Monthly Cyber Briefing

December 4, 2025

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Healthcare's Monthly Cyber Briefing

Agenda + Speakers:

- Cyber Update
- 2025 in Review: What the Breaches, Threats, and Data Tell Us Now
- Q+A

Dave Bailey, VP of Security Services, Clearwater

Steve Akers, CTO & Corporate CISO, Clearwater

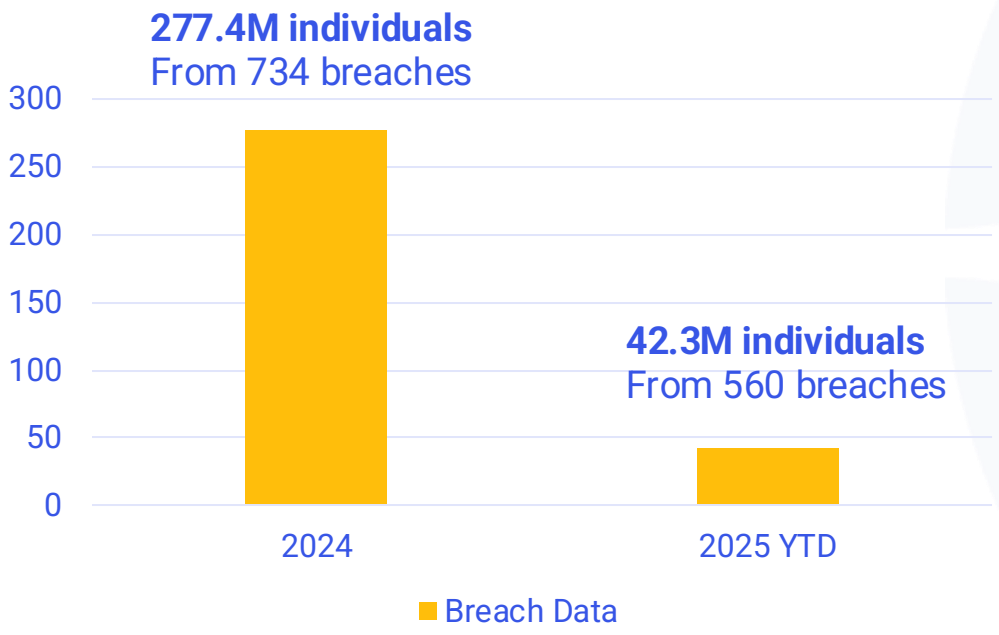
Healthcare Industry Threat Information

Relevant Threat Information for Healthcare
Nov 2025

Clearwater | Google Threat Intelligence

14 Breaches Added Since Oct

Breach Data Dashboard



1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 11/30/25, pulled 12/2/25)

Insights:

- **456** of the 560 reported breaches are currently under investigation
- **3** of the 14 added were Business Associates

Class Action Trend

- **June 2025 -** Newly emerged ransomware group emerged Kawa4096
- **July 17th** - WICHITA, Kan. (KWCH) - Susan B. Allen Memorial Hospital is investigating a potential cyberattack after patients reported they couldn't reach the facility to schedule critical appointments.
- **Jul 22nd** – Kawa4096 uploaded data to its data leak site alleging to have stolen 210GB of data
- **July 25th** - Susan B Memorial Hospital was hit with a data breach class action

Clearwater

2025 Enforcement By the Numbers

Total cyber-related enforcement actions

14

12

Cite failure to conduct an accurate and thorough risk analysis.

