Monthly Cyber Briefing

August 7, 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.

Agenda + Speakers

- Cyber & Regulatory Update
- From Innovation to Exposure: How Healthcare Tech Trends Are Reshaping Cyber Risk
- Q+A

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

Chief Executive Officer
Clearwater

Erik Pupo

Director
Guidehouse

Clearwater

Cyber & Regulatory Update

Steve Cagle, MBA, HCISPP, CHISL, CDH-E

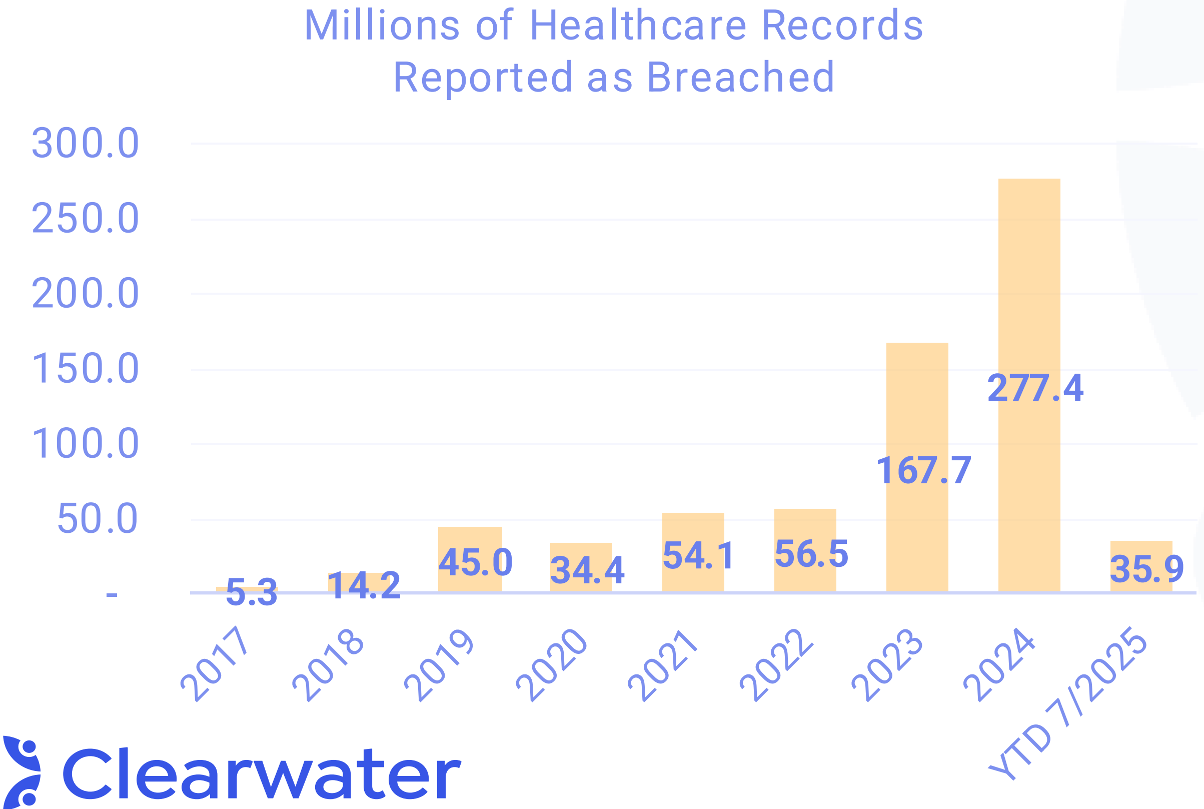
CEO, Clearwater

Clearwater

Breach Reports via OCR Breach Portal & SEC Reporting

OCR Breach Portal Data[1]

- 2024 breach data: 277.4M records from 734 breaches
- YTD 2025 breach data: 35.9M individuals from 418 breaches - ~6.1M records reported in past month



Notable Breaches

- Anne Arundel Dermatology - 1.9M records; two ransomware attacks within 3 months
- Radiology Associates of Richmond - 1.4M records breached following cyber attack
- About 103,000 CMS beneficiaries may have been impacted by the creation of fraudulent Medicare.gov accounts over two years

Clearwater

[1] The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 7/30/25, pulled 7/3/25)

