Monthly Cyber Briefing

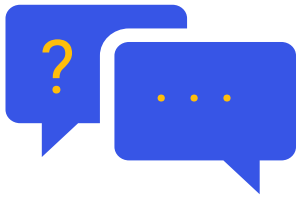
July 10, 2025

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.

Clearwater

Agenda + Speakers

- Cyber & Regulatory Update
- Enterprise Cyber Risk Management: Benchmarking Maturity, Prioritizing Risk, and Building a Resilient Program
- Q+A

Dave Bailey, EMBA, CISSP

VP, Consulting Services, Security
Clearwater

Jon Stone, MPA, PMP, HCISPP, CRISC

SVP & Chief Product Officer
Clearwater

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

Chief Executive Officer
Clearwater

Cyber & Regulatory Update

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

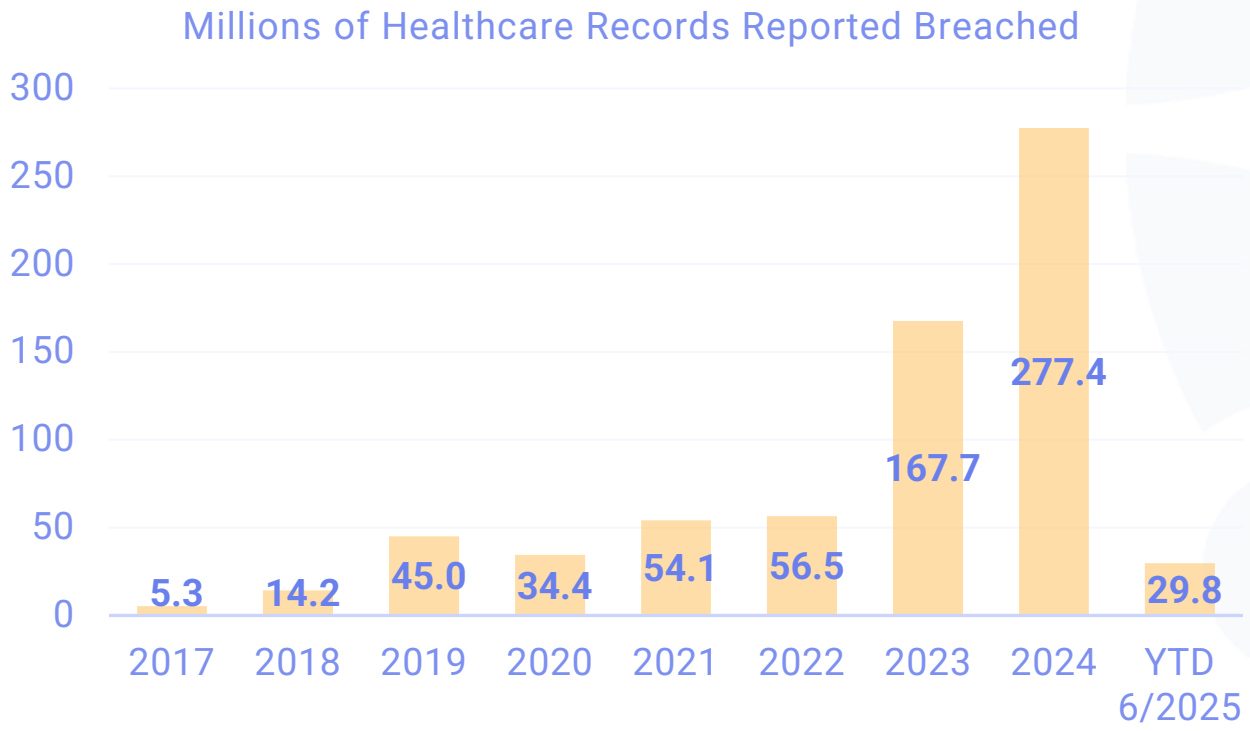
CEO, Clearwater

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: 28.8M individuals from 341 breaches - ~6M records reported in past month



Notable Breaches

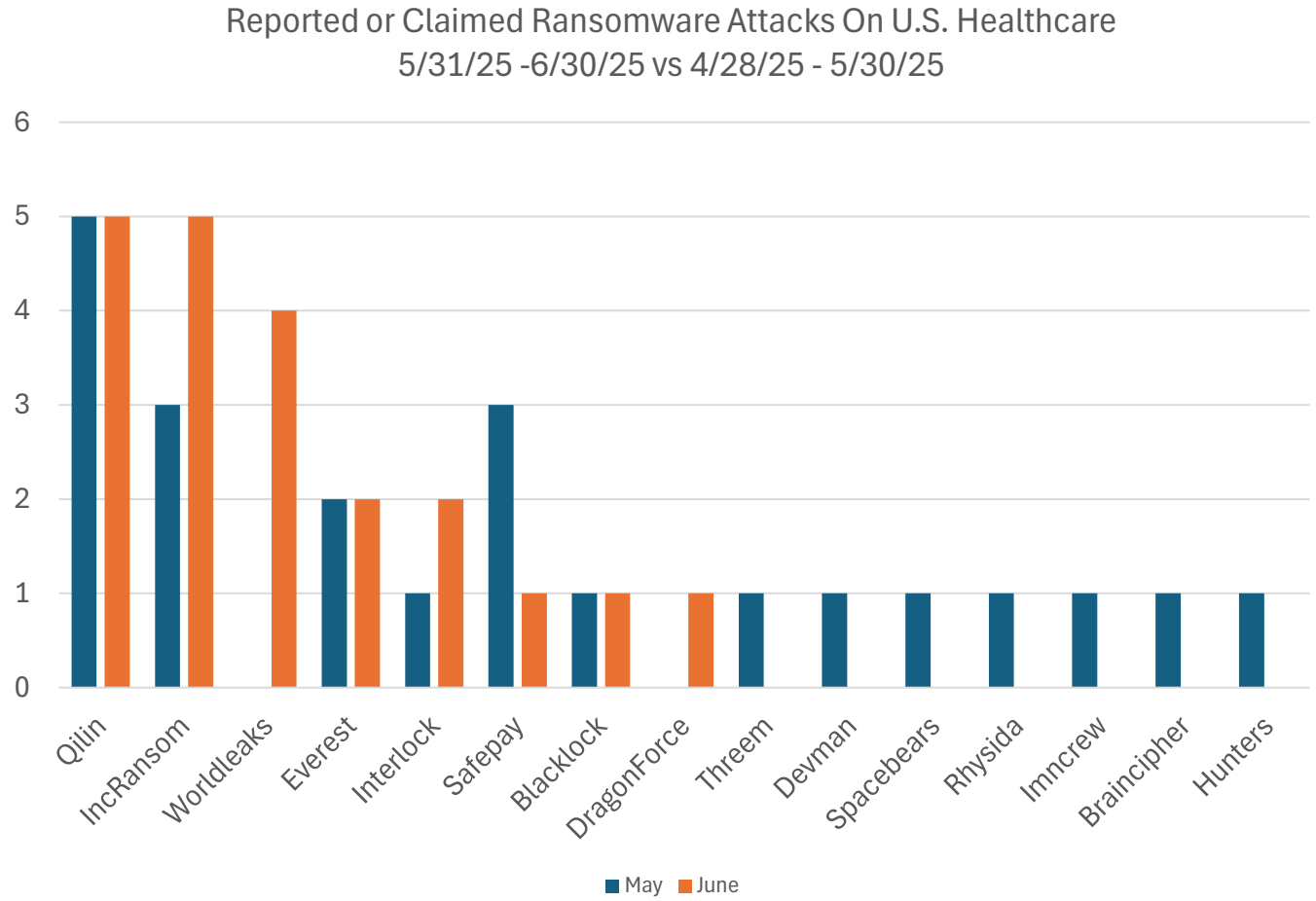
- Episource – a Subsidiary of Optum (UnitedHealth) – 5.4 Million records
- Ocuco Inc. – optical software company attacked by KillSec – 241K records
- Aflac Insurance – Reported to SEC on 6/20 that it had been breached on 6/12 (by Scattered Spider). Still determining extent of breach.

