Healthcare's Cyber Briefing

April 2, 2026

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.

Clearwater

Healthcare's Cyber Briefing

- Critical Threat Brief
- Education Session: Inside Washington: What's Moving on the Hill and at HHS
- Q+A

FEATURING:

Dave Bailey, VP of Consulting Solutions & Strategy

Cassie Ballard, Senior Director of Congressional Affairs at CHIME

Andrew Mahler, Clearwater VP of Consulting Services, Privacy & Compliance

Healthcare Industry Threat Information

Relevant Threat Information for Healthcare

Google Threat Intelligence

Clearwater

Threat Level Elevated

Iranian Cyber Threat Escalation Following U.S.–Israel Strikes

On February 28, 2026, coordinated U.S. and Israeli military strikes targeted Iranian assets. Within hours, Iranian-affiliated cyber groups initiated retaliatory operations.

Healthcare has historically been considered a high-impact civilian target during geopolitical escalation due to its operational sensitivity and patient safety implications.

Federal partners indicate there is currently no specific credible threat directed at U.S. healthcare organizations. However, historical patterns show that military escalation often coincides with increased cyber activity targeting civilian infrastructure.

This escalation materially increases risk to U.S. healthcare organizations through:

1. Heightened likelihood of disruptive cyber activity
2. Potential disruption of medical and pharmaceutical logistics tied to Middle East shipping routes

Executive leadership should treat this as a near-term resilience event — validate cyber readiness while confirming supply continuity for critical medications and devices.

Stryker experienced a large-scale cyberattack that caused global operational disruption

- **Method of Destruction:** Attackers compromised high-level administrative credentials to gain access to Stryker's **Microsoft Intune** management console . They weaponized the platform's native **remote wipe** feature to simultaneously trigger factory resets on over **200,000 corporate devices**, including servers, laptops, and mobile systems .
- **Attribution:** The attack was claimed by **Handala** (also known as the Handala Hack Team), a threat actor persona associated with the Iranian Ministry of Intelligence and Security (MOIS) . Analysts track this cluster as **UNC5203** (or Void Manticore), noting that the group uses "hacktivist" branding to provide plausible deniability for state-sponsored destructive operations.
- **Impact:** The disruption halted global manufacturing, order processing, and administrative functions in the U.S. and Ireland. In Maryland, hospitals were forced to temporarily suspend digital connections with Stryker and revert to radio communication for emergency medical services .
- **Data Exfiltration:** Handala claimed to have exfiltrated **50 TB of sensitive data** prior to triggering the wipe commands, positioning the incident as a "hack-and-leak" operation motivated by retaliation for geopolitical military strikes .

The Stryker disruption was not a device failure event but a systemic IT/operational cyber crisis

Supply chain fragility: Even when devices are unaffected, IT disruption at manufacturers cascades into clinical care delays

Identity/MDM risk: Compromise of centralized device management can enable enterprise-wide destructive attacks

Healthcare targeting escalation: Attack signals a shift toward strategic disruption of critical healthcare infrastructure

Resilience gap: Traditional focus on device safety must expand to enterprise IT and operational resilience

Regulatory pressure likely to increase around cybersecurity controls for medtech manufacturers

Cloud-Based EHR Vendor Incident Signals Downstream Risk

- Cloud-based EHR vendor CareCloud disclosed a March 16 cyber incident involving unauthorized access to one of its EHR environments
- Incident caused temporary disruption and lasted approximately eight hours before containment
- Environment stores patient information; organization is still assessing whether data was accessed or exfiltrated
- Vendor supports more than 40,000 healthcare providers, creating potential for broad downstream impact across client organizations
- Highlights concentration risk and the operational dependency healthcare organizations have on third-party EHR platforms

8 hours of unauthorized access
40,000+ providers supported

Clearwater

Breach Portal Updates

Dave Bailey, VP Consulting Solutions & Strategy

Clearwater

Breach Portal Activity Remains Quiet, But Risk Signals Persist

- The OCR Breach Portal has not reflected significant new reported breaches since our last review
- This is not uncommon and may reflect:
  - Reporting delays
  - Ongoing investigations
  - Timing of submission batching
- Recent data continues to show:
  - Concentrated impact from fewer incidents
  - Continued exposure tied to business associates
  - Access-related events driving the largest breaches
- Portal now explicitly says OCR investigates both **PHI** and **Part 2** breaches affecting **500 or more individuals**, and that a breach involving both must be reported **separately**.