2025 IBM/Ponemon “Cost of A Data Breach” Report

Globally, data breach costs have declined for the first time in five years, dropping to USD $4.44 million, due to faster breach containment, **however, in the U.S., breach costs increased by 9% to $10.22 million.**

$7.4	Cost of breach in healthcare – highest of any sector (-24% vs LY)
600	Number of organizations breached
3,470	Number of interviews with IT, Security & C-Suite
113,600	Largest breach included in the study

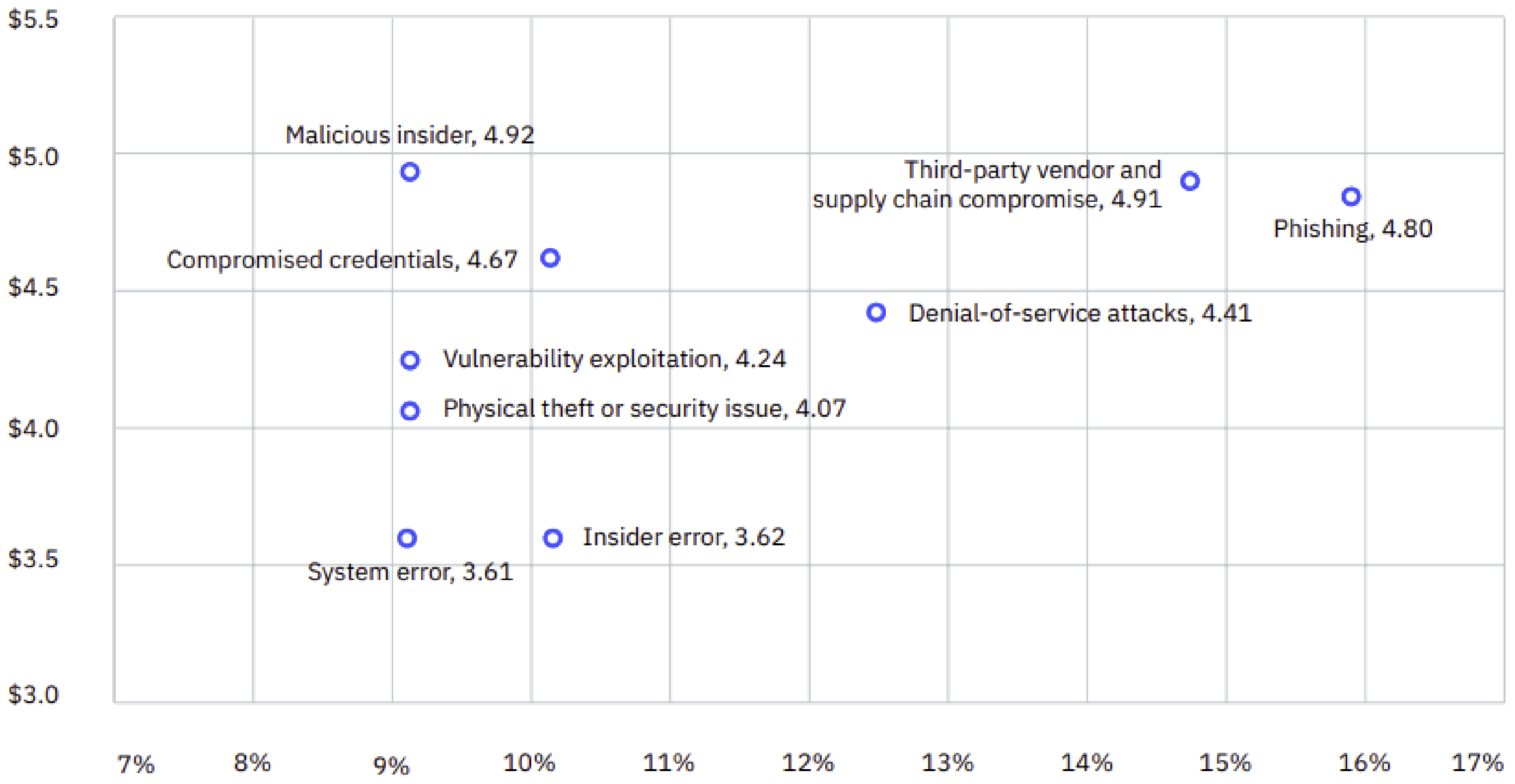
- Organizations are skipping over security and governance for AI in favor of “do-it-now” AI adoption
- In 16% of breaches attackers used AI, most commonly phishing and deepfakes were used in the attacks
- 50% of breaches were discovered by security teams (vs. third party or hacker) – an increase over previous years
- 76% of organizations took more than 100 days to recover from the breach, with 26% taking over 150 days