Clearwater

1 The HHS Breach Portal (2024 data through 12/31/24, pulled on 3/30/25; 2025 data through 6/30/25, pulled 7/2/25)

Ransomware Attacks on Healthcare Since Last Briefing

22 newly identified ransomware attacks on U.S. Healthcare organizations 5/31/25 – 6/30/25.*

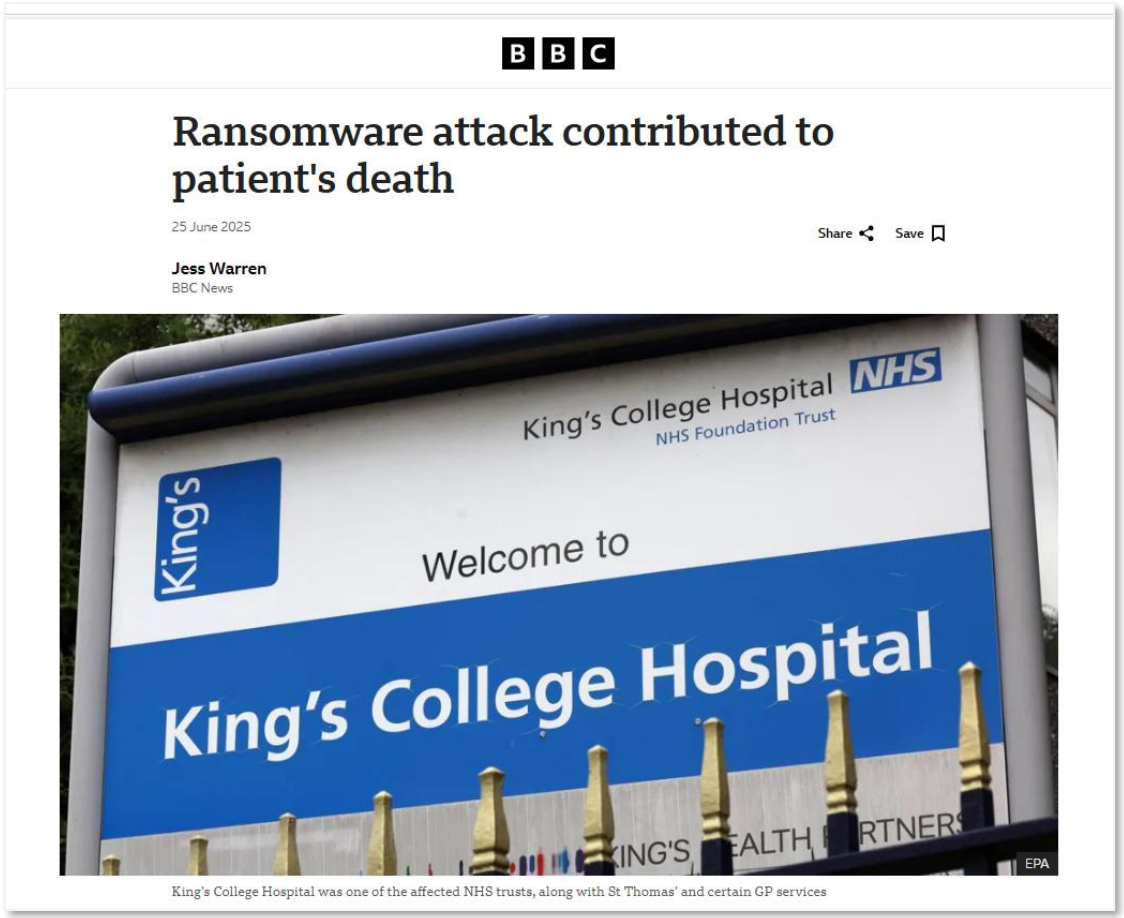


- Physician practice management, specialty care, and other ambulatory providers are majority of reported ransomware attacks
- Qilin and Inc IncRansom continue to be top two attackers on healthcare sector
- Safepay fewer attacks in June
- Hunters International has created a new “project” called WorldLeaks. They have shut down their RaaS business – see next slide
- New threat actor “Payouts King” recently reported as new ransomware group with 2 attacks in U.S. Healthcare providers

Clearwater

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

Ransomware Attack Contributed to Patient's Death



BBC

Ransomware attack contributed to patient's death

25 June 2025

Share Save

Jess Warren
BBC News

King's College Hospital was one of the affected NHS trusts, along with St Thomas' and certain GP services

[Link to article: NHS ransomware attack contributed to patient's death]

Investigation finds that Qilin Ransomware Attack on UK National Health Service in June 2024 led to patient death

- June 2024 cyberattack by Qilin crippled pathology services run by Synnovis, an NHS partner between hospitals and clinics in London.
- Over 10,000 appointments were canceled as blood tests could not be obtained
- Long wait for blood test results limited ability to diagnose and treat patients
- The Health Service Journal (HSJ) reported there were nearly 600 "incidents" linked to the attack, with patient care suffering in 170 of these.
  - One case of "severe" harm (death)
  - 14 "moderate" harm
  - remaining "low harm"

Clearwater

CISA Advisory: Play Ransomware / SimpleHelp

JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA23-352A
June 4, 2025

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

#StopRansomware: Play 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.*

Note: Updates to this advisory, originally published December 18, 2023, include:

- **June 4, 2025:** The advisory was updated to reflect new TTPs employed by Play ransomware group.

PLAY NEWS | CONTACT | FAQ

PLAY FAQ

- What happened?

- We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.

- How can i get my organization back to normal?

- The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.
Deal scenario:
1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.

- How can i trust you?

- We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

FBI, CISA warn Play ransomware targeting critical infrastructure with evolving techniques

- Among most highly successful ransomware gang: +900 victims
- Recently targeting exploit of vulnerabilities in SimpleHelp RMM
  - The most notable flaw, CVE-2024-57727 (reported in January) allows an unauthenticated attacker to download files and perform remote code execution
- Play ransomware binary is re-compiled for every attack making it difficult to detect
- Play's ransom note directs victims to contact Play by email
- Play is now calling victims to pressure payment

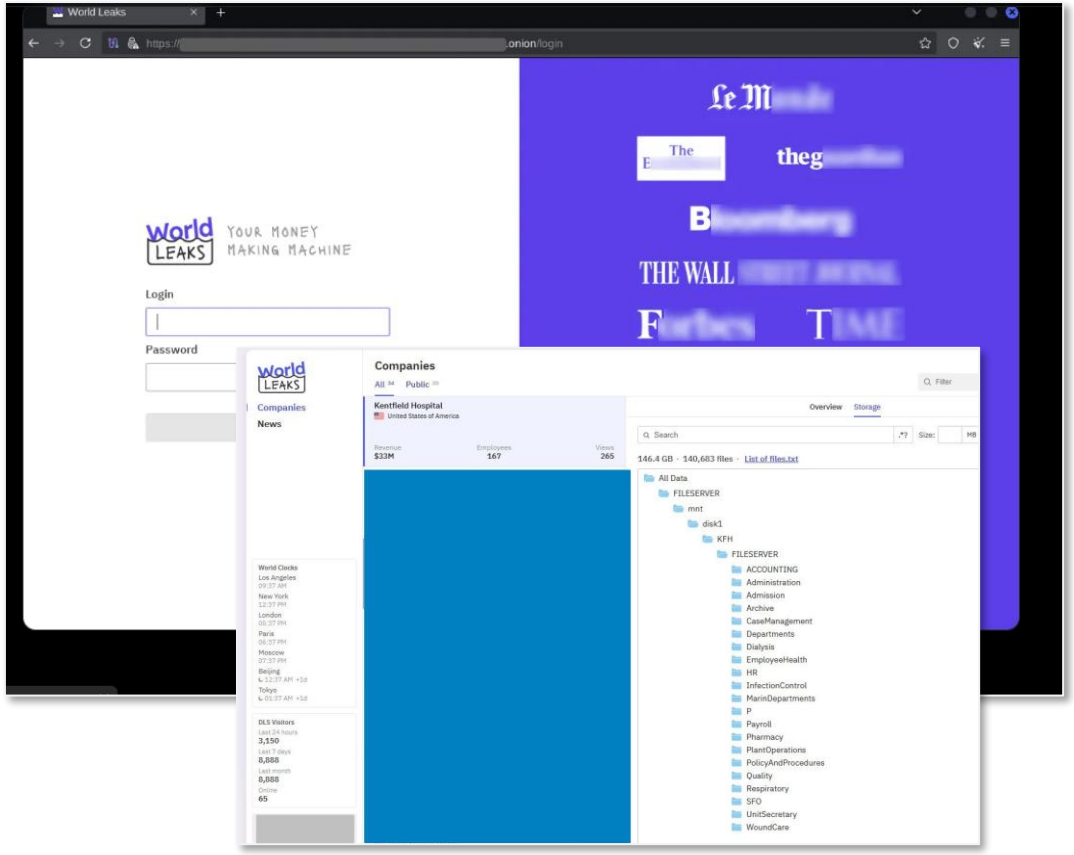
NOTE: Other threat actor groups are also exploiting Simplehelp vulnerability including affiliates of DragonForce (potentially Scattered Spider)

