

# Monthly Cyber Briefing

June 5, 2025

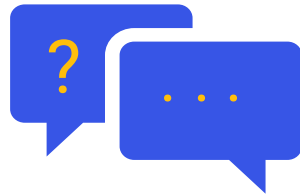


# Meeting Logistics



## 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

- Cyber & Regulatory Update
- Uncensored AI: Understanding the Rising Threat of Malicious Use by Cybercriminals
- Q+A



**Steve Akers**

CTO & Corporate CISO  
Clearwater



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

Chief Executive Officer  
Clearwater

# Cyber & Regulatory Update

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

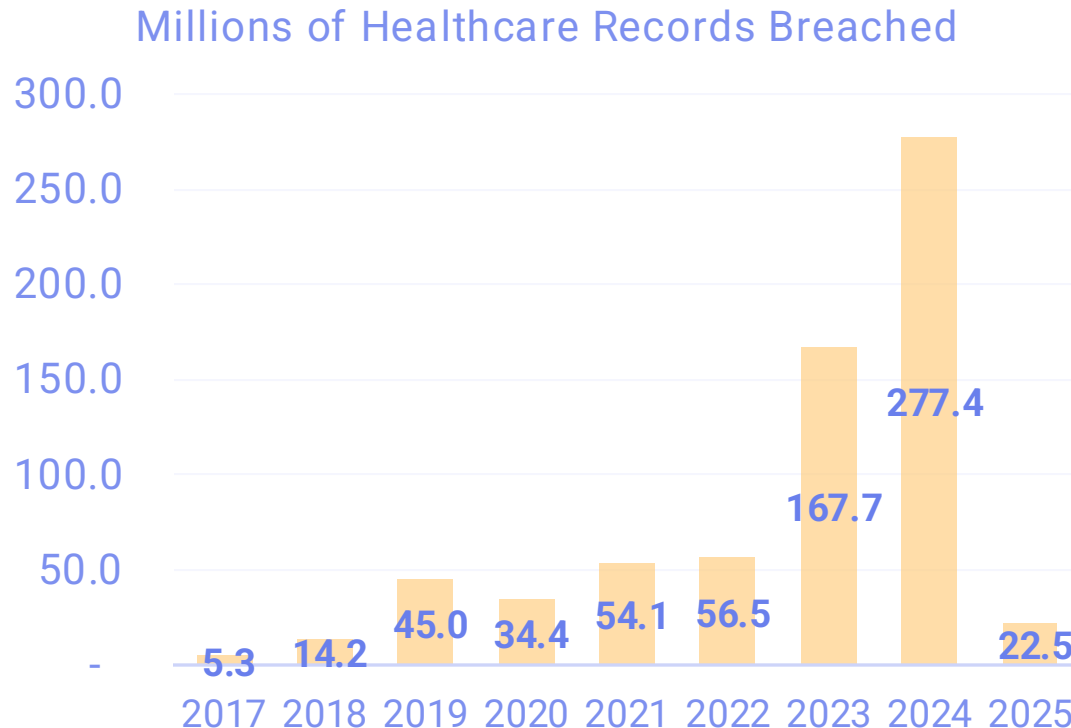
CEO, Clearwater



# Breach Reports via OCR Breach Portal

## OCR Breach Portal Data<sup>1</sup>

- 2024 breach data: 277.4M records from 734 breaches
- YTD 2025 breach data: 22.5M individuals from 295 breaches - ~3M records reported in past month