Clearwater

Link to Cost of a data breach 2025 | Ponemon Research | Sponsored By IBM

Ponemon “Cost of A Breach” Report - Sources of Attacks

Figure 9.
Measured in USD millions; percentage of all breaches



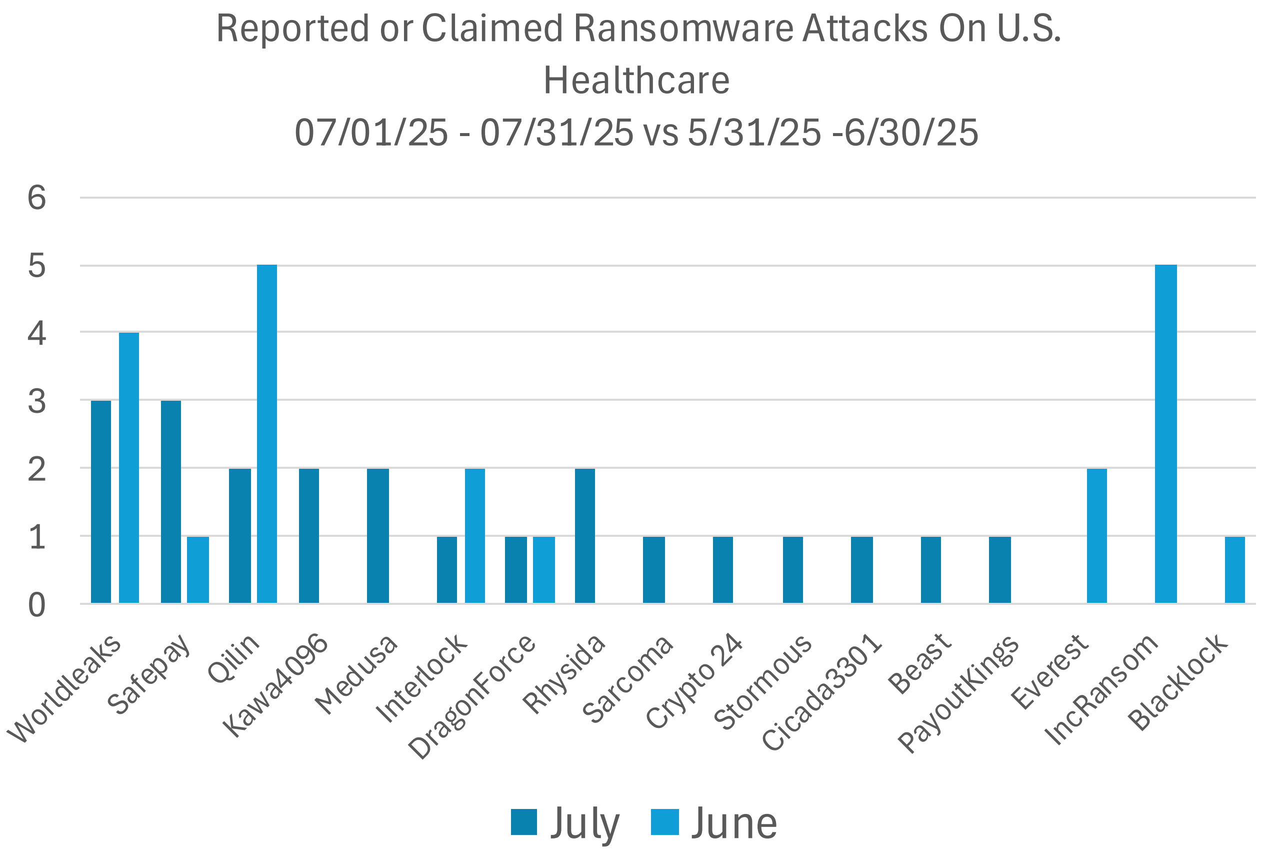
- Phishing replaced stolen credentials this year as the most common initial vector attackers used to gain access to systems (16%)
- Supply chain compromise surged to become the second most prevalent attack vector (15%) and almost tied for costliest ($4.91M) after malicious insider threats ($4.92 million).

