

Cyber Threat Landscape: Risk, Impact and Preparedness – Part Two

**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

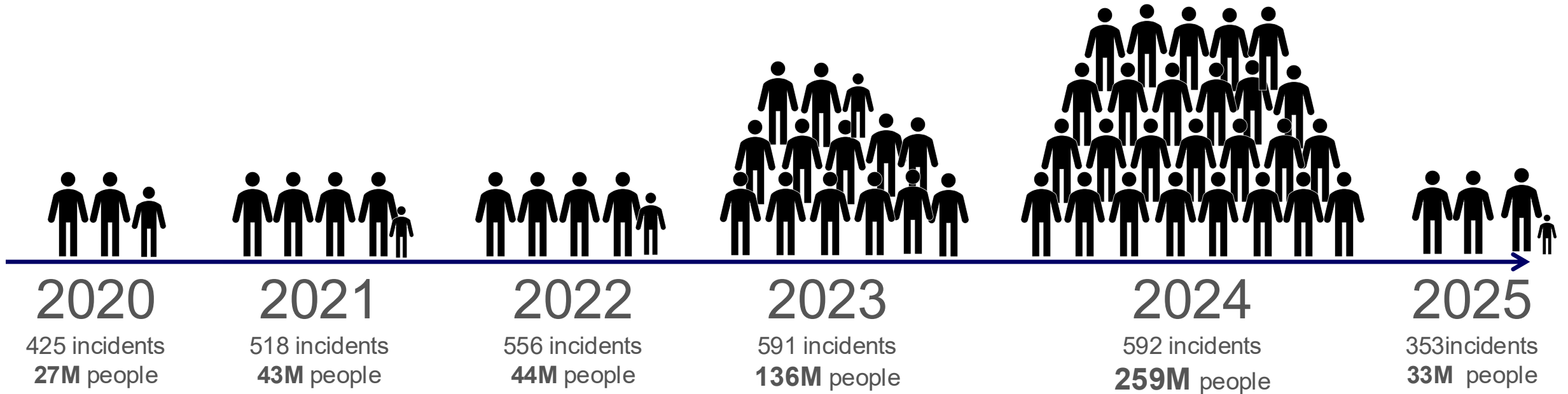
October 1, 2025




Preparedness for Clinical Continuity

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
		364 Incidents	33,289,884	Individuals impacted		

RANSOMWARE ATTACK AT UMC

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.

Data breach at Yale New Haven Health impacts 5.6M people

It's the largest healthcare breach

Published April 24, 2025

 **Emily Olsen**
Reporter

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

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

by Caden DeLisa | Aug 2, 2024

A cyberattack has disrupted hospitals
and health care in several states

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

Volpenhein

Wisconsin Journal Sentinel

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

BY PAT EATON-ROBB
Updated 8:35 PM EDT, August 4, 2023

AP

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

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

U.S. NEWS

Cyberattack hits 2 New York hospitals forces ambulance diversions

Great Plains Regional Medical Center Victim of Ransomware Attack

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 Jacques Hospital in Newburyport, Massachusetts, has recently notified regulators and patients about a cyberattack and data breach that occurred on Christmas Day in 2023.

Kidney Dialysis Services Provider DaVita Hit by Ransomware

DaVita has not named the ransomware



By **Ianut Arghire**
April 15, 2025



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

- Radiology / Imaging / PACS down - other diagnostic technology lost. Remote radiology lost. All could lead to stroke and trauma diversion
- Cath lab down = heart attack diversion
- **Risk to patient safety. ED's shutdown - Ambulances placed on full divert - rural distance** delay of emergency treatment. Trauma Center availability
- **Telemetry systems inoperable** – additional staff required for patient monitoring - Home health care telemetry. *Patients at home, greater risk?*
- **EHR rendered inaccessible.** Patient history, treatment protocols, drug allergies / interactions unknown – delay in rendering care
- Lab and Pathology disrupted
- Elective **surgeries** cancelled
- **ADT** forms and instructions unavailable
- **Drug cabinet/ pharmacy** systems down
- **Loss of VoIP phones and email systems**
- **Ransomware “blast radius” – effect on other providers who are dependent** for ED, EMR, labs, imaging, cancer treatment and other third parties also disrupted.
- **Regional impact** and stress based upon **capacity** of surrounding hospitals
- Simultaneous loss of all network and internet connected information, medical and operational technology – **Downtime computers lost or limited data.**
- **ED wait times significantly increased.**



- Radiation oncology (RADONC) treatment may be dependent upon network and internet connected technology.
- Extended delay of treatment when diverted to alternate RADONC treatment facilities.
- **Chemotherapy** and RADONC treatment plans may not be available.
- **Staff unprepared for extended clinical downtime procedures functions and paper EMR charting lasting up to three months.**
- **Three to four week recovery time for mission critical systems paid or not, residual impacts lasting 6 months - 2 years**
- **Backups corrupted or only 65% restoration from uncorrupted backups. RTO and RPO not fully understood.**
- Legacy systems unrecoverable
- **Revenue** interruption and revenue **loss** due to incomplete **days cash on hand – no income for 60 days.**
- **Scheduling, timekeeping and payroll systems disrupted**
- **Operational and physical security technology impact,**
- **Third parties** requesting independent certification before reconnection
- Increased **insurance** premiums or loss of coverage
- **Civil liability** for publicly released PHI or negative outcome
- State and federal **regulatory liability + Reputational Harm**