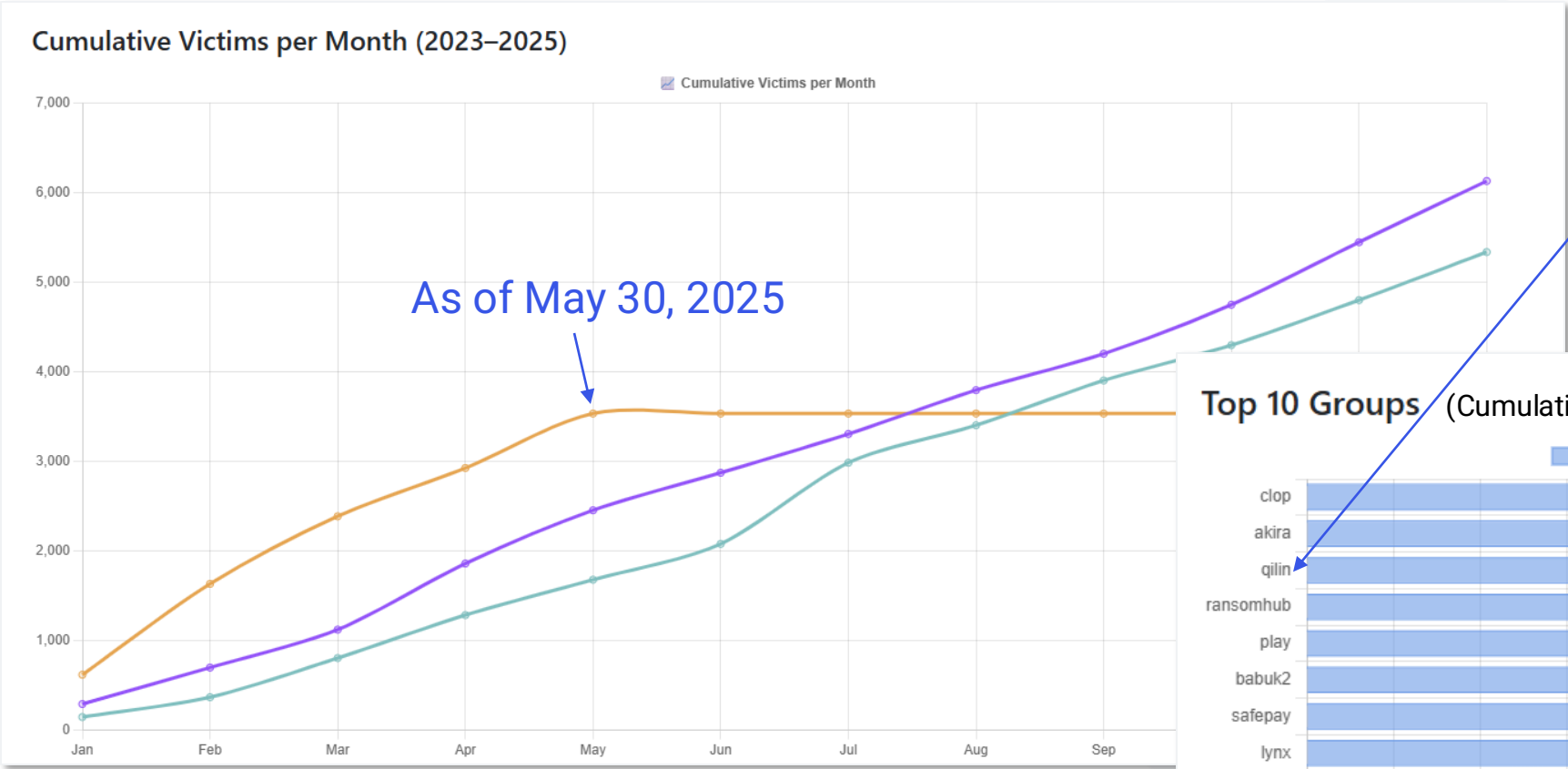


## Notable Breaches

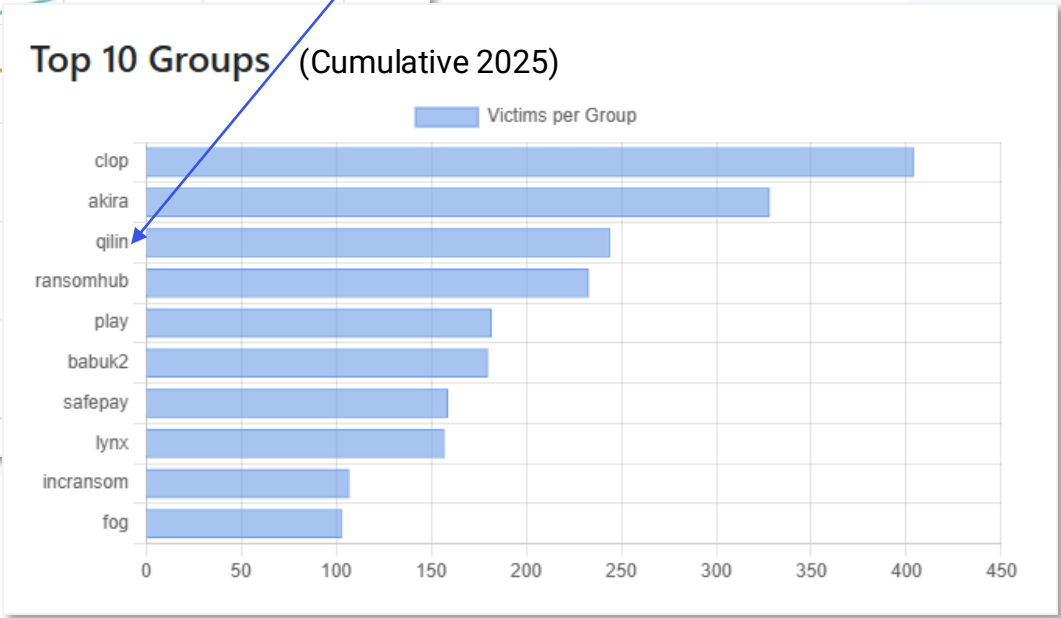
- Onsite Mammography email account compromise resulted in 357K breach
- Union Health (health system) experienced breach resulting from previously reported Cerner/ Oracle Health security incident
- Ascension inadvertently disclosed 437K records to a vendor that was breached
- Serviceaide reported a breach of Catholic Health data after exposing Cloud-based database to the web

# Global Ransomware Trends

Ransomware attacks in 2025 continue to trend well above 2024 levels. Majority are in the U.S.