0 new breaches reported in March

Source: U.S. Department of Health & Human Services - Office for Civil Rights

Clearwater

OCR Enforcement Signals Expand to Business Associates

- **15M individuals impacted**
- **12th Risk Analysis Initiative enforcement action**

- OCR announced a March 5, 2026 settlement with MMG Fusion, a business associate, impacting approximately 15 million individuals
- Marks the 12th enforcement action under OCR's Risk Analysis Initiative, reinforcing continued focus on foundational program gaps
- OCR emphasized that business associates must notify covered entities of breaches without unreasonable delay and within 60 days of discovery
- Signals increased scrutiny on vendor breach response, communication timelines, and downstream impact to covered entities

Ransomware Update

Impacts from Ransomware in March

Google Threat Intelligence

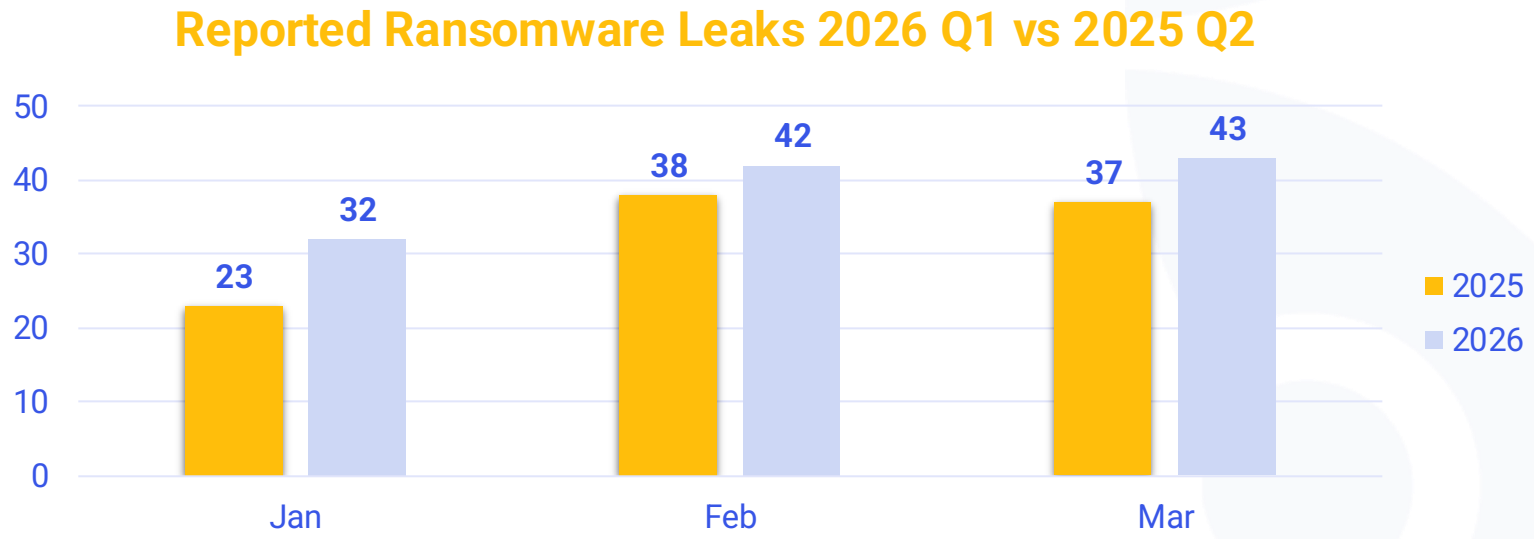
Clearwater

Healthcare has retained its position as the industry most targeted by cyber actors, an unwanted accolade that the sector has held for more than a decade, and in 2025, healthcare had the highest average ransom payments, averaging $1,154,245