$3M

Highest fine: Solara Medical Supplies

$486k

Average Fine

8 of 14

Involved ransomware

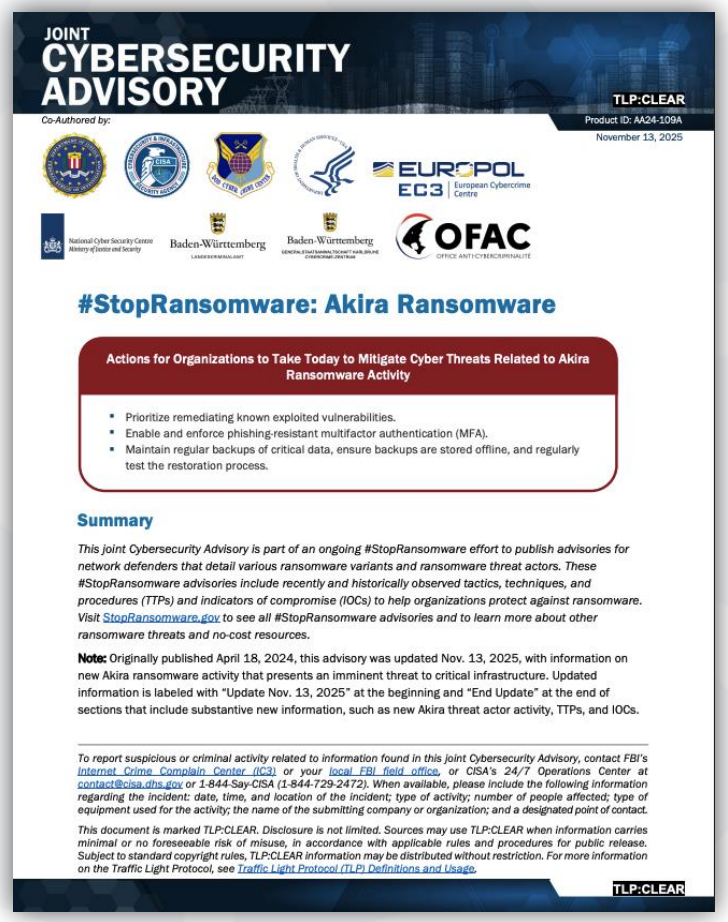
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Google Threat Intelligence Group (GTIG) collected intelligence surrounding a campaign by UNC6566 that leverages a Software Supply Chain Compromise

- **Activity:** observed between Nov 21st – 25th
- **UNC6566** is a threat cluster that conducts software supply chain attacks by distributing a trojanized npm package, identified as the "Shai-Hulud" worm, to **steal developer and cloud credentials**
- **Associated Malware**: **TRUFFLEHOG:** a commercial credential theft tool used to hunt for secrets on disk and in repositories.
- TTPs: mitre-attack
- Directly observed activity has impacted organizations in Canada and the **United States** and across the **healthcare**, legal & professional services, manufacturing, and retail industries

CISA published an **update** to its Akira ransomware advisory, explicitly flagging **new Akira activity** as an **imminent threat to critical infrastructure**

- **Akira** ransomware threat actors are associated with other groups known as **Storm-1567**, **Howling Scorpius**, **Punk Spider**, and **Gold Sahara**, and may have connections to the defunct **Conti** ransomware group. Akira threat actors primarily target small- and medium-sized businesses, but have also impacted larger organizations across various sectors
- Must DO's
  - Prioritize mitigating Known Exploited Vulnerabilities (KEV)
  - Implement phishing resistant MFA
  - Have effective offline backups



JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-109A
November 13, 2025

EUROPOL EC3 European Cybercrime Centre

National Cyber Security Centre Ministry of Justice and Security

Baden-Württemberg

Baden-Württemberg

OFAC OFFICE OF FOREIGN ASSETS CONTROL

#StopRansomware: Akira Ransomware

Actions for Organizations to Take Today to Mitigate Cyber Threats Related to Akira Ransomware Activity

- Prioritize remediating known exploited vulnerabilities.
- Enable and enforce phishing-resistant multifactor authentication (MFA).
- Maintain regular backups of critical data, ensure backups are stored offline, and regularly test the restoration process.

Summary

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.

Note: Originally published April 18, 2024, this advisory was updated Nov. 13, 2025, with information on new Akira ransomware activity that presents an imminent threat to critical infrastructure. Updated information is labeled with "Update Nov. 13, 2025" at the beginning and "End Update" at the end of sections that include substantive new information, such as new Akira threat actor activity, TTPs, and IOCs.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact FBI's Internet Crime Complain Center (IC3) or your local FBI field office, or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). 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.

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 Traffic Light Protocol (TLP) Definitions and Usage.