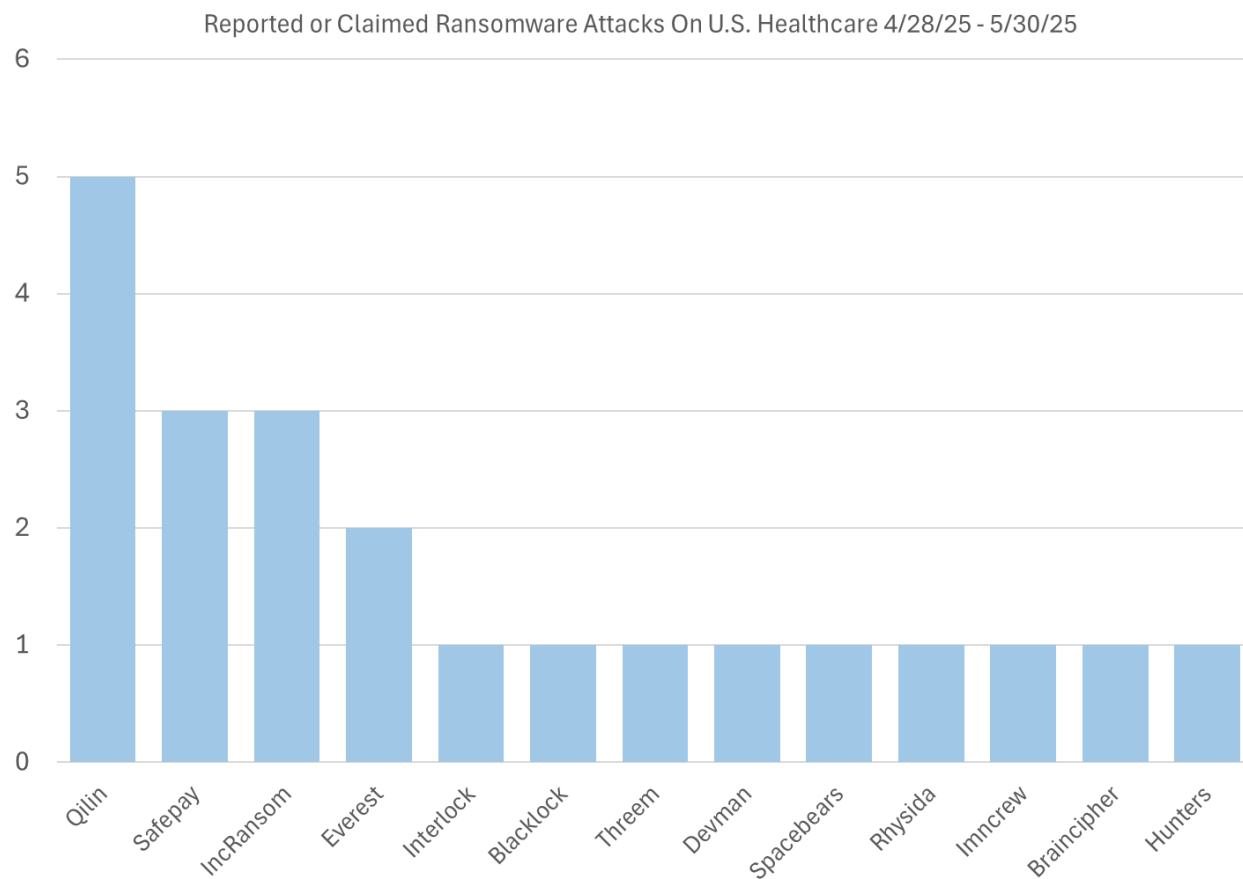


With the recruitment of much of RansomHub’s affiliate network, Qilin has quickly become a top 3 RaaS



# Ransomware Attacks on Healthcare Since Last Briefing

22 newly identified ransomware attacks on U.S. Healthcare organizations 4/28/25 – 5/30/25.\*



- Majority of attacks continue to occur on specialty provider groups, ambulatory surgical centers, physician practices, behavioral health and assisted living facilities
- Qilin had more reported attacks than any other threat actor in healthcare
