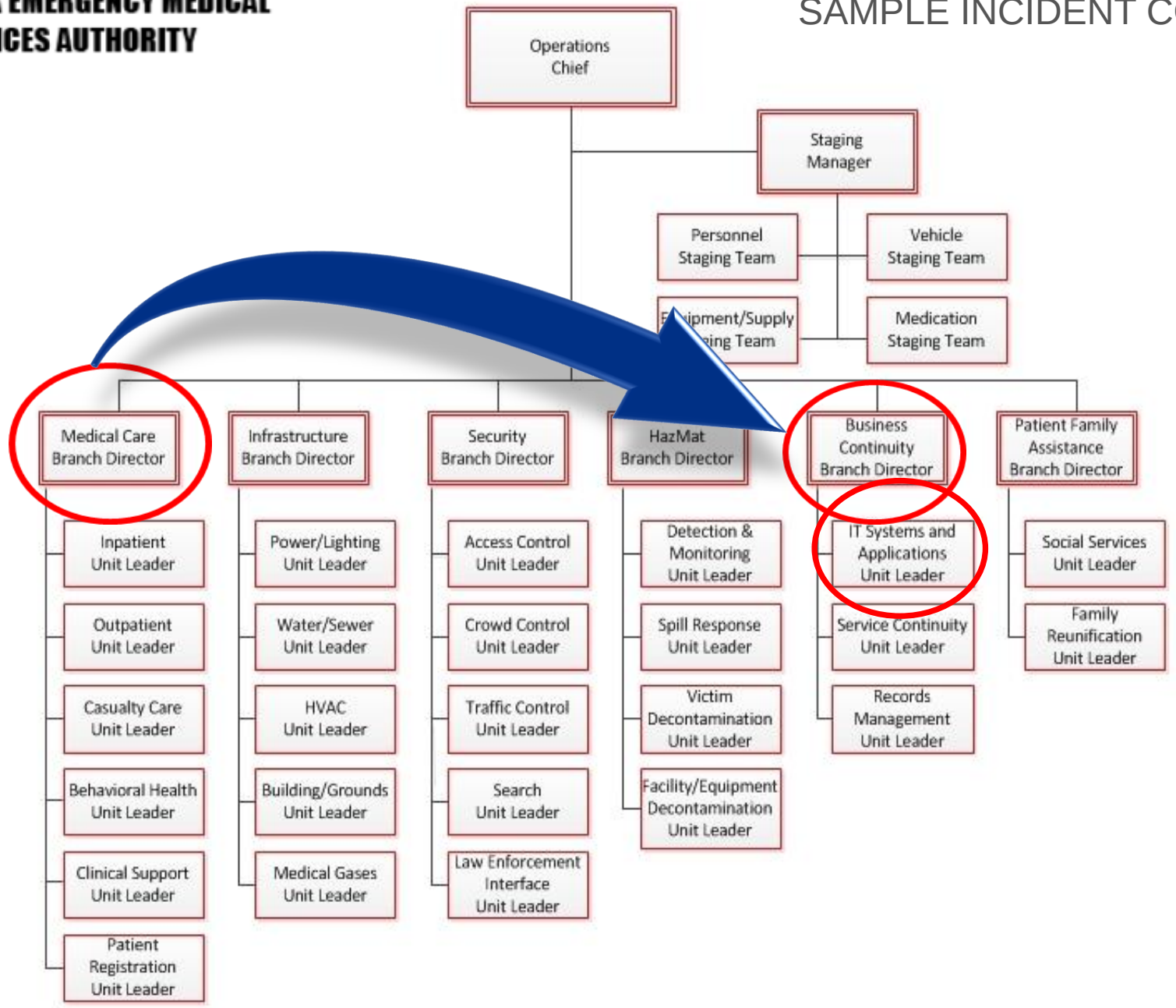
- Modern health care is vulnerable to disruption in many ways
- Preparation for technology outages like ransomware is critical
- Also applicable for non-malicious technology disruptions - like Crowdstrike
- The impact to patient care and safety are the same

"The question isn't if you will be attacked. The question is are you prepared?"