TLP:CLEAR

Clearwater Google Threat Intelligence

Ransomware Update

Impacts from Ransomware in November

Clearwater | Google Threat Intelligence

November Recorded the 3rd Highest Month of Ransomware Activity with Qilin Leading the Way

November ransomware activity shows **high operational intensity**, **actor diversification**, and a **heavy focus on outpatient medical organizations**

37

November concluded with **37** reported ransomware incidents against the U.S. healthcare sector across **hospitals, medical practices, dental offices, and behavioral health facilities.** While a decrease of 26% from the year high month of October (50), November recorded the 3rd highest month of activity YTD.

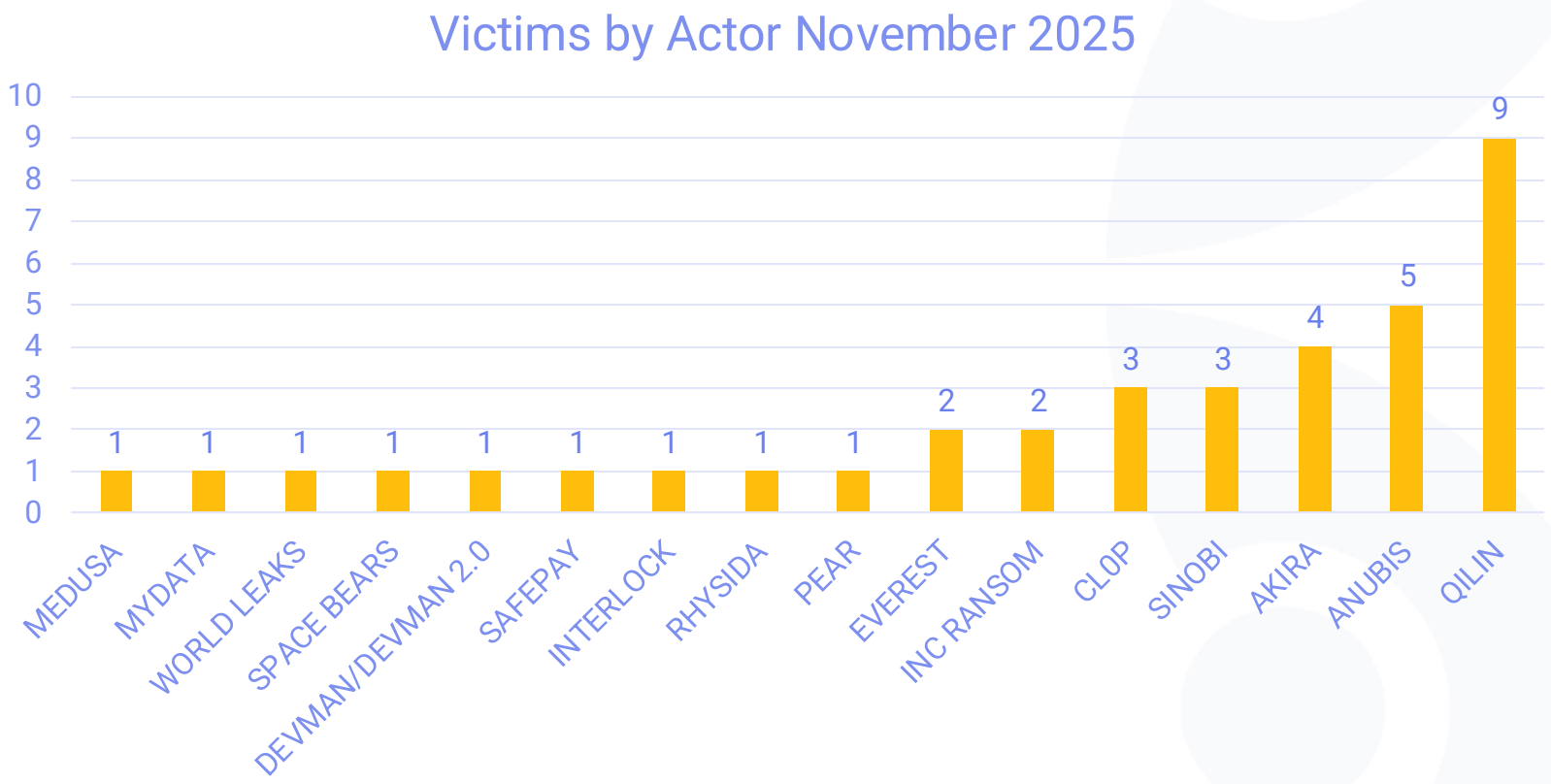
65%

Key ransomware operators—**Qilin, ANUBIS, Akira**, **CL0P**, and **Sinobi** —accounted for **65%** of total activity, underscoring sustained, coordinated targeting of healthcare networks and patient information systems.