  - Attacks on Clinpath (labs), The Holiday (SNF), New Season (Rehab), Dermatologists of Birmingham, and LaTouche Pediatrics
- IncRansom continues to be a front-runner
- SafePay moved to top 3 attackers after no activity last month

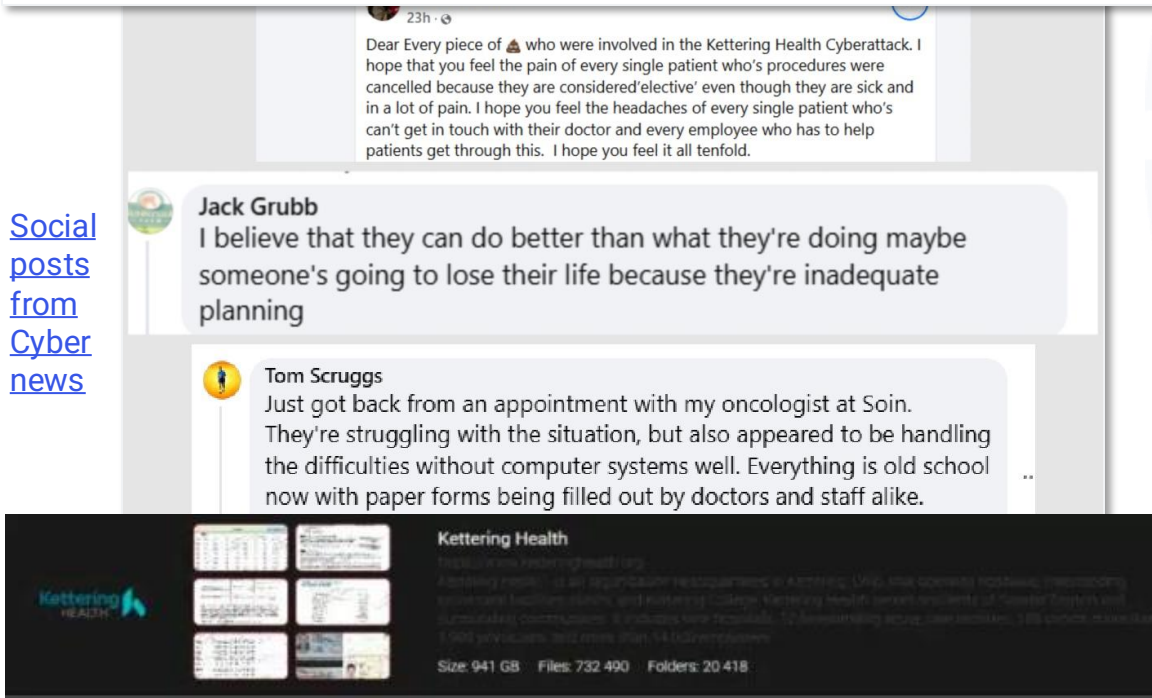


# Kettering Health Ransomware Attack

Self-described “relentless” **Interlock** attacks yet another large healthcare organization as it “enforces accountability” of security standards in healthcare.