American Hospital Association™
Advancing Health in America

CALIFORNIA EMERGENCY MEDICAL SERVICES AUTHORITY

SAMPLE INCIDENT COMMAND CHART



American Hospital Association™

Advancing Health in America

Top Recommendations and Observations

INTEGRATE PLANS:

- Cyber incident response
- Emergency management
- Incident command
- Business continuity
- Disaster recovery plans
- Business continuity plans should specify plans for ***clinical continuity*** *during a loss of critical technology*

***READINESS, RESPONSE, RESILIENCY AND RECOVERY*:**

- Plans should be developed across the organization
- All system, hospital and department level actions and responses
- Including IT, operational, business and clinical functions
- Defined in the plan for the duration of the incident and for post incident recovery

REGIONAL, READINESS, RESPONSE, RESILIENCY AND RECOVERY:

- **REGIONAL** cyber incident response and communication plans
- Leverage existing emergency preparedness plans and mutual aid agreements
- Plans should accommodate **diversion of patients** and functions between facilities
- **Provide assistance to impacted facilities** - surge personnel, communications, medical devices and technology
- Regional facilities will also face increased strain or collateral impact

Top Recommendations and Observations

ENHANCE DOWNTIME PROCEDURES: BE ABLE TO SUSTAIN OPERATIONS FOR UP TO 4 WEEKS

- Be prepared to sustain clinical and business operations for up to 4 weeks
- For *every* **life critical, mission critical and business critical system and technology**
- Practice clinical, operational, financial and administrative downtime processes on all shifts
- *Ensure downtime supplies are in place or external printing arrangements have been made to continue operations and care delivery through manual procedures in the event of a loss of all medical, information and operational technology.*

IDENTIFY MISSION CRITICAL THIRD PARTY SERVICES:

- Establish downtime procedures if their services are unavailable
- Include cloud and technology service providers
- Determine clinical, operational and information technology impact if their services become unavailable
- Establish compensating on-premises downtime procedures, including manual procedures and backup strategy

DESIGNATE DOWNTIME COACHES AND DOWNTIME SAFETY OFFICERS FOR EACH SHIFT:

- Loss of access to the EMR may cause disruption and delay to healthcare delivery
- Staff may not be proficient in manual downtime procedures
- Loss of embedded safety and treatment protocols in the EMR may pose risk to patient safety

Top Recommendations and Observations

NETWORK BACKUP STATUS, SEGMENTATION AND SECURITY

- Recommend regular cadence of vulnerability and penetration testing of backups
- Review, document and communicate estimates of network restoration time
- Implement immutable backup solution as part of 3-2-1 backup strategy. 3-2-1**+1 immutable backup copy**

DOCUMENT ROLES WHICH HAVE DESIGNATED AND DELEGATED AUTHORITIES

- Authorized to make independent, high impact decisions during a cyber incident/crisis
  - Disconnection of the organization from internet
  - Shutting down of large parts of the network
  - *Defined* urgent circumstances. (**D**ocument **D**esignate and **D**elegate authorities)
  - Board notifications, authority and involvement?

DEFINE TRIGGERS:

- Facts and circumstances triggering high impact decisions
- Specify leadership escalation, incident command activation and staff notification protocols
- Trigger examples: indication that ransomware is spreading or beaconing to external C2, ongoing data exfil

DEFINE IMPACT TO LIFE CRITICAL, MISSION CRITICAL AND BUSINESS CRITICAL DEVICES AND SERVICES:

- Map clinical, operational and administrative impact of shuting down internal network or internet connection
- Document impact, incorporate in incident response plan
- Communicate to leadership

Top Recommendations and Observations

DEFINE EXTERNAL DEPENDENCIES, IMPACT:

- Especially external clinical dependencies
- Who depends on you?
- What would impact of an attack on your organization and loss of your network on them?
- Impact to other hospitals in the region, clinics and homecare telemetry?

REVIEW CYBER INSURANCE COVERAGE:

- Determine sufficiency of coverage based upon risk profile and current cybersecurity posture
- Determine proficiency of incident response assets and your confidence in them prior to an incident
- Review “act of war” exclusion given current geopolitical events
- Keep coverage information secured, preferably off network to prevent adversary discovery

REVIEW BAAs FOR BREACH NOTIFICATION, INSURANCE REQUIREMENTS:

- Determine to whom breach is to be reported 24/7 and timeline
  - 24 – 72 hours for data theft
  - Immediate for ransomware, including weekends and off hours
- **Test!**
- Ensure cyber insurance requirements scale with level of cyber risk presented by the BA