https://www.hipaajournal.com/bakerhostetler-report-2026-healthcare/

Near 20% increase in reported ransomware data leaks in Q1 2026 compared to Q1 last year

Attackers are scaling operations for smarter, broader, and more systemic attacks



2025 Q1 Reported Data Leak Victims: 98

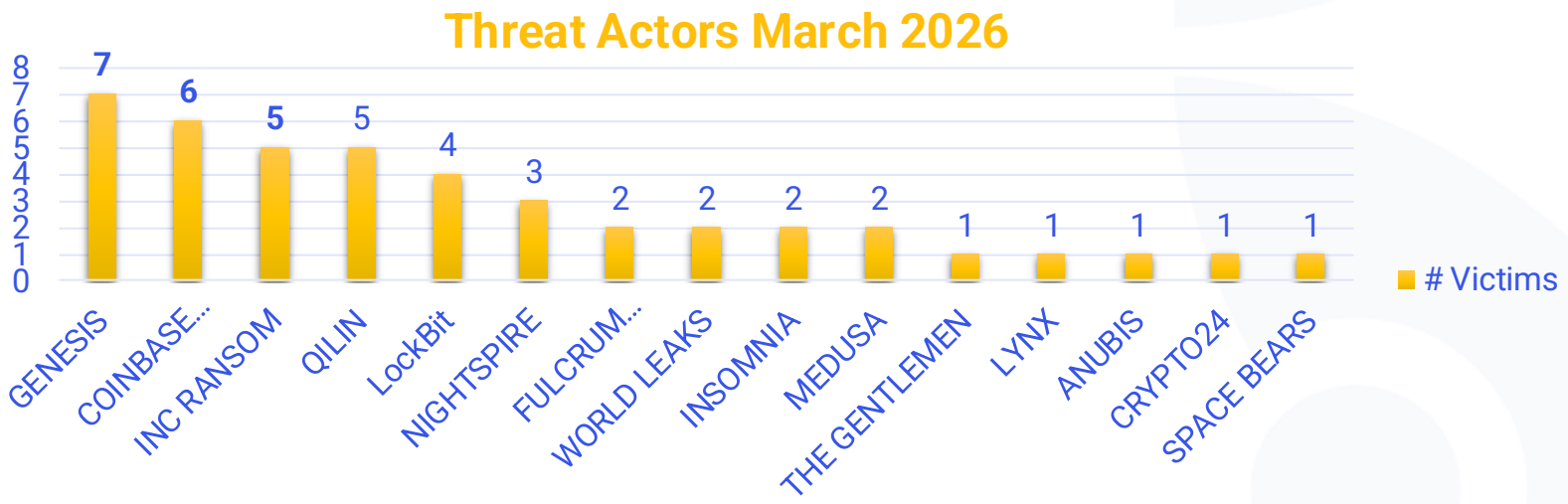
2026 Q1 Reported Data Leak Victims: 117

Clearwater

Google Threat Intelligence

43 Ransomware victims in March from 15 threat actors

Genisis, Coinbase Cartel, Inc Ransomware, Qilin, & Lockbit make up 63% of the reported data leaks in March



Clearwater

Google Threat Intelligence

43
Victims

15
Threat Actors

Reported victims included specialty clinics, dental and eye-care practices, behavioral health providers, pharmacies and healthcare service firms, biotech and genomics companies, and medical product organizations