## Kettering hospitals scramble after ransomware attack, thousands patient procedures canceled

[Social posts from Cyber news](#)



- Ransomware attack took place May 20<sup>th</sup>, causing ambulance diversion, canceled procedures, canceled radiation treatments, and other delays
- Impact spilled over to other hospitals handling higher volume
- Patients reported lack of communication and posted disgruntled messages on social media
- Secondary wave of attacks: Scammers have been calling patients claiming to be from Kettering and requesting their credit card information to pay bills
- Interlock leaked data to their leak site June 4
- **Interlock continues to be a major threat to healthcare**, and has also been observed launching new, more sophisticated malware in higher education, which we may see soon

**Refer to February 2025 Cyber Briefing where we warned of Interlock and discussed their specific tactics, techniques and procedures**



# SafePay – Emerging Threat Actor Targeting Healthcare

SafePay has shown a preference for targeting healthcare and education sectors. According to Cyble, on a global basis, it led with ransomware attacks in the month of May, overtaking Qilin.



SAFEPAY

```
1 Greetings! Your corporate network was attacked by SafePay team.
2 Your IT specialists made a number of mistakes in setting up the security of you
3 It was the misconfiguration of your network that allowed our experts to attack
4 We ve spent the time analyzing your data, including all the sensitive and confi
5 Now we are in possession of your files such as: financial statements, intellect
6 Furthermore we successfully blocked most of the servers that are of vital impor
7 We are suggesting a mutually beneficial solution to that issue. You submit a pa
8 In the event of an agreement, our reputation is a guarantee that all conditions
9 In order to contact us, please use chat below, you have 10 days to contact us,
10
11 To contact us follow the instructions:
```

*SafePay leak site and ransomware note.*

- Relatively new threat actor first noticed October 2024
- Approximately 200 ransomware attacks, with primary focus on U.S. and Germany
- Claim they work independently (not a RaaS)
- Take advantage of misconfigured firewalls to gain access, and then use password spraying or compromised credentials to gain access from internal network
- Have gained access through RDP, disable Windows Defender, and escalate privileges undetected
- Targeted data collection and exfiltration
- Search for and disable or delete back-ups making it difficult or impossible to recover

# Threat Actor Alert: Scattered Spider

Threat actor employing IT Help Desk Scams and other identity based TTPs. While they are not new, they have become much more effective, and highly successful.



- Previous HC3 alert in 2023 and updated October 2024.
- Highly active again with recent major attacks on UK retailers
- Behind well publicized attacks on UK retailers
- Use detailed research on social media to have specific information about the user they are trying to compromise
- English speaking threat actors are highly convincing
- Targeting users thought to have admin privileges
- Uses other sophisticated AI, vishing and smishing social engineering scams as well as SIM swapping and MFA fatigue

[M&S cyber attack: What we know about it and its impact](#)

# HHS OCR Update

HHS OCR has been active with several new settlements and appointing of new Director.



Paula M. Stannard announced as Director of HHS Office for Civil Rights



- Previous experience at HHS in legal affairs under first Trump and George W. Bush administrations
- Replaces Alex Azar who was in interim role

[HHS Announces Paula M. Stannard as Director of the Office for Civil Rights | HHS.gov](#)

Enforcement Actions Since Last Cyber Briefing, Both with 2 Year Corrective Action Plans

- BayCare Health System: 16 hospitals, malicious insider, 586K individuals - 5/28/25 - \$75,000
- Comstar: medical billing and collection company, ransomware, single complainant 5/30/25 - \$800,000