Clearwater

CISA Alert: #stopransomware-play-ransomware_2_revised.pdf

Hunters International Transforms to WorldLeaks

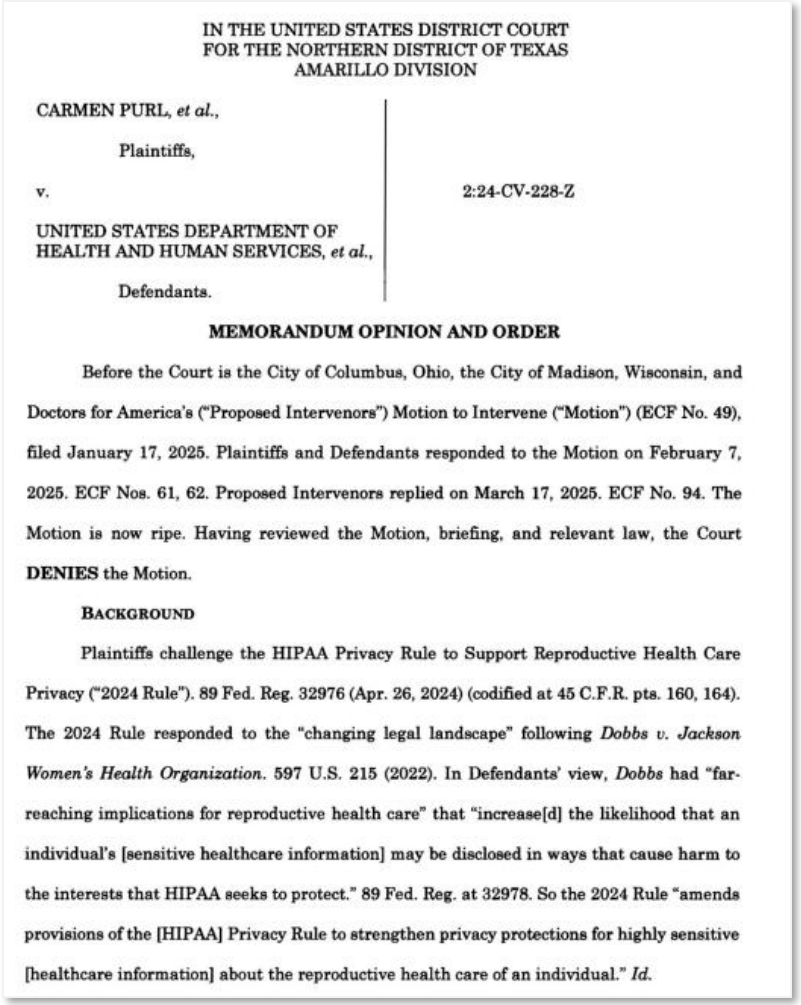
Members of Hunters International abandon traditional ransomware in favor of “extortion as a service”.



- Potential splintering or rebrand of Hunters International, who was known for several large healthcare ransomware attacks (Fred Hutchinson, Omni Family Health)
- Hunters International shutting down due to law enforcement pressure. They are offering free decryptor keys to victims
- WorldLeaks started up in January by members of Hunters. They are focused on theft and extortion.
- They claim to have a “100% fully undetectable” exfiltration tool
- Operate 4 distinct platforms from their website, including a dedicated page for journalists to receive breach notifications
- WorldLeaks appears to have 5 healthcare-related breaches in June, and already one hospital in July

Clearwater

Regulatory Update – HIPAA Privacy Rule to Support Reproductive Health Care Privacy



IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
AMARILLO DIVISION

CARMEN PURL, *et al.*,

Plaintiffs,

v.

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES, *et al.*,

Defendants.

2:24-CV-228-Z

MEMORANDUM OPINION AND ORDER

Before the Court is the City of Columbus, Ohio, the City of Madison, Wisconsin, and Doctors for America's ("Proposed Intervenors") Motion to Intervene ("Motion") (ECF No. 49), filed January 17, 2025. Plaintiffs and Defendants responded to the Motion on February 7, 2025. ECF Nos. 61, 62. Proposed Intervenors replied on March 17, 2025. ECF No. 94. The Motion is now ripe. Having reviewed the Motion, briefing, and relevant law, the Court **DENIES** the Motion.

BACKGROUND

Plaintiffs challenge the HIPAA Privacy Rule to Support Reproductive Health Care Privacy ("2024 Rule"). 89 Fed. Reg. 32976 (Apr. 26, 2024) (codified at 45 C.F.R. pts. 160, 164). The 2024 Rule responded to the "changing legal landscape" following *Dobbs v. Jackson Women's Health Organization*. 597 U.S. 215 (2022). In Defendants' view, *Dobbs* had "far-reaching implications for reproductive health care" that "increase[d] the likelihood that an individual's [sensitive healthcare information] may be disclosed in ways that cause harm to the interests that HIPAA seeks to protect." 89 Fed. Reg. at 32978. So the 2024 Rule "amends provisions of the [HIPAA] Privacy Rule to strengthen privacy protections for highly sensitive [healthcare information] about the reproductive health care of an individual." *Id.*

Purl vs HHS – Ruling Vacates the *HIPAA Privacy Rule to Support Reproductive Health Care Privacy*

- Carmen Purl and her medical clinic argued that HHS had exceeded its statutory authority in the Rule
- U.S. District Court for the Northern District of Texas agreed. Issued order on June 18th vacating the HIPAA Privacy Rule to Support Reproductive Health Care
- Updates to 164.520 (NPP related to Part 2) remain
- *HIPAA-regulated entities must now revert to their HIPAA compliance programs prior to the final rule being issued*

OCR Enforcement For Risk Analysis Failure

OCR Settles HIPAA Security and Privacy Rule investigation with The Behavioral Health Solution of Deer Oaks, resulting in a $225,000 settlement and 2-year Corrective Action Plan

Key Finding: Deer Oaks Failed to Conduct a HIPAA Risk Analysis Prior to OCR's Investigation

- Following a complaint in May 2023, OCR's investigation substantiated allegations and verified that ePHI was accessible publicly via the Internet
- OCR determined a coding error in patient portal made patient data exposed to the Internet and cached by search engines
- OCR expanded the investigation to a breach of 172K individuals due to compromised account. Threat actor claimed it exfiltrated data and demanded ransom.

Key quotes from new OCR Director Paula Stannard:

"Identifying potential risks and vulnerabilities to ePHI is a key step in preventing or mitigating breaches of protected health information."

"Common deficiencies include lacking a risk analysis entirely or failing to update existing risk analyses when implementing new technologies or expanding operations that affect the security of ePHI."

Recommendations

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

- Assess whether your vulnerability management program is robust, timely and flexible enough to address the current threat landscape
- Enable multifactor authentication (MFA) for all services to the extent possible
- Get a third-party security assessment on any third party MSPs or other critical service providers
- Implement and execute processes for updating workforce on latest social engineering techniques
- Require multi-person approval or in-person validation for password/account resets
- Minimize user permissions and monitor for suspicious behavior on devices
- Upgrade your detection and response capabilities, and test incident response, BCP and DR processes
- 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

Enterprise Cyber Risk Management: Prioritizing and Benchmarking Risk, Building a Resilient Program

Dave Bailey, VP of Consulting Services, Security, Clearwater

Jon Stone, SVP & Chief Product Officer, Clearwater

Clearwater

Many Organizations Are Drowning in Assessments

A growing challenge for healthcare leaders

HIPAA Risk Analysis	A required process under HIPAA to identify and assess risks to all information systems with ePHI.	Identifies information systems and components. Pinpoints vulnerabilities, prioritizes mitigation, and strengthens overall security posture.
HIPAA Security Rule	Federal regulation mandating safeguards for protecting electronic protected health information (ePHI).	Ensures legal compliance, safeguards patient privacy, and avoids costly penalties.
HHS CPGs	Voluntary goals from the U.S. Department of Health and Human Services to enhance healthcare cybersecurity resilience.	Improves baseline security, aligns with federal priorities, and reduces breach risks.
NIST CSF 2.0	A flexible, risk-based security objectives framework from the National Institute of Standards and Technology to manage cybersecurity.	Strengthens risk management, enhances adaptability, and supports industry best practices. Recognized Security Practice under HITECH Act.
405(d) HICP	Practical cybersecurity guidelines developed under the Cybersecurity Act of 2015 for healthcare organizations.	Reduces common threats, simplifies compliance, and protects patient data cost-effectively. Recognized Security Practice under HITECH Act.