Clearwater

Link to Cost of a data breach 2025 | Ponemon Research | Sponsored By IBM

Healthcare Ransomware Attacks/Leaks Since Last Briefing

22 newly identified ransomware attacks on U.S. Healthcare organizations 7/1/25 – 7/31/25.*

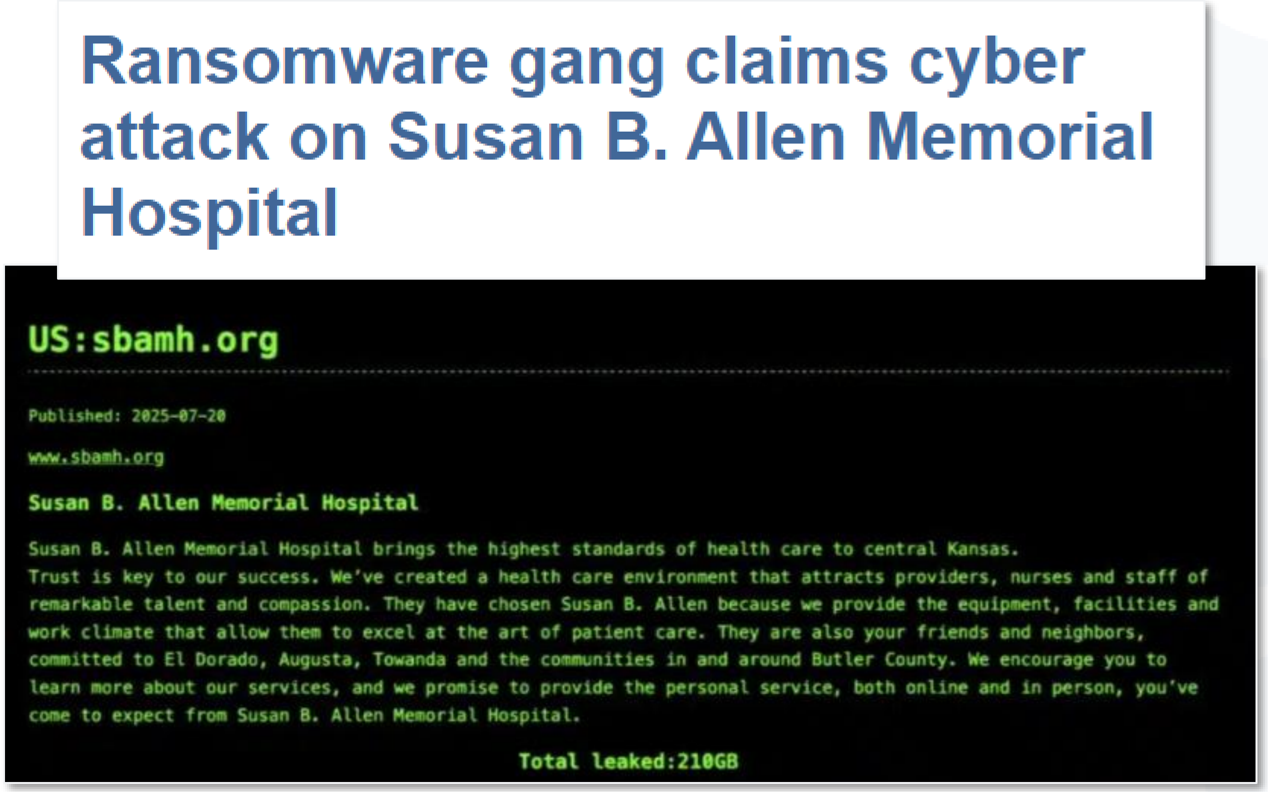


- No reported attacks from INC Ransom who was previously leading attacks in healthcare
- Worldleaks, Safepay and Qilin continue to lead in the number of published attacks
- New threat actor Kawa4096 – 2 attacks in U.S. Healthcare recently
- Major Disruptions last month
  - Susan B Allen Memorial Hospital on July 16 (Kawa4096)
  - Accu Reference Labs on July 1 (Qilin)
  - Cookeville Regional Medical Center on July 13 (Rhysidia)
  - Florida Hand Center (Rhysidia)