Notable Nov Campaign Timelines

Clearwater Google Threat Intelligence

Ransomware Attacks Continue to Disrupt Operations, Delay Patient Care, and Expose Millions of Patient Records



Industry Focus:

- **Medical Practice Focus**: Increase in attacks on mid-size organizations and other healthcare business
- **Dominance in Data Exfiltration**: Data theft is a critical component with many groups abandoning encryption
- **Geographic Concentration**: The U.S. remains the country with the highest number of ransomware attacks on healthcare orgs

A Fast Start to December:

- December has already claimed (3) victims
  - (1) **Inc Ransomware**
  - (1) **Sinobi**
  - (1) **DevMan**

Clearwater Google Threat Intelligence

ANUBIS Makes Returns in November With 5 Victims and Qilin Continues to Lead in Victim Count

ANUBIS

- The ANUBIS data leak site (DLS) is operated by the ANUBIS Ransomware-as-a-Service (RaaS) group, which emerged in February 2025
- The group employs "non-standard methods" to pressure victims into paying ransoms, including informing regulatory bodies and victims' clients about the breach and publicizing their activities on platforms like X (formerly Twitter)
- Unlike many ransomware actors, ANUBIS meticulously details the stolen data in its leak posts, emphasizing sensitive information to further coerce and shame victims
- It is important to note that there is also an unrelated ANUBIS malware family