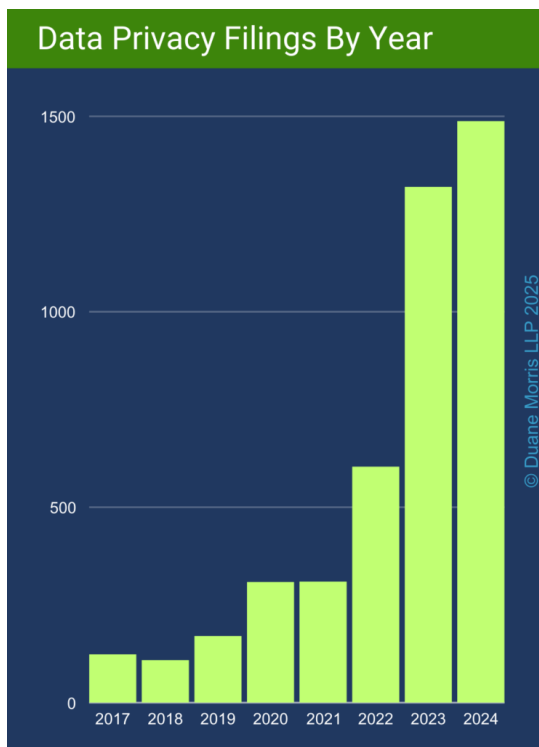
*Risk Analysis, Risk Management Plans, and Review of System Activity continue to be top areas of focus for OCR Enforcement.*

[Link to OCR's Final Guidance on Risk Analysis](#)

[Link to Differences Between HIPAA Security Evaluations and Risk Analysis - Clearwater](#)

# Data Breach Class Action Lawsuits Increasing

Data breach has emerged as one of the fastest growing areas of class action litigation, with significant costs related to responding to the litigation. 1,488 Data breach-related class action filings in 2024 vs 604 in 2022.



[January 2025 – DuaneMorris Class Action Defense](#)

## Examples of settlements reach in healthcare range from \$1M - \$65M

- Medstar – up to \$3,000 per individual (184K individuals) (Dec. 2023)
- Lee High Valley Network – \$65M (114K individuals) (Nov 2024)
- Tampa General Hospital – \$6.8M (2.1M individuals) (Jan 2025)
- Professional Finance Company – \$2.5M (1.9M individuals) (Jan 2025)
- Solara Medical Supplies – \$3M (114K individuals) (Jan. 2025)
- St. Louis University and SSM Health Saint Louis University Hospital – \$2M (93K individuals) (April 2025)
- Rite Aid – \$6.8M (2.2M individuals) (Mar. 2025)
- Practices Resources – \$1.5M (942K individuals) (May 2025)

[Doe v. LVHN - Home](#)

[MedStar data breach class action settlement](#)

[Tampa General Hospital agrees to \\$6.8 million settlement in data breach class action | Health News Florida](#)

[Class action lawsuit settlement HIPAA - Google Search](#)

[Solara Medical Supplies to pay \\$3M to settle cyber violations | HME News](#)

[Saint Louis University Agrees to \\$2 Million Settlement to Resolve Data Breach Lawsuit](#)

[Rite Aid Settles Data Breach Lawsuit for \\$6.8 Million](#)

[Practice Resources Agrees to \\$1.5 Million Data Breach Settlement](#)

# Recommendations

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

- Ensure firewalls, RDP servers, cloud environments and other points of access are configured properly. Assess security posture and perform penetration testing.
- Monitor for suspicious activity of Remote Access Tools, RDP, RMM, Powershell, etc. and attempts to disable EDR and other IOCs from TAs using Living off the Land Techniques.
- Implement and execute processes for updating workforce on latest social engineering techniques in a timely manner.
- Require multi-person approval or in-person validation for password/account resets.
- Ensure strong policies for authorizing access to ePHI, strong user access controls, and reviews to identify excess permissions or dormant accounts.
- Implement activity and log monitoring tools, and/or regularly review records of information system activity.
- Implement recognized security practices\*, and assess your organization through a third party to demonstrate adoption and compliance with your policies and controls.
- Conduct OCR-Quality Risk Analysis – all systems with ePHI (or other critical systems) must be in scope.