Sophisticated emerging groups

Genisis

- The Genesis ransomware group is a significant emerging threat that transitioned from its initial discovery in October 2025 to a high-volume operational phase in early 2026.
- As of March 31, 2026, the group has demonstrated a sophisticated "double extortion" strategy, frequently prioritizing the exfiltration and public shaming of victims on their TOR-based data leak site (DLS) to force rapid ransom settlements .
- During the month of March, Genesis maintained a high tempo of attacks, primarily focusing on mid-market organizations. While the group is relatively new, its impact has been felt across critical sectors.
- Intelligence suggests the group is increasingly leveraging "data-only" extortion, where they skip the encryption phase entirely to avoid detection by automated EDR responses, focusing instead on the reputational damage of leaked sensitive information

Coinbase Cartel

- The Coinbase Cartel emerged as one of the most prolific ransomware threats in March 2026, ranking as the third most active group globally during this period.
- The group is characterized by its aggressive targeting of high-value sectors and its international reach, claiming victims across North America, Europe, and Asia.
- Global Reach: The group does not appear to have a single geographic focus, successfully compromising organizations in the United States, United Kingdom, Germany, France, and Taiwan.
- The Coinbase Cartel should be considered a Top-Tier Threat. Their ability to simultaneously manage multiple high-profile compromises across different time zones and languages suggests a large, well-funded organization with advanced affiliate management or highly efficient automated discovery tools.

Ransomware Targeting Patterns

Impacts from Ransomware in March

Google Threat Intelligence

Clearwater

Ransomware actors are not focusing on a single healthcare segment. Instead, they are exploiting the sector’s fragmentation targeting a wide range of smaller, specialized, and operationally critical organizations where cybersecurity is typically less mature

Specialty and outpatient providers represent the highest concentration of victims targeted by top 6

Threat Actor	Hospitals	Specialty Practices	Dental	Senior Care	Diagnostic	Pharma/ Pharmacy	Research
GENESIS	○	●	○	○	○	○	○
COINBASE CARTEL	○	●	○	◐	○	○	●
INC RANSOM	○	●	○	○	○	○	○
QILIN	○	●	○	○	○	○	○
LockBit	○	●	○	○	○	●	○
NIGHTSPIRE	◐	◐	○	○	○	○	◐

● Multiple victims observed
◐ Single victims observed
○ No victims observed

Clearwater Google Threat Intelligence

Sector Updates

HHS Focus on Cybersecurity

Clearwater

The FTC is significantly escalating oversight of healthcare markets

- The initiative is driven by concerns that **market consolidation and anticompetitive practices** are increasing costs, reducing quality, and limiting access to care: particularly for vulnerable populations

Key Actions:

- Establish a cross-agency task force combining competition, consumer protection, economics, policy, and technology expertise
- Coordinate enforcement, investigations, and advocacy across the FTC
- Focus on anticompetitive conduct, deceptive practices, and regulatory barriers in healthcare markets
- Conduct proactive monitoring to identify emerging risks

HHS is re-architecting the regulatory and operational foundation of U.S. healthcare technology

Centralization of Technology Authority	▪ HHS is consolidating key technology roles—Chief AI Officer, Chief Technology Officer, and Chief Data Officer—under the Office of the Chief Information Officer (OCIO)

Refocusing ONC on Policy & Interoperability	▪ The Office of the National Coordinator for Health IT (ONC) is:
	  ▪ Returning to its core mission
	  ▪ Focused on interoperability, standards, and certification

Acceleration of Data Liquidity (Interoperability at Scale)	▪ HHS is doubling down on nationwide health data exchange initiatives (e.g., TEFCA) Goal: Enable real-time, secure, patient-controlled data flow across systems
AI Enablement as a Core Policy Priority	▪ AI is being operationalized as a system-wide capability, not a pilot initiative Leadership alignment enables: Faster deployment of AI in clinical care, operations, and public health ▪ Unified AI governance and risk management
Affordability Through Digital Transformation	▪ Digital transformation is now explicitly tied to national healthcare affordability goals