Qilin

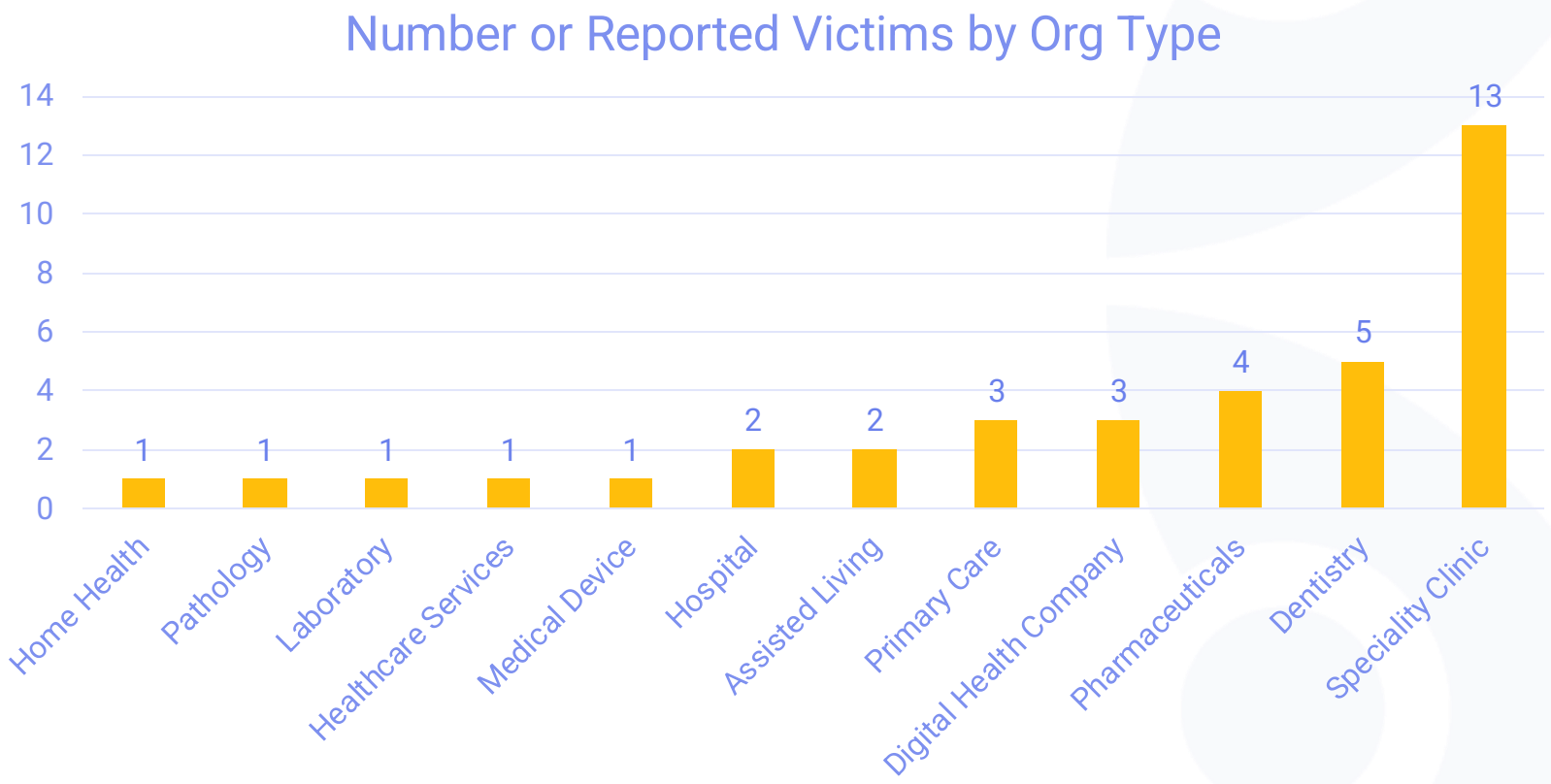
- The Qilin ransomware group, active since at least August 2022, operates a ransomware-as-a-service (RaaS) model, employing **double extortion tactics**: The ransomware used is known as “Agenda”
- Recently enhanced its offerings to affiliates, introducing a "Call Lawyer" feature in early May 2025
- Introduced a distributed denial-of-service (DDoS) capability in April 2025. Other planned features include a DDoS panel, an email spamming tool, a call/SMS spamming tool/service, and the involvement of journalists.
- Initial access is typically gained through leaked credentials via a virtual private network (VPN), followed by the deployment of tools like Cobalt Strike and Mimikatz for persistence and further credential theft

Ransomware Targeting Patterns

Impacts from Ransomware in October

Clearwater | Google Threat Intelligence

Specialty Clinics Hit Hardest During November

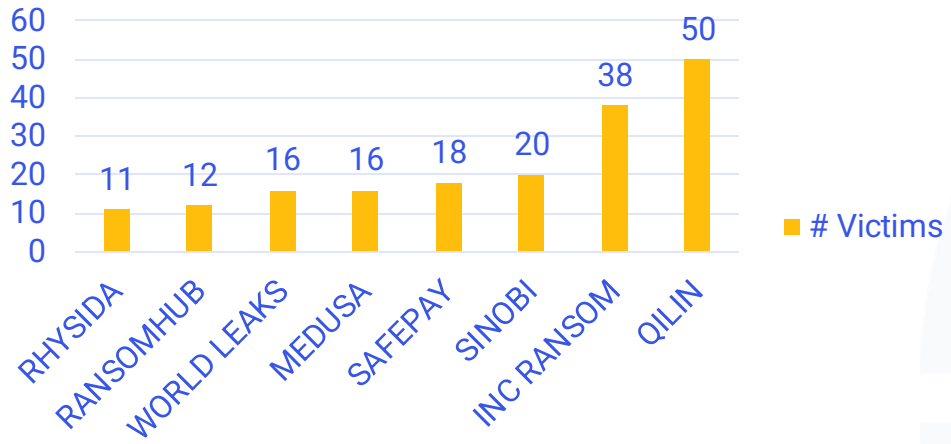


Industry Focus:

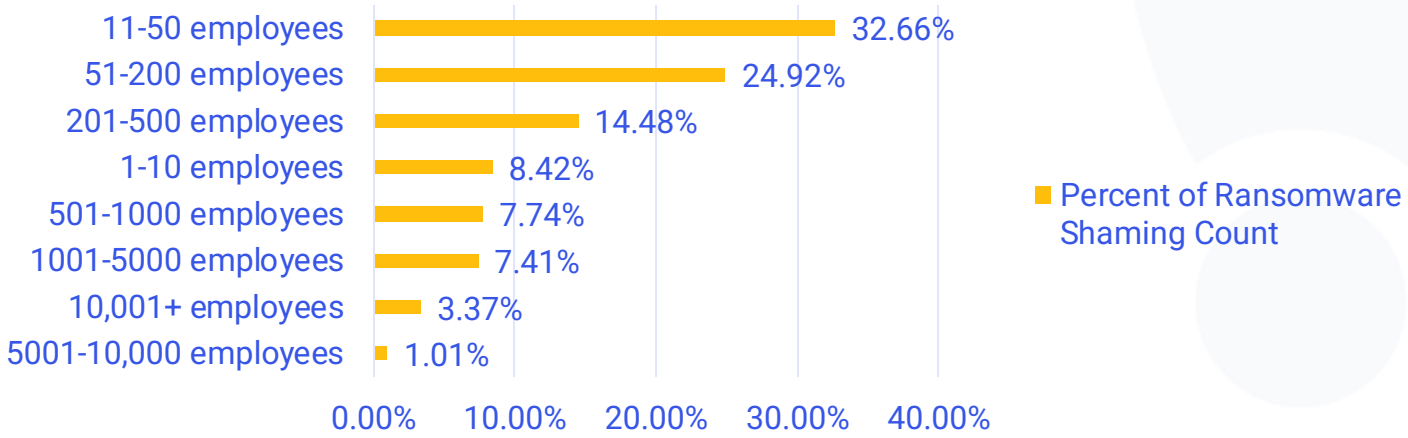
- **Medical Practice Focus**: Continued increase in attacks on mid-size organizations and other healthcare business
- **Dominance in Data Exfiltration**: Data theft is a critical component with many groups abandoning encryption
- **Geographic Concentration**: The U.S. remains the country with the highest number of ransomware attacks on healthcare orgs

2025 Outcome is Dominated by Ransomware

Top 8 Threat Actors (YTD)



% Victims by Employee Size (YTD)



YTD
324 Victims
57 Threat Actors

Clearwater

Google Threat Intelligence

Sector Updates

HHS Focus on Cybersecurity

Clearwater | Google Threat Intelligence

Relevant Updates From the HSCC CWG

Health Sector Publishes **Updated Cybersecurity Model Contract**
The HSCC Cybersecurity Working Group (CWG) of the Healthcare and Public Health Sector Coordinating Council (HSCC) published an updated reference for shared cooperation and coordination between Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) regarding the security, compliance, management, operation, and services of medical technology in the clinical environment

Health Sector Publishes **Previews to AI Cybersecurity Guidance**
This series of one-page summaries of five separate HSCC Cybersecurity workstreams on Artificial Intelligence offers a preview of best practices and white papers that the Cybersecurity Working Group will publish in 2026 about A.I.:

1) Education and Enablement
2) Cyber Operations and Defense
3) Governance
4) Secure by Design
5) Third Party Risk and Supply Chain Transparency.

Clearwater

Recommended Actions for Healthcare Organizations

Focus Area	Actions
Strengthen Access & Identity Controls	▪ Enforce MFA on all accounts, especially remote access, VPNs, RDP and admin ▪ Limit external remote access to minimum necessary; strong RBAC ▪ Monitor & restrict third-party/vendor access
Vulnerability Management & Patch Hygiene	▪ Maintain a robust vulnerability management program ▪ Prioritize patching ▪ Ensure secure configuration of devices and hardening
Backup, Disaster Recovery & Resilience	▪ Maintain immutable, offline, air-gapped backups ▪ Regularly test backup restorations (table-top and live tests) ▪ Maintain an incident response plan for ransomware
Detection & Monitoring	▪ Deploy advanced endpoint detection & response (EDR) ▪ Have continuous monitoring of events ▪ Use threat intelligence to monitor for TTPs
Network Architecture & Segmentation	▪ Segment critical clinical networks ▪ Harden and monitor network boundaries ▪ Logically isolate backups
Vendor & Third-Party Risk Management	▪ Assess cybersecurity posture of vendors, MSPs, medical-device suppliers ▪ Require vendor access to be tightly controlled ▪ Include in contracts obligations for incident reporting, security reqs, and audits