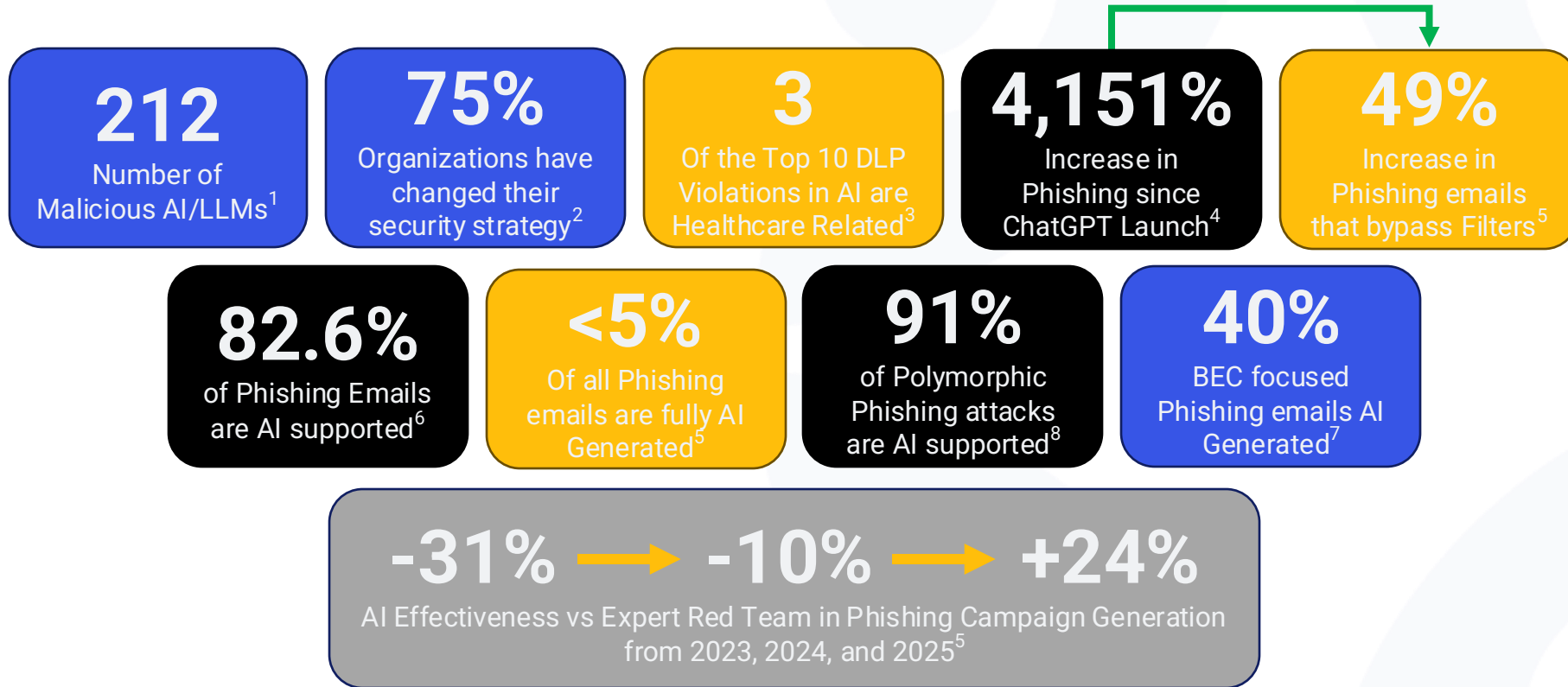
# Uncensored AI: Understanding the Rising Threat of Malicious Use by Cybercriminals

Steve Akers, CTO & Corporate CISO

Clearwater



# AI in Cybersecurity





# What are threat actors using AI / LLMs for?



## Reconnaissance

- Target Research
- Attack Methods
- Best Path for Lateral Movement
- Vulnerabilities



## Development

- Exploit Identification
- Malicious Code
- Troubleshooting
- Refinement



## Automation

- Malware Development
- Mass Phishing
- Adaptive Social Engineering
- Obfuscation
- APT Lifecycle