ECRM: See Risks Clearly

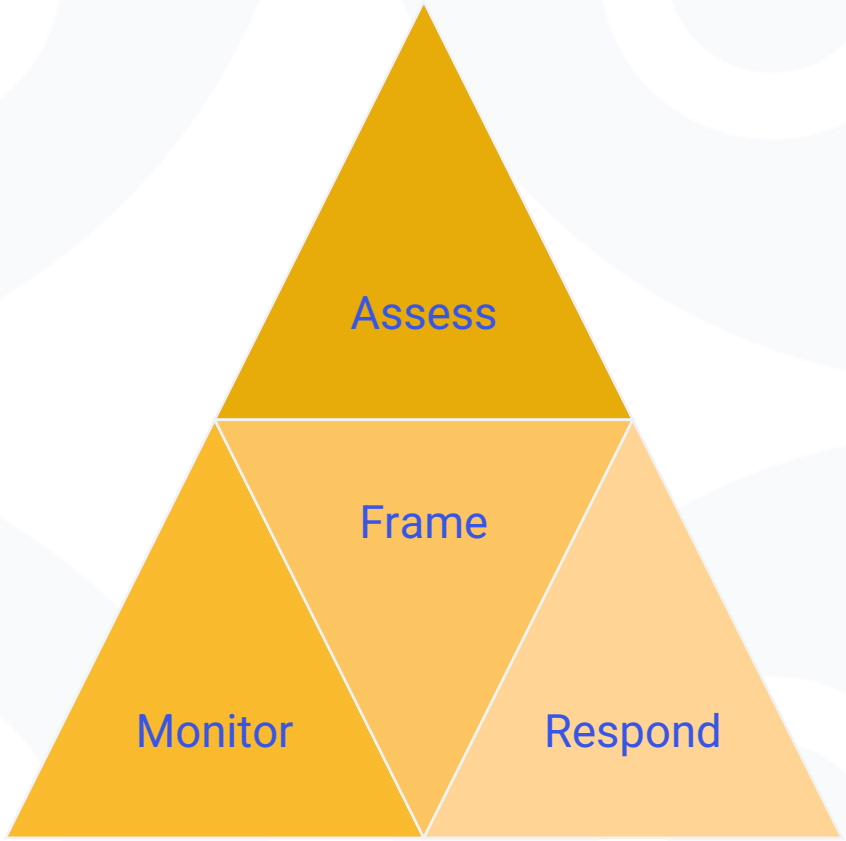
Know where you stand

- Inventory of in scope systems and component groups
- Documented criticality of systems and component groups
- Assessment of foundational and asset/component group level controls
- Asset & Component level Risk Analysis (Likelihood x Impact=Risk)
- Identify risk treatment options
- Update risk analysis as changes occur

How You Analyze Risk is Foundational to Managing It

- Your risk analysis should help you identify
  - threats to your organization (operations, assets, or individuals)
  - threats directed through your organization
  - internal and external vulnerabilities
  - the harm that may occur given the potential for threats exploiting vulnerabilities
  - the likelihood that harm will occur
- The end result is a determination of risk (the degree of harm and likelihood of harm occurring)

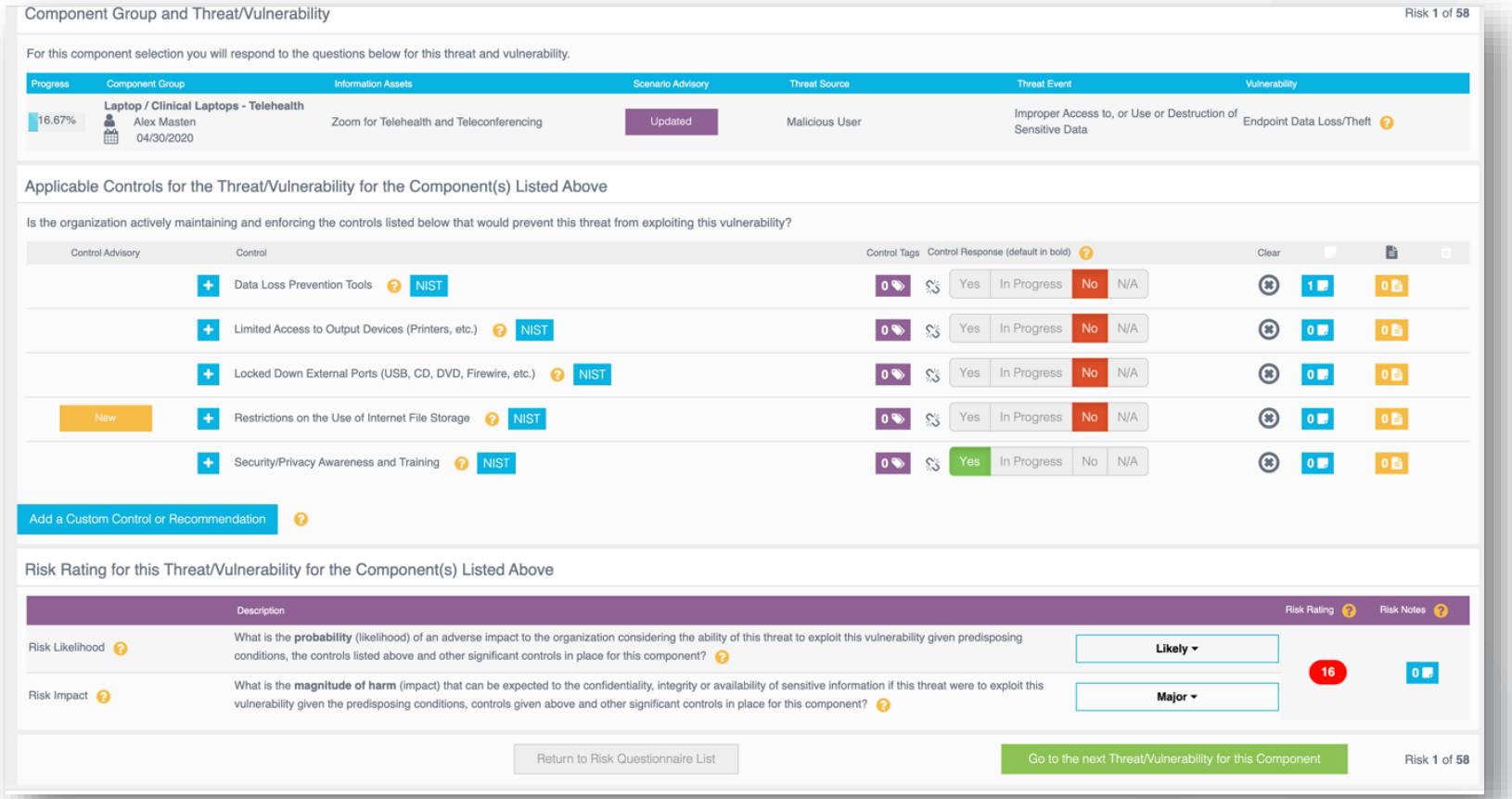
Source : NIST Special Publication 800-39