South Dakota
Association of Healthcare Organizations

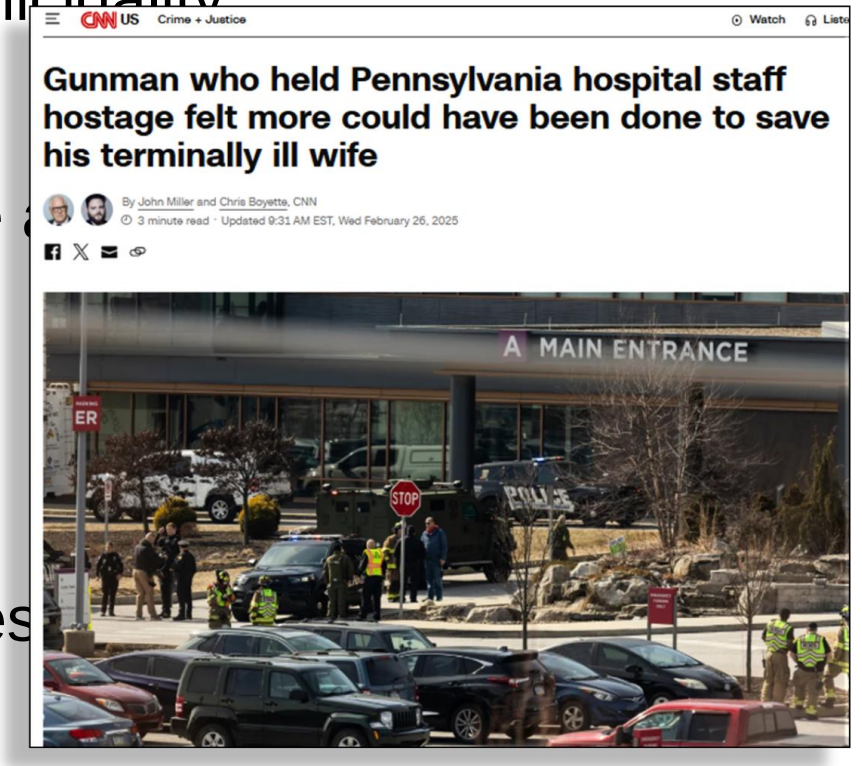
Physical Security and Risk

American Hospital Association™
Advancing Health in America

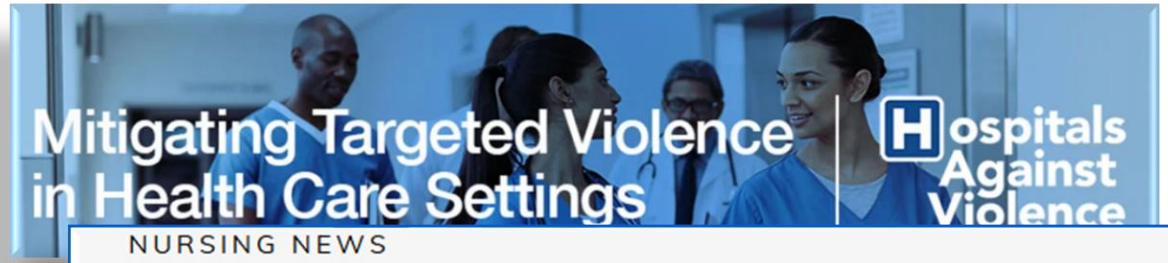
Physical Threats Targeting Health Care

1. Targeted violence against staff and executives increasing – murder of United Healthcare CEO Brian Thompson.
   - Perceived grievances by patients and staff
   - The tipping point – from thought to the first physical action step
   - The connection between suicidality and homicidality
   - Online threats to physical threats
   - Extremist threats and mistrust of health care a future political environment
   - The SAVE Act

2. Executive protection risk assessment and measures



Our Work With the FBI – AHA HAV and Cyber and Risk



NURSING NEWS

Save Healthcare Workers Act Would Make Violence Against Healthcare Workers a Federal Crime

- The Save Healthcare Workers Act would implement federal penalties for those who knowingly assault healthcare employees.
- The bipartisan bill, introduced in the House and Senate, would be the first to establish assault on a healthcare worker as a federal crime.
- Penalties would range from fines to up to two decades in prison, depending on the severity of the attack.

KARI WILLIAMS
Nursing CE Central

MAY 19, 2025

AHA | FBI RESOURCES

PODCAST

FBI Violence Prevention Strategies to Assess and Manage Threats Against Health Care

Explores the meaning of threat assessment and threat management (TATM) teams and how it applies to the threat of violence against hospitals and health care teams.

Listen

FBI RESOURCE

U.S. Department of Justice - FBI's Behavioral Analysis Unit. Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks

A practical guide on assessing and managing the threat of targeted violence containing concrete strategies to help communities prevent these types of incidents.

Learn More

ISSUE BRIEF

Mitigating the Risk of Violence

Shares considerations when assessing potential risks, strategies to mitigating violence and insights on making the care environment safer.

Download

FBI RESOURCE

Active Shooter Planning and Response in a Healthcare Setting

Provides guidance on how to prepare and respond to an active shooter in health care and includes law enforcement tactics and integrated medical and mental health response.

Learn More

Workforce and Workplace Violence Prevention Resources

Cybersecurity

CONVENING LEADERS FOR EMERGENCY AND RESPONSE

The CLEAR Field Guide for Preparedness

FBI's Prevent Mass Violence Initiative

https://www.aha.org/mitigating-targeted-violence-health-care-settings

American Hospital Association™
Advancing Health in America

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 Security Rule rewrite

South Dakota
Association of Healthcare Organizations

Discussion – Thoughts on Changes?

Scott Gee

sgee@aha.org

American Hospital Association™
Advancing Health in America