Key Takeaways

1. Resilience over prevention
2. Third-party risk governance
3. Identity security investment
4. Downtime readiness

Google Threat Intelligence

Clearwater

Healthcare's Cyber Briefing

Inside Washington: What's Moving on the Hill and at HHS

FEATURING:

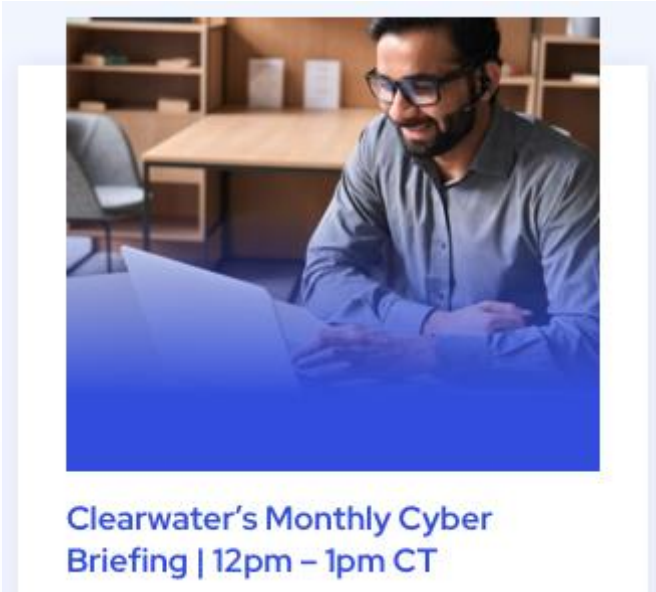
Cassie Ballard, Senior Director of Congressional Affairs at CHIME

Andrew Mahler, VP of Consulting Services, Privacy & Compliance

Q&A

Clearwater

Upcoming Webinars and Virtual Events



- Next session May 7th
- Health Sector Coordinating Council Cybersecurity Working Group Chair Chris Tyberg will join us for a discussion of systemic risk across the healthcare sector and the upcoming national cyber exercise led by HSCC and H-ISAC

The Virtual Forty-Third National HIPAA Summit

- Clearwater experts will be speaking in multiple sessions during this premier industry conference, including a Cybersecurity Leaders Roundtable moderated by Senior Director of Consulting Services Jackie Mattingly; the conference is being presented April 7-10