Healthcare's Cyber Briefing

2025 in Review: What the Breaches, Threats, and Data Tell Us Now

Steve Akers, CTO & Corporate CISO, Clearwater

2025 Predictions – Review

- Common Threads
  - AI in everything
  - Ransomware and Extortion will evolve
  - More vulnerabilities than ever before
  - Quantum
  - Supply Chain
  - New Tech to Save the Day (again)

2025 Predictions – AI

Predictions
Threat actors will leverage AI more for attacks
▪ More Social Engineering
▪ Phishing
▪ Vishing
▪ Deepfakes
▪ Voice and Video Enabled with AI
Faster and Automated Exploitation

2025 Activity Analysis

16.7%
Increase in automated scans activity

36K
Scans Per Second

500%
Increase in logs from compromised systems

Risk Impact to Healthcare based on 2025:

Likelihood: ↑ Impact: ↑

Accuracy Analysis

★★★★★

Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Ransomware

Predictions
No Slow Down in Attacks
Tactics Will Change – move beyond encrypt only
▪ Data Harvesting
▪ Complex Extortion Schemes
▪ Leak Only Attacks
▪ CaaS – Cybercrime as a Service
▪ Apply Regulatory Exposure Pressure
▪ AI Will Drive evolution

2025 Activity Analysis

146%
Increase in attempts

5 Mins
Prep time for Campaign down from 16 hours

1/6th
Of breaches involved use of generative AI

Risk Impact to Healthcare based on 2025:

Likelihood: ↑ Impact: ↑

Accuracy Analysis

★ ★ ★ ★

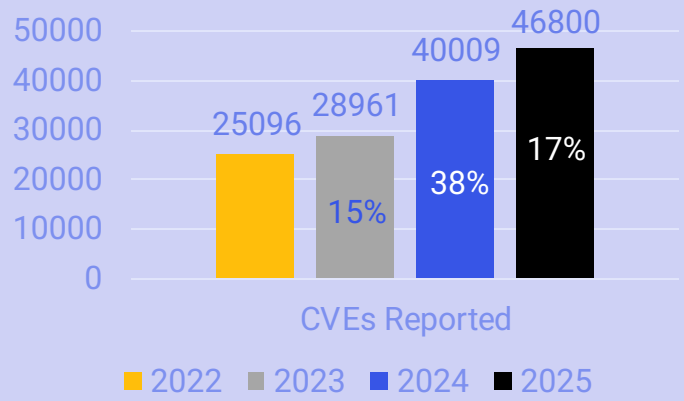
Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Vulnerabilities

Predictions
Number of Vulnerabilities will be largest ever
More Critical and Highs Reported
Exploitation time will be reduced

2025 Activity Analysis



42,924

CVE's in 2025 so far

>24

Hours for 28% of exploits

Risk Impact to Healthcare based on 2025:

Likelihood: ↑ Impact: ↑

Accuracy Analysis

★ ★ ★ ★

Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Quantum

Predictions
Expected impact of Quantum will drive initiatives
Potential for Y2K “Like” Impact
Post Quantum Crypto planning and POCs

2025 Activity Analysis
▪ Major Cloud Providers / IaaS Providers ahead ▪ Lack of real threat vs. potential limiting focus   ▪ Good Hygiene now, Tracking Standards ▪ NIST Published PQC Standards ▪ Real world performance testing has been promising
Risk Impact to Healthcare based on 2025:
Likelihood: — Impact: —
Accuracy Analysis


Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Supply Chain

Predictions
Supply Chain will remain major attack vector
One or Two Large Scale attacks will likely occur
Third Party components and software will lead to increases in the number of breaches

2025 Activity Analysis

100%
YoY Increase of breaches involving third party

30%
Of all breaches involve a third party

<50%
Vendors meet organizational cybersecurity requirements

Risk Impact to Healthcare based on 2025:

Likelihood: ↑ Impact: ↑

Accuracy Analysis

★ ★ ★ ★

Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Silver Bullet Solutions

Predictions
One Unified Platform supported by AI
▪ Security, Compliance and Governance
Zero Trust for the Masses – Wide Adoption
Security Operations – Fully AI Assisted
▪ Discover threats no human could

2025 Activity Analysis

▪ XDR, Orchestration platforms with AI continue to gain transaction
  ▪ True merging of these areas in a way that drives value is limited
▪ Zero Trust Adoption is growing, however
  ▪ Limited deployment scope
  ▪ Often smaller organizations
▪ SOCs are actively using AI, but mileage varies

Risk Impact to Healthcare based on 2025:
Likelihood: — Impact: —
Accuracy Analysis
★ ★

Clearwater

↑ Critical ↑ High ↑ Moderate — No Change

2025 Predictions – Scorecard

Prediction	Outcome	Accuracy
AI will add scales and sophistication to threat actor activity	Correct	★ ★ ★ ★ ★
Ransomware will still be prominent, but evolve	Correct	★ ★ ★ ★
The number of vulns will only get larger	Correct	★ ★ ★ ★
Preparing for Quantum computers will be the next Y2K	Incorrect	⊗
Supply chains will continue to be a major attack vector and grow in impact	Correct	★ ★ ★ ★
This is the year, solutions with AI, will be the silver bullet to our woes	Incorrect	★ ★
Overall Scores:	67% Correct	★ ★ ★ ½

Clearwater

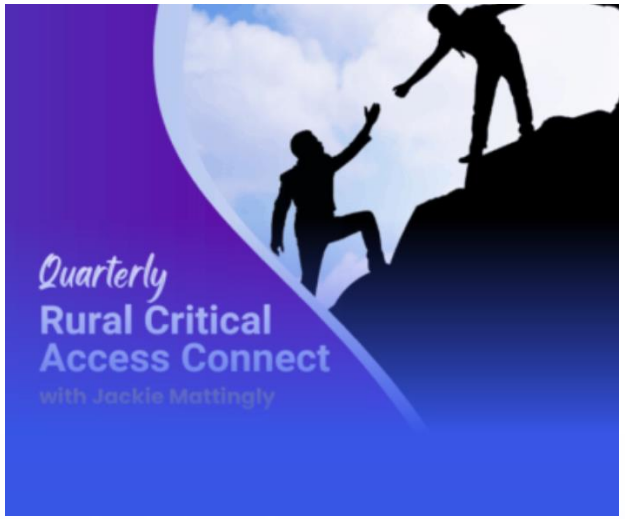
The way too early 2026 predictions

- Securing AI will be the most significant focus
  - Data Poisoning will be a huge attack vector and vendor solution focus
- One AI platform will have major breach
- Threat actors will deploy full AI Supported and real time enabled attack ware
- Regulations will be adopted to better govern usage of AI
- Agentic AI we become another “identity” to attack

Clearwater

Q&A

Upcoming Webinars + Events



Clearwater's Rural Critical Access Connect | December 18, 2025 | 10:30am – 11:30am CT

- This session features **Roger Neal, VP/COO of Duncan Regional Hospital**, joining **Jackie Mattingly and Chad Walker** to share 2025 lessons and practical, high-impact cybersecurity priorities for rural and critical access hospitals—with clear guidance on top risks, resource-focused actions, and how leaders can realistically strengthen their programs in 2026.
- Learn more here

Conversation with Greg Garcia |Monthly Cyber Briefing | January 8, 2026 | 12:00pm - 1 CT

- We're excited to welcome Greg Garcia, Executive Director of the Health Sector Coordinating Council (HSCC), for next month's Cyber Briefing. Greg will share what he's seeing across the healthcare ecosystem- emerging industry developments, new HSCC work products, and the regulatory signals that may shape 2026.

2026 Monthly Cyber Briefings:

- The meeting will be held on the second Thursday of the month due to New Year's holiday.
- All attendees from today will be automatically rolled over into the new 2026 series. Look out for an invite coming later this month.

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.


WISHING YOU
SEASON'S GREETINGS
2025
Clearwater
Healthcare - Secure, Compliant, Resilient

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.