NIST Risk Management Process SP800-39

Clearwater

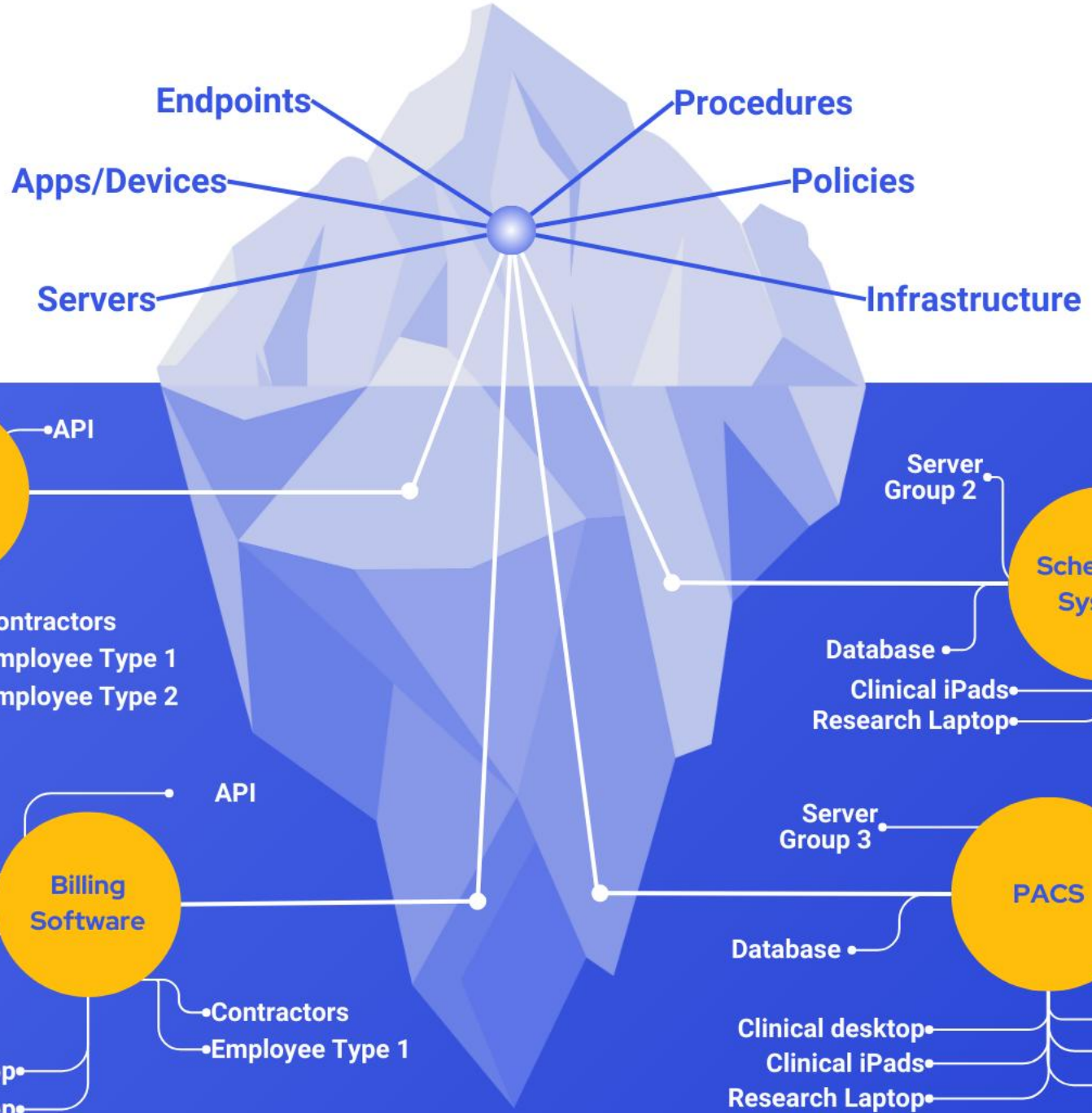
Analysis Occurs at the Asset (Component Group)-Threat-Vulnerability Level



During the Analysis Phase, reasonably anticipated threat and vulnerability combos are generated based on the qualities of each component group. Risk analysts make determinations on likelihood and impact given the safeguards in place and guided by AI recommendations.

Clearwater

Program Level Assessment



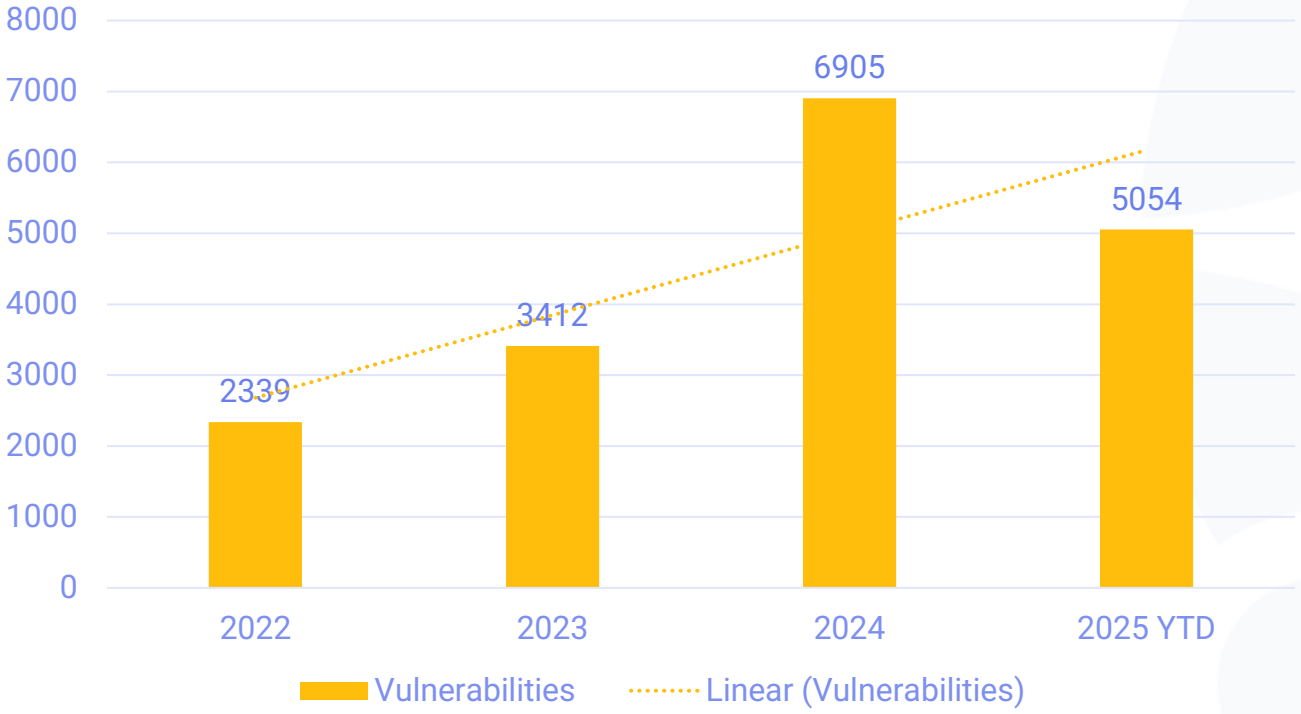
Asset-Based Risk Analysis

- **EHR**
  - Server Group 1
  - API
  - Database
  - Clinical iPads
  - Research Laptop
  - Finance Desktop
  - Contractors
  - Employee Type 1
  - Employee Type 2
- **Scheduling System**
  - Server Group 2
  - API
  - Database
  - Clinical iPads
  - Research Laptop
  - Employee Type 2
  - Contractors
- **Billing Software**
  - API
  - Server Group 1
  - Database
  - Contractors
  - Employee Type 1
  - Registration laptop
  - Finance Desktop
- **PACS**
  - Server Group 3
  - API
  - Database
  - Clinical desktop
  - Clinical iPads
  - Research Laptop
  - Contractors
  - Employee Type 1
  - Employee Type 2