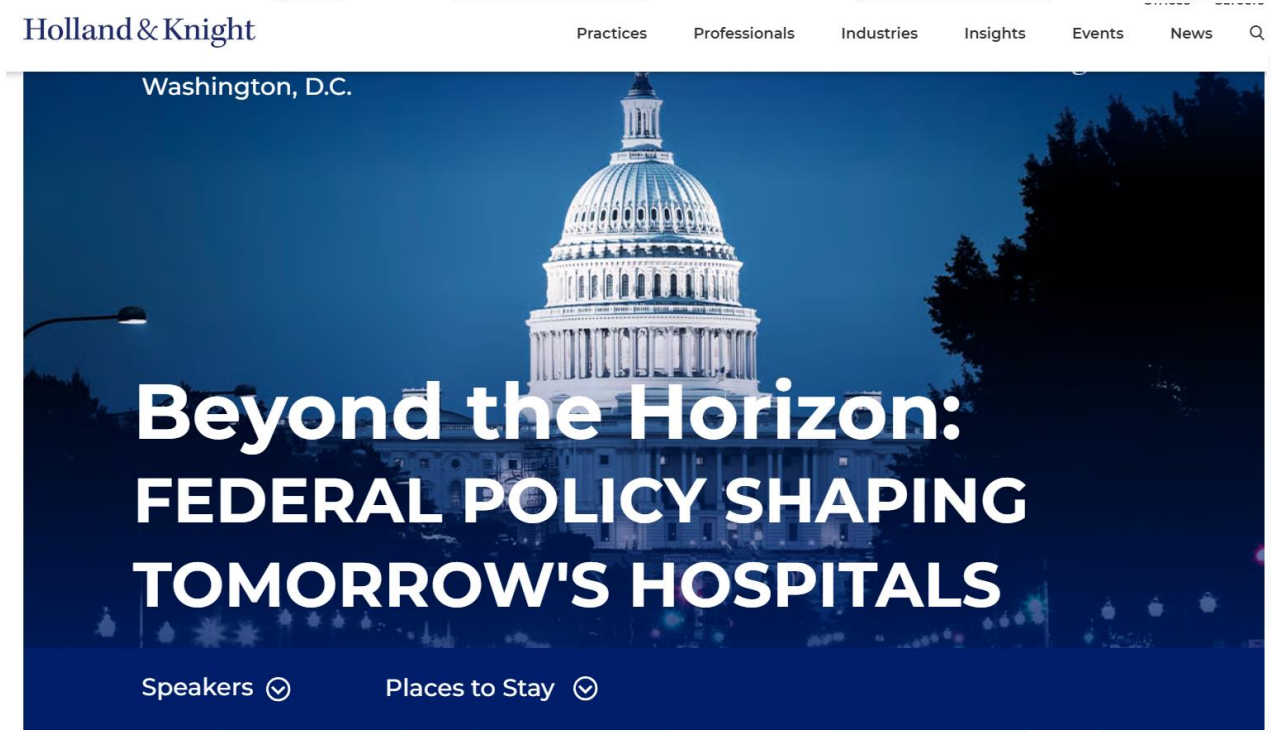
View session information + register

Clearwater

Hospitals & Health Systems Symposium **May 18–19, 2026 | Washington, DC**

From Capitol Hill to Patient Bedside: The Intersection of Health Policy and Medical Innovation
Moderator:
Andrew Mahler
Vice President, Consulting Services – Privacy & Compliance, Clearwater
Panelists:
Mari Savickis, VP, Public Policy, CHIME

https://clearwatersecurity.com/events/hospital-horizons-symposium-may-18-19-2026-washington-dc/



Upcoming In-Person Events

Scale Community Gold Club Retreat | April 10-12, 2026 | Park City, UT

- Clearwater's David Kolb, VP, PPMG + Austin Holland AE, PPMG attending
- This exclusive gathering of senior leaders from Management Services Organizations (MSOs) in healthcare.

Learn more + book a meeting

HCCA Annual Compliance Institute | April 27-30, 2026 | Orlando, FL

- Clearwater is excited to participate in this premier conference for healthcare compliance and ethics professionals, bringing together industry leaders to explore best practices, regulatory updates, and emerging risk
- Several Clearwater experts speaking and visit us at booth 419

Learn more + view sessions

Cooley HealthTech Conference | April 28, 2026 | Palo Alto, CA

- Clearwater is proud to sponsor
- This invite-only event will spotlight the key forces driving innovation and growth industrywide, with focused discussions on strategies for healthtech, medical device, medtech and digital health companies.

Learn more + book a meeting

Clearwater

Upcoming In-Person Events

McGuireWoods Healthcare Private Equity & Finance Conference | April 29-30 | Chicago, IL

- David Kolb, VP. PPMG, Dave Bailey, VP Consulting Strategy & Solutions and Richmond Donnelly, Senior Account Exec, Private Equity attending

Learn more+ book a meeting

McDermott Health Tech Investment Forum | April 30, 2026 | San Franciso, CA

- Clearwater is proud to sponsor this new event convening investors, c-suite operators and founders in healthcare tech.
- Alex Masten, VP, Digital Health & Jeff Englander, Executive Business Advisor, Business Development attending

Learn more + book a meeting

Clearwater

We are here to help.

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

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.