*Source: Ransomware.live - Last ransom claims or publicly reported but not yet leaked

New Threat Actor Targeting Healthcare - Kawa4096

2 attacks on healthcare in July: Susan B. Allen Memorial Hospital and CareSTL Health



Ransomware gang claims cyber attack on Susan B. Allen Memorial Hospital

US:sbamh.org

Published: 2025-07-20

www.sbamh.org

Susan B. Allen Memorial Hospital

Susan B. Allen Memorial Hospital brings the highest standards of health care to central Kansas.
Trust is key to our success. We've created a health care environment that attracts providers, nurses and staff of remarkable talent and compassion. They have chosen Susan B. Allen because we provide the equipment, facilities and work climate that allow them to excel at the art of patient care. They are also your friends and neighbors, committed to El Dorado, Augusta, Towanda and the communities in and around Butler County. We encourage you to learn more about our services, and we promise to provide the personal service, both online and in person, you've come to expect from Susan B. Allen Memorial Hospital.

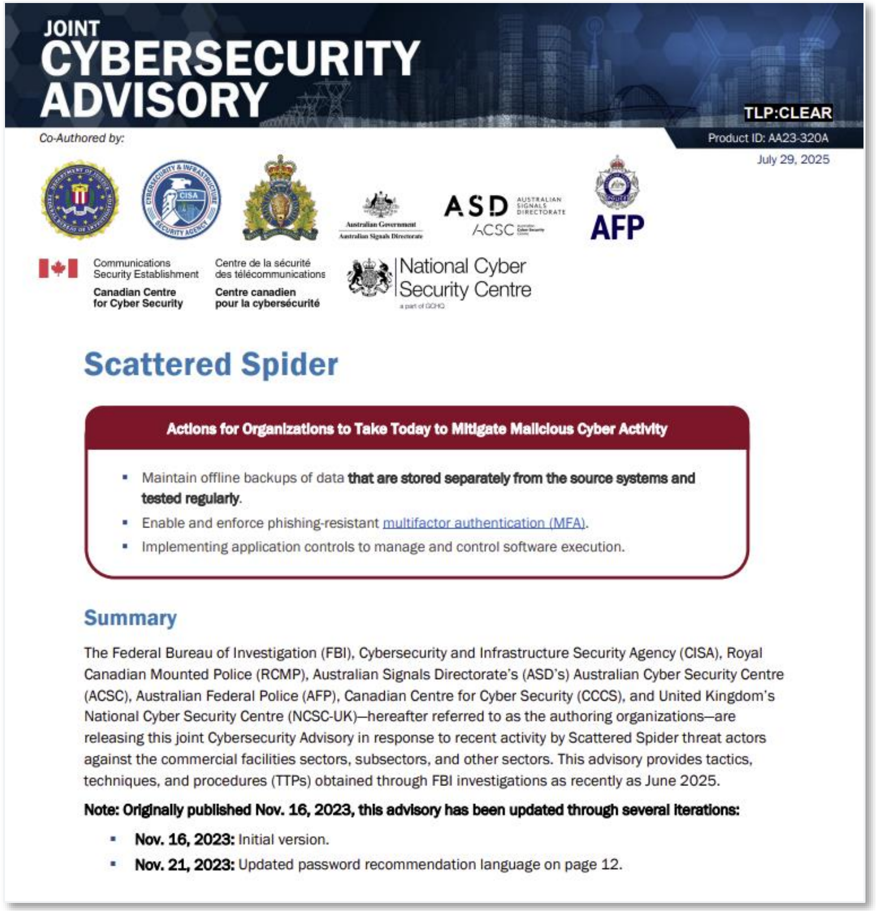
Total leaked:210GB

Image related to Susan B. Allen Memorial Hospital attack taken from Kawa406 leak site

- New as of June 2025 – 17 attacks so far
- Mimics other high profile threat actors (e.g., Qilin and Akira)
- Uses multithreaded encryption engine to speed up encryption
- Terminates security software/disables EDR
- Employs aggressive anti-recovery tactics
- Focuses on maximum impact encryption
- Uses double extortion, including publicizing and pressuring victims

CISA Advisory Update: Scattered Spider

"An increasing number of impactful ransomware attacks create a "serious and ongoing threat" to organizations."



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA23-320A

July 29, 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC

AFP

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

Scattered Spider

Actions for Organizations to Take Today to Mitigate Malicious Cyber Activity

- Maintain offline backups of data **that are stored separately from the source systems and tested regularly**.
- Enable and enforce phishing-resistant multifactor authentication (MFA).
- Implementing application controls to manage and control software execution.

Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Royal Canadian Mounted Police (RCMP), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Australian Federal Police (AFP), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as the authoring organizations—are releasing this joint Cybersecurity Advisory in response to recent activity by Scattered Spider threat actors against the commercial facilities sectors, subsectors, and other sectors. This advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as June 2025.

Note: Originally published Nov. 16, 2023, this advisory has been updated through several iterations:

- **Nov. 16, 2023:** Initial version.
- **Nov. 21, 2023:** Updated password recommendation language on page 12.

- Intrusion and extortion crew that partners with ransomware gangs to monetize their access capabilities
- Active since 2022; operations evolved and intensified recently
- Masters of social engineering techniques; use creative tactics to exploit corporate practices
- Recently posing as employees to convince IT and/or helpdesk staff to reset passwords & re-assign MFA
- Successful at Vishing, MFA Push bombing, SIM Swapping
- Effective at employing living off the land techniques
- Have searched target's Slack, Microsoft Teams, and Microsoft Exchange Online for emails or conversations regarding the intrusion and security response & even joined meetings
- Hundreds of members worldwide who exercise stealth and persistence, changing techniques to avoid patterns

Link to CISA Updated Scattered Spider Advisory

CISA Advisory Update: Interlock

Interlock continues to target the U.S. Healthcare sector, continuing its campaign initiated in Fall 2024

JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Co-Authored by:

MS-ISAC Multi-State Information Sharing & Analysis Center

Product ID: AA25-203A

July 22, 2025

#StopRansomware: Interlock

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

- Prevent initial access by implementing domain name system (DNS) filtering and web access firewalls, and training users to spot social engineering attempts.
- Mitigate known vulnerabilities by ensuring operating systems, software, and firmware are patched and up to date.
- Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization.
- Implement identity, credential, and access management (ICAM) policies across the organization and then require multifactor authentication (MFA) for all services to the extent possible.

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.*

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC)—hereafter referred to as "the authoring agencies"—are releasing this joint advisory to

- Uses TTPs known as a "drive-by attack" or also called a "drive-by download attack", including via compromising legitimate websites
- Observed using the ClickFix social engineering technique for initial access and tricking target into executing a malicious payload
  - Typically made to look like Google Chrome, MS Edge, or MS Teams updates
- Deploy multi-stage attack
  - Info stealing malware, credential harvesting, data exfiltration
  - Customized encryption (ransomware) tools tailored to environment

Clearwater

Link to CISA Interlock Advisory

Link to HC3 ClickFix Attacks Sector Alert

OCR Enforcement For Risk Analysis Failure

OCR finds that failure to conduct risk analysis related to ransomware attack that resulted in a breach of 24,891 individuals. *14th Ransomware Enforcement Action.*

Syracuse Ambulatory Service Center (doing business as Specialty Surgery Center of Central New York) agreed to 2-year Corrective Action Plan

- Reported to HHS that an unauthorized individual had accessed its network in March 2021
- Investigation revealed they were victim to a ransomware attack
- ASC never conducted an accurate and thorough risk analysis to determine the risks and vulnerabilities to the ePHI it held
- OCR also found that Syracuse ASC failed to timely notify affected individuals and HHS of the breach

Key quotes from new OCR Director Paula Stannard:

“Conducting a thorough HIPAA-compliant risk analysis (and developing and implementing risk management measures to address any identified risks and vulnerabilities) is even more necessary as sophisticated cyberattacks increase”

“[Covered] entities and business associates ***make themselves soft targets for cyberattacks if they fail*** *to implement the HIPAA Security Rule requirements"*

Recommendations

Relevant actions based on current healthcare threat actor TTPs & regulatory enforcement trends discussed in this briefing.

- Implement DNS filtering to block access to malicious websites & use web application firewalls to filter harmful traffic
- Implement and execute processes for updating workforce on latest social engineering techniques in a timely manner
- Enhance monitoring for risky logins, high value users and critical vendor / third-party connections
- Enable MFA for all services to the full extent possible – but remember it is not a silver bullet!
- Require multi-person approval or in-person validation for password/account resets
- Update incident response playbooks to leverage external communication channels
- Maintain secure, offline, and immutable backups of critical data
- Move to *on-going, continuous* OCR-Quality Risk Analysis if you have not already done so; if not continuous, then at least annually with updates as part of your change control process

Healthcare's Monthly Cyber Briefing

From Innovation to Exposure: How Healthcare Tech Trends Are Reshaping Cyber Risk

Steve Cagle, Clearwater CEO
Erik Pupo, Director Guidehouse

Guidehouse

JULY 2025

Guidehouse 2025 Tech Trends - Cybersecurity

Erik Pupo and Cate Ciccolone

outwit complexity™

What do we see in 2026? How is transformation changing risk management and driving innovation

Time for a poll!

CONNECTED RESILIENCE

DATA VERACITY

DATA ECOSYSTEM

FOCUS ON THE FOUNDATION

What threats are emerging?

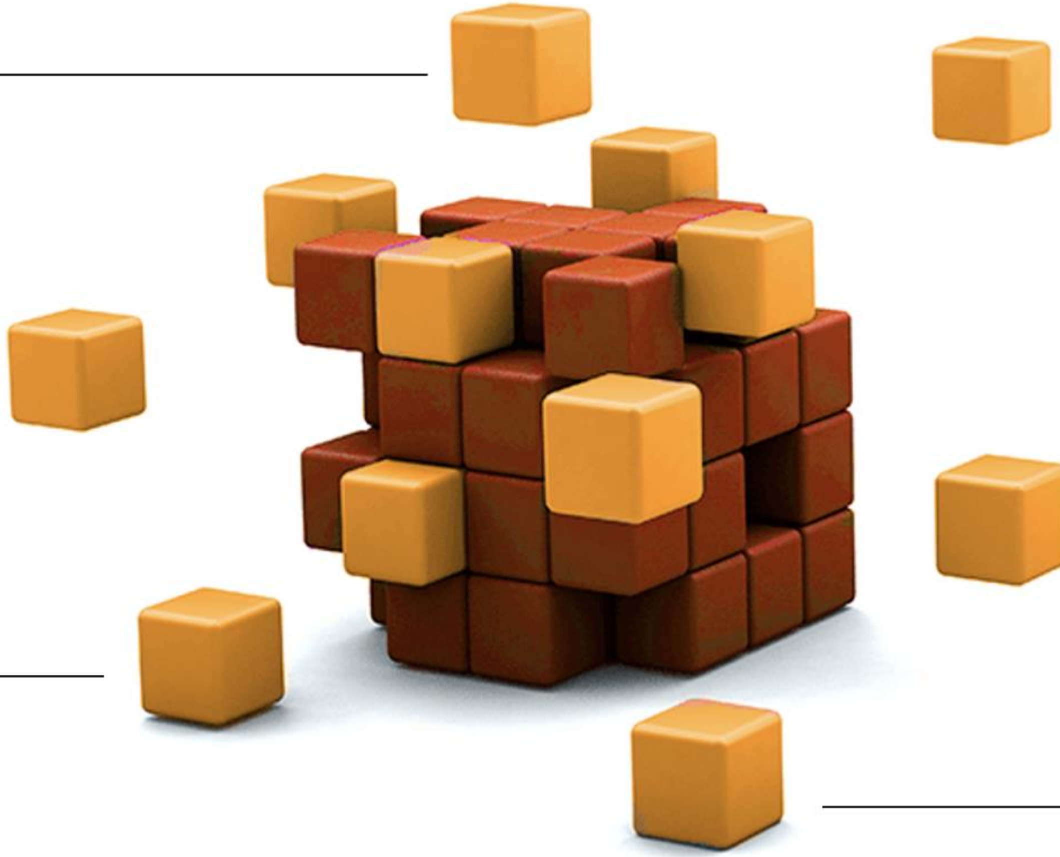
Security Interoperability

Human-Centric Attack Vectors

Too Much Data

Big Budgets, Small Skills

Where do blind spots exist?



DATA ECOSYSTEM

IMPORTANCE OF GOOD DATA VS. TOO MUCH DATA

DATA VERACITY

HUMAN ERROR, SOCIAL ENGINEERING, AND THE DESIRE FOR MORE

CONNECTED RESILIENCE

INVEST IN THE TISSUE JUST AS MUCH AS THE SKIN

FOCUS ON THE FOUNDATION

LARGE TOOLING BUDGETS WITH CORRESPONDING STAFFING PROBLEMS

Time for a poll!

Q&A

Monthly Cyber Briefing – Help Us Spread the Word

Next Session September 4

OCR Enforcement Findings in Cloud Environments and the Ramifications to HIPAA Risk Analysis

Steve Cagle, CEO, Clearwater

Dave Bailey, VP Security, Clearwater

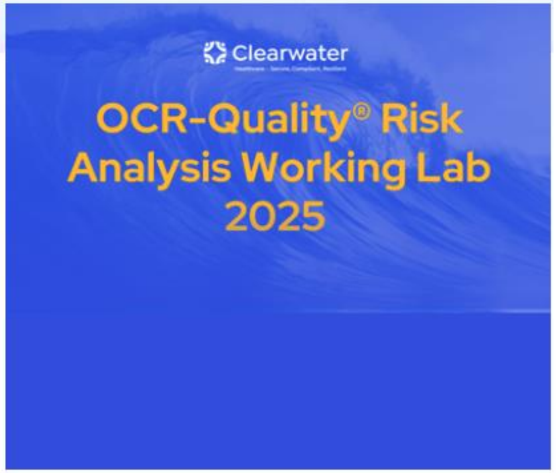
- Register link: https://clearwatersecurity.com/monthly-cyber-briefing/

Monthly Cyber Briefing

Scan to Register or Visit

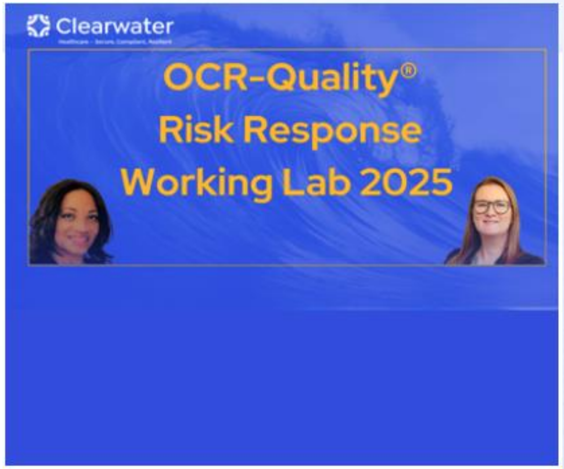
https://bit.ly/monthlycyberbriefing

Upcoming Webinars



OCR-Quality® Risk Analysis Working Lab 2025: Beginning August 6 @ 11:00 am CT

- 5-part series kicked off August 6th and runs through September. This is a hands-On, Interactive E-Learning Series to help you minimize cyber risk exposures and Meet Compliance Requirements
- Risk Analysis Register here



OCR-Quality® Risk Response Working Lab 2025: Beginning September 10 @ 11:00 am CT

- Following the Risk Analysis Working Lab comes the Risk Response 2-part webinar series on September 10th and 17th.
- Register here

AHLA Webinar: Health Care's Due Diligence Dilemma | September 16, 2025 | 2:00 – 3:00 pm ET

- Andrew Mahler, VP Privacy and Compliance Services presenting on how organizations can address cybersecurity and data privacy challenges during health care mergers and acquisitions.
- Register here

Clearwater's
Rural Critical Access Connect
With Jackie Mattingly
QUARTERLY
Uniting Cybersecurity Leaders for Resilient Healthcare
THURSDAY

Clearwater's Rural Critical Access Connect | September 18, 2025 | 12pm – 1pm CT

- An interactive space for rural and critical assess teams to share common challenges, success and come together.
- Register here

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.