Cost per day for healthcare

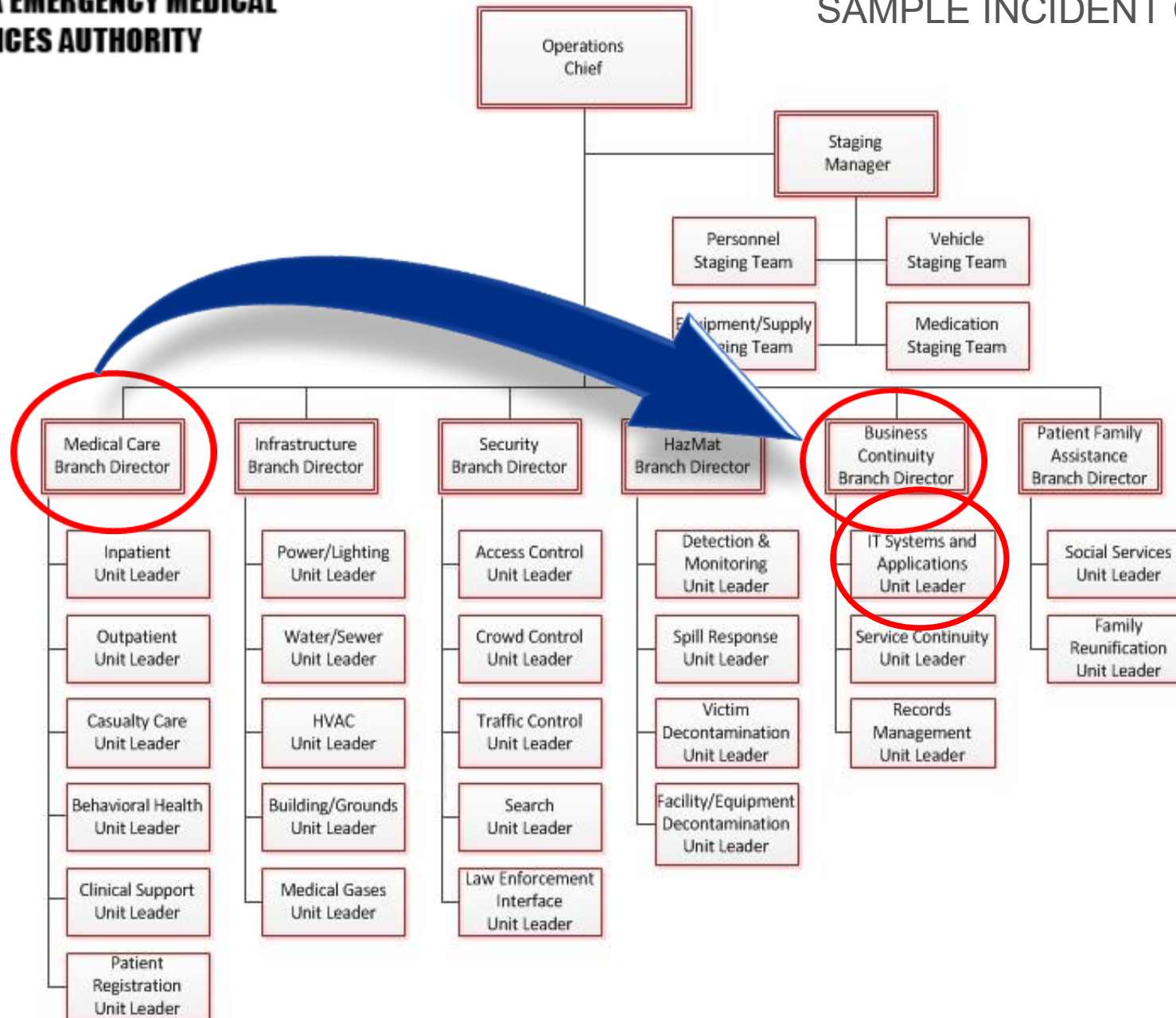
\$1.9
million

Estimated amount lost by healthcare organizations on average per day of downtime following ransomware attack from 2018-2024, per Comparitech³².



CALIFORNIA EMERGENCY MEDICAL SERVICES AUTHORITY

SAMPLE INCIDENT COMMAND CHART



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 shutting 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



PROTECT YOUR ORGANIZATION'S RESILIENCY WITH AHA'S CLINICAL CONTINUITY ASSESSMENT PROGRAM

How Would You Provide Care for 30 Days Without Technology?

With cyberattacks against hospitals and mission-critical third-party providers escalating in both frequency and severity, it's an unfortunate reality that continued attacks are inevitable. Not only do these incidents represent data theft and financial crimes, but for hospitals, they are threat-to-life crimes designed to shut down vital systems and cause maximum delay and disruption to patient care.

How prepared is your hospital to continue providing life-saving care during an extended disruption? Given the prevalence of attacks and the disruption caused by ransomware, ensuring that your hospital can continue to provide safe and quality care without critical technology for at least 30 days is not just an option: It's a necessity.

The **AHA Clinical Continuity Assessment Program** helps you evaluate your hospital's readiness to maintain patient care during such disruptions. Led by our team of nationally recognized and uniquely experienced health care cybersecurity experts, this comprehensive assessment provides the insights, recommendations and structure needed to ensure your organization can function without access to mission-critical and life-critical technology.



What We Do

Our trusted experts help you understand how well your hospital is prepared to maintain critical clinical and operational functions during a cyberattack. Our Clinical Continuity Assessment Program goes far beyond traditional cybersecurity checks; we dig deep into plans, conduct interviews and visit care sites. Leveraging our experience in assisting hundreds of ransomware victims, we provide specific strategic and operational recommendations across all functions — to maintain clinical continuity and business resiliency during prolonged outages.



“ The question isn't if an attack will happen.
The question is: are you ready? ”

— John Riggi

National Advisor for Cybersecurity and Risk for the American Hospital Association (AHA)



AHA CLINICAL CONTINUITY ASSESSMENT PROGRAM

“The question isn’t if you will be attacked. The question is are you prepared?”





Discussion and Questions

Scott Gee
sgee@aha.org