## Content Generation

- Deepfakes
- Video (Live)
- Voice (Live)
- Complete Persona



## Translation and Localization

- Correct Language and Context
- Culturally aligned

# How are threat actors attacking AI / LLMs?



## Prompt Injection

Providing prompts designed to circumvent the rules or boundaries

*Impact:* Divulge information or generate questionable content



## Data Poisoning

Inject fake or misleading information into training data

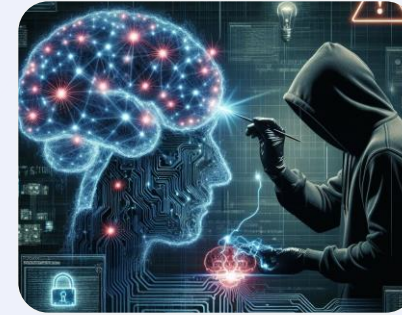
*Impact:* Accuracy or Objectivity



## Evasion

Apply subtle changes to input data shared with the model

*Impact:* Incorrect predictions or decisions



## Model Tampering

Adjust the parameters or structure of a pre-trained model

*Impact:* Accuracy of returned results

# Jailbroken vs Uncensored?

## ■ Jailbroken

- Refers to bypassing the built-in safety mechanisms/restrictions of AI Models
  - Prompt Injection | Adversarial Attacks
- Get the AI to do something it was not intended to do
  - Bypass ethical guidelines
  - Produce harmful content
  - Access/display restricted data

## ■ Why?

- Significant resources behind the largest models
  - ChatGPT, Copilot, Gemini, Alexa, and Siri
- Access to untold levels of PII, ePHI, Source Code, etc.



# Jailbroken vs Uncensored?

- Uncensored

- Refers to AI Models that can generate any type of content without regard for harm, appropriateness, or ethical boundaries
- Get it to do something other AIs won't without being jailbroken

- Why?

- Bad Guys

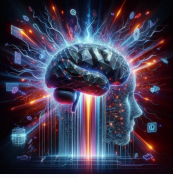
- Research, Code Troubleshooting, Content Generation, Development

- Good Guys

- Source Code Analysis, Better Testing, Training, Red and Blue Teams



# Uncensored



- Uncensored Models are a force multiplier for Threat Actors
  - Reduced knowledge/skill requirements
  - Ability to produce output equivalent to a team of “experts”
- Easily Accessible
  - Runs on consumer grade hardware
  - SaaS Model
    - Often delivered via apps like Telegram
    - Monthly/Annual/Lifetime Subscription
    - Full Upgrades and Rapid Support
    - No Logging
    - Some even have reviews!!



# Uncensored

CHATGPT LIMITATIONS

OFF

FEATURES

UNLIMITED CHARACTERS

PRIVACY FOCUSED

PERFECT CODING

PRIVACY FOCUSED

\*We do not store your personal data.

WormGPT | Private. Uncensored. Exclusive.

Take WormGPT on the go with seamless performance across all platforms, ensuring maximum privacy:

Android | Linux | Windows | MacOS / iOS iPhone

Powered by cutting-edge AI, WormGPT is your go-to for hacking, coding, and elite online operations. Achieve unmatched results for any task you throw at it.

Features:

Reasoning (Think) Feature: Solve the toughest problems in seconds with advanced logic.

File Upload: Upload code or text, analyze instantly, and break all limits.

Updated LLM Model: Get real-time, accurate data with minimal errors.

Next-Gen Encryption: Keep your chats ultra-confidential with top-tier security.

Automated Exploit Generator: Craft custom exploits for vulnerabilities in minutes.

Dark Web Scanner: Scrape dark web markets for leaked data and target intel.

Social Engineering Toolkit: Build targeted phishing campaigns with high success rates.

Malware Builder: Create undetectable keyloggers, stealers, or ransomware with ease.

AND MORE!

Example Projects with WormGPT:

Phishing Empire: Build a fake banking site with email templates to steal credentials.

Customers can DM or Telegram us for proofs and vouches. We accept Escrow. Check our Telegram and Discord for shared proofs to ensure trust.

Payment Options:

We accept cryptocurrency for secure, anonymous transactions.

BUY NOW

WORM GPT

Contact Developer / Support: <https://t.me/forsasuke>

Telegram Channel: <https://t.me/wormgptchannel> | Shut Down by Telegram Team Contact [t.me/forsasuke](https://t.me/forsasuke)

Official Website: <https://wormgpt.net/>

Note:

Customers can DM or Telegram us for proofs and vouches. We accept Escrow. Check our Telegram and Discord for shared proofs to ensure trust.

Start Contract

WormGPT Pricing

To access our High Quality product "WormGPT", we offer you payment plans. More info is given below.

MOST POPULAR

\$200 | Lifetime

Contact Us

\$