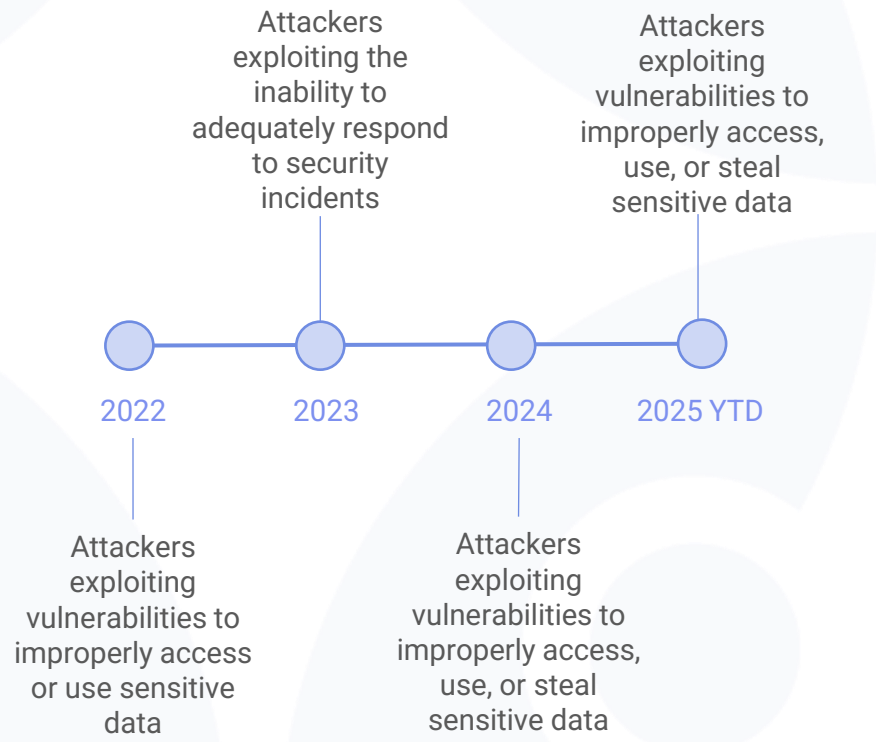
Key Findings From Clearwater's Risk Analysis Work

As the Vulnerability Trend Continues to Rise, Attackers are After Your Data

Vulnerabilities identified from risks above the threshold (Critical and High Risks)



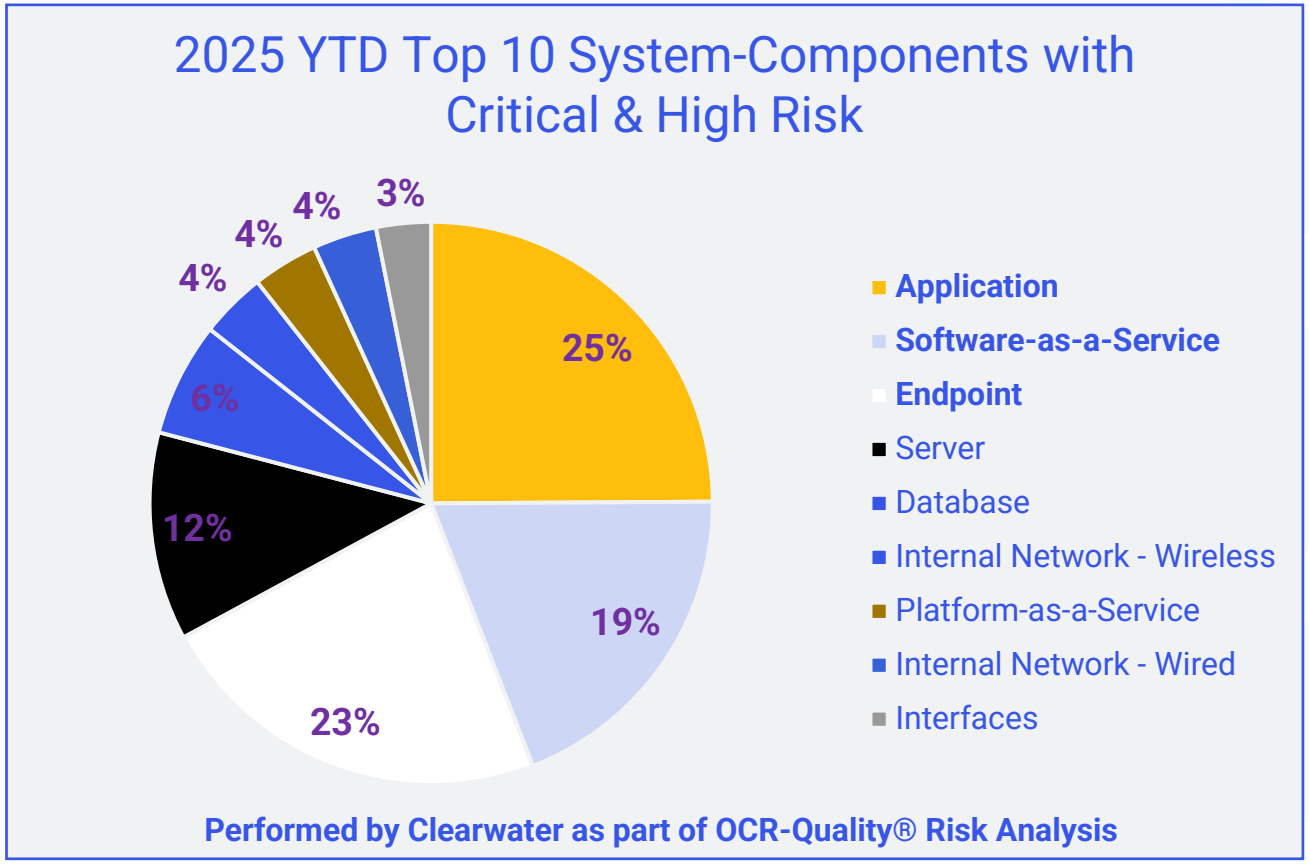
The top threat event identified as part of asset-based risk analysis



Clearwater

Asset-Based Risk Analysis Highlights How Adversaries Can Exploit the Attack Surface

Application, Software-as-a-Service and Endpoint components of systems that store, process, and transmit sensitive information are of high risk to adversarial and unintentional threats



67% of all the critical and high risks identified were from Applications, Software-as-a-Service and Endpoint Components

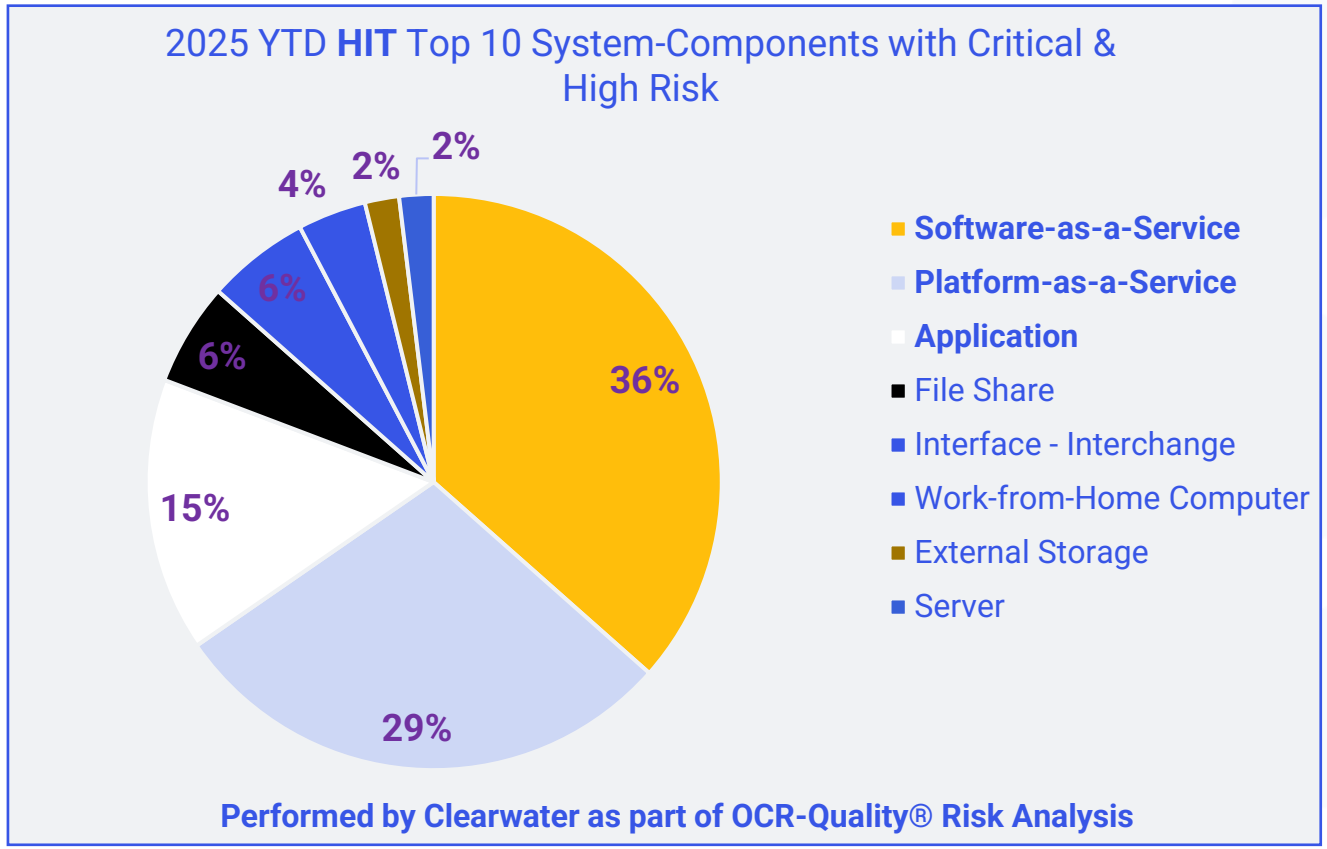
The top 5 vulnerabilities identified with the highest likelihood of exploitation:

1. User Authentication Deficiencies
2. Dormant Accounts
3. Excessive User Permissions
4. Untrained Staff
5. Network Configuration Deficiencies

Clearwater

Adversarial Threats are Most Likely to Exploit User Accounts and Poor Authentication in Digital Health

Software-as-a-Service, Platform-as-a-Service and Application components of systems that store, process, and transmit sensitive information are of high risk to adversarial and unintentional threats



80% of all the critical and high risks identified were from Software-as-a-Service, Platform-as-a-Service and Application Components

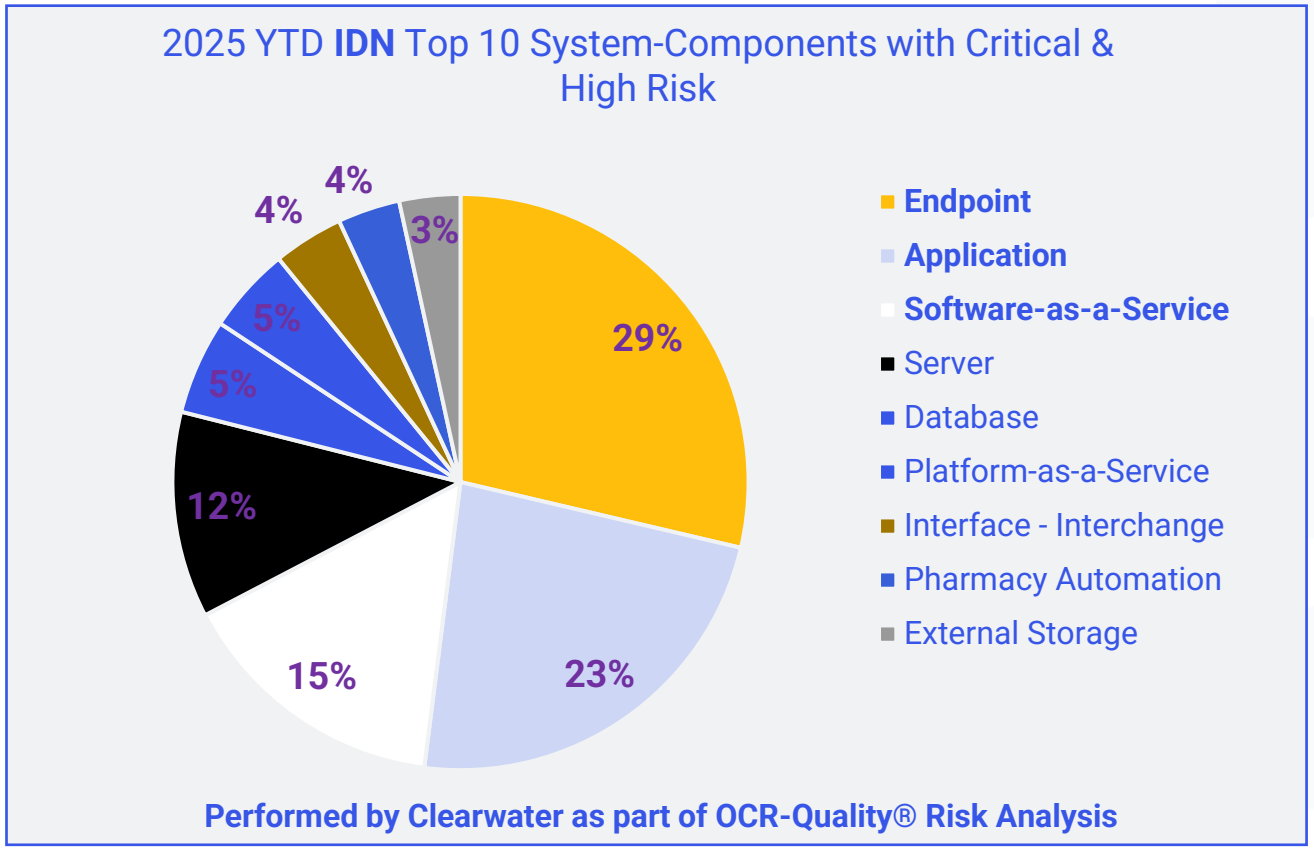
The top 5 vulnerabilities identified with the highest likelihood of exploitation:

1. Dormant Accounts
2. User Authentication Deficiencies
3. Data Leakage
4. Excessive User Permissions
5. Ransomware

Clearwater

Adversarial Threats are Most Likely to Exploit Poor Authentication and Excessive Permissions in Hospitals

Endpoint, Application and Software-as-a-Service components of systems that store, process, and transmit sensitive information are of high risk to adversarial and unintentional threats



67% of all the critical and high risks identified were from Endpoint, Application and Software-as-a-Service components

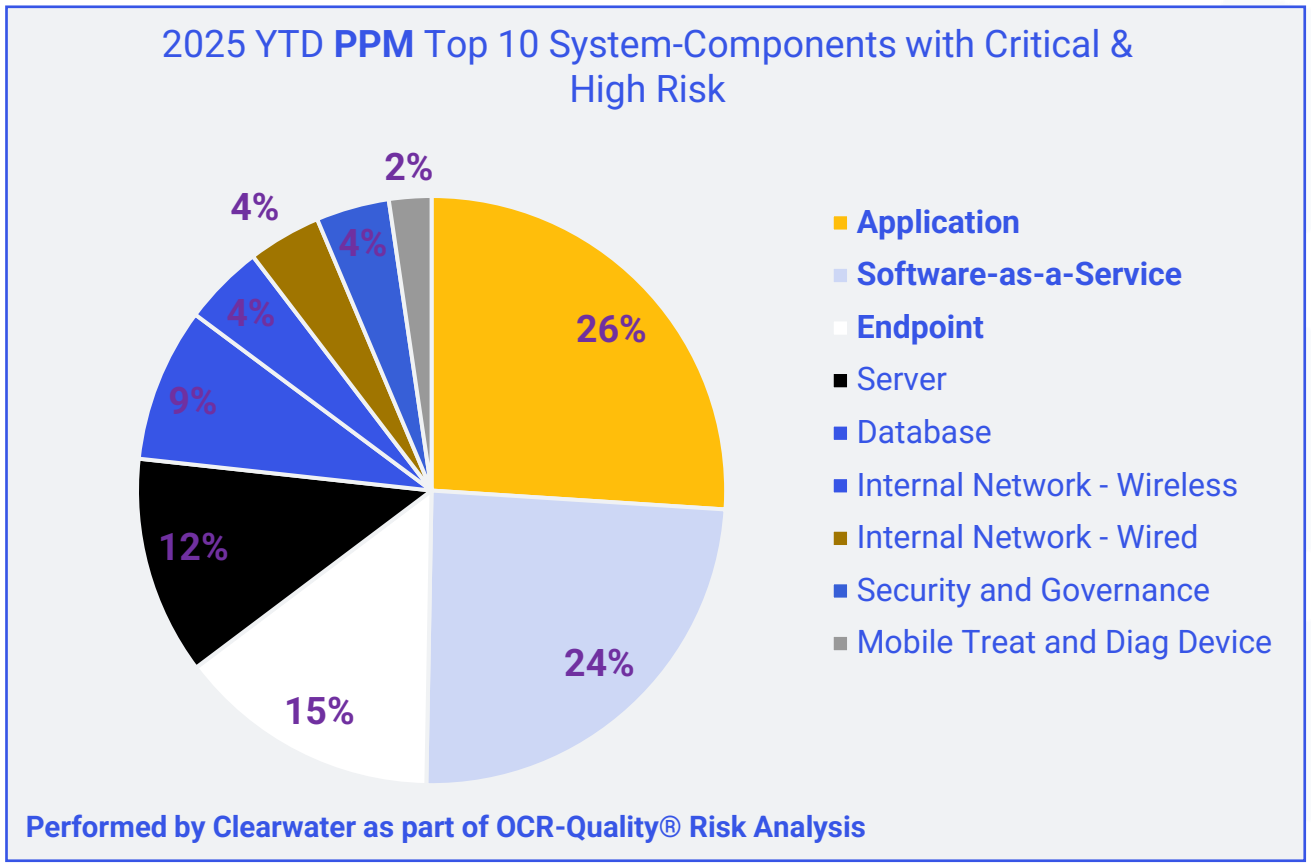
The top 5 vulnerabilities identified with the highest likelihood of exploitation:

1. Dormant Accounts
2. User Authentication Deficiencies
3. Excessive User Permissions
4. Data Leakage
5. Contractual Agreement Deficiencies

Clearwater

Adversarial Threats are Most Likely to Exploit Poor Authentication and Network Config in Physician Groups

Endpoint, Application and Software-as-a-Service components of systems that store, process, and transmit sensitive information are of high risk to adversarial and unintentional threats



65% of all the critical and high risks identified were from Endpoint, Application and Software-as-a-Service components

The top 5 vulnerabilities identified with the highest likelihood of exploitation:

1. User Authentication Deficiencies
2. Network Configuration Deficiencies
3. Excessive User Permissions
4. Untrained Staff
5. Theft of Equipment

Clearwater

Driving Real Risk Reduction Thru an Effective Risk Response Process

Respond with Precision

Follow a well-proven, five step approach to responding to risks

Initiate

- Identify program participants, responsibilities and schedules for planning.

Evaluate

- Review the risk analysis risks above threshold.
- Align risks to business processes, system components, or critical functions for clear ownership.

Treat

- Choose an appropriate response strategy for each risk:
  - Mitigate
  - Transfer
  - Accept
  - Avoid

Plan

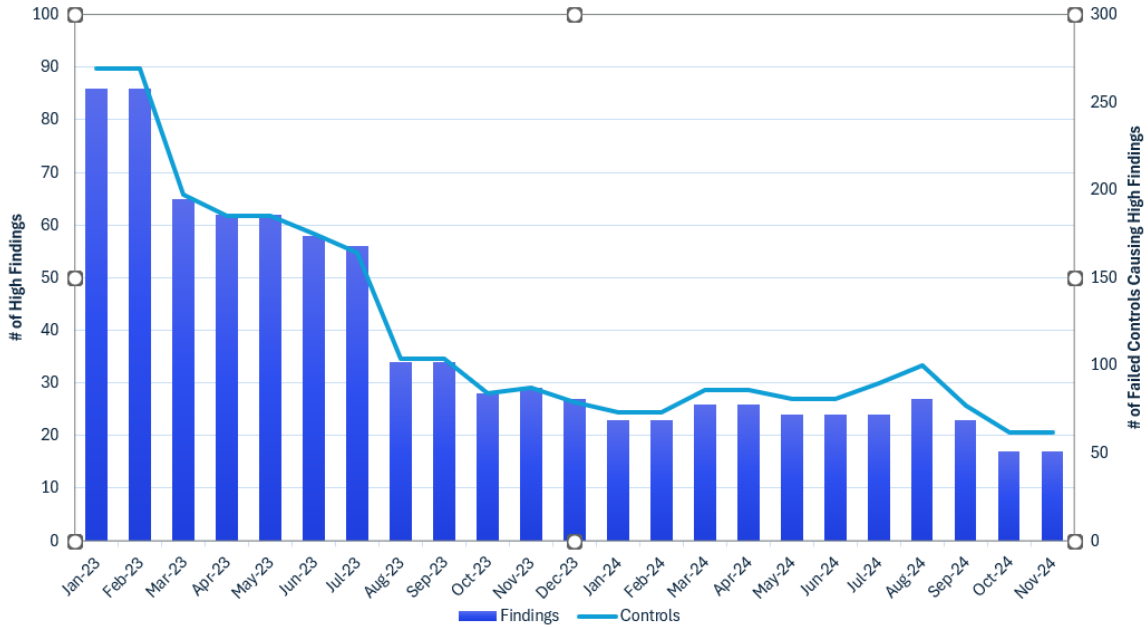
- Assign ownership.
- Define action plans, timelines, budgets, and resources required.
- Establish security controls, policies, and procedural changes.
- Ensure alignment with regulatory requirements (e.g., HIPAA, NIST CSF, 405(d)).

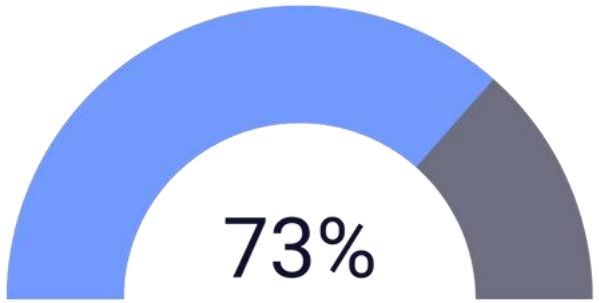
Monitor

- Track remediation efforts.
- Report progress.
- Validate new/updated controls and reconcile risks

Proven Risk Reduction Outcomes

Organizations can drive significant risk reduction and achieve measurable improvements in cybersecurity maturity in a short period of time.





Progress Year over Year

Across our client base, the average percentage of risks at or above clients' risk threshold dropped by over 73% over the course of a typical 3-year engagement.

Values generated from a sampling of actual Clearwater client outcomes.

Clearwater

Q&A

Virtual AI Summit Now On-Demand

June 23-25, 2025

Virtual Event – **Now on Demand**

- If you previously registered, the replay page has already been sent to you
- Can register now to watch on demand
- Topics include governance, regulatory developments, compliance, risk management, and cybersecurity

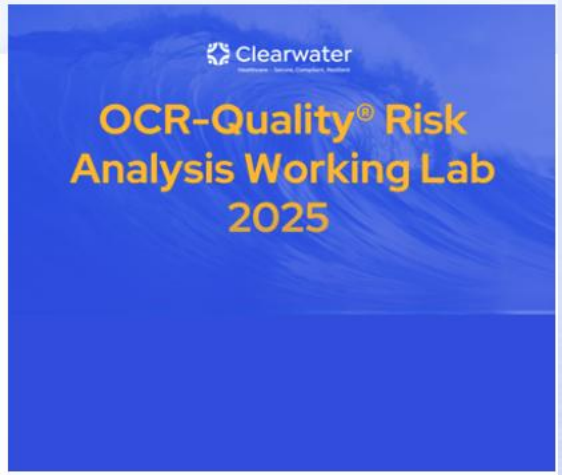
Click here to register

Clearwater

Upcoming Webinars

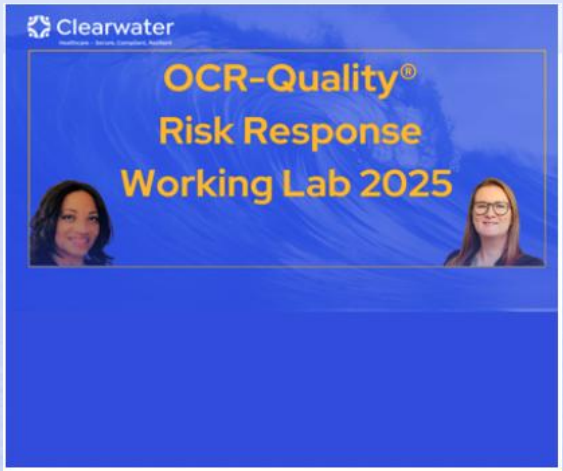
Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- (Add topic here)
- Next session August 7
- You are already registered and will automatically be enrolled in next month's briefing.



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

- 5-part webinar series every Wednesday starting August 6th This is a hands-On, Interactive E-Learning Series to help you minimize cyber risk exposures and Meet Compliance Requirements
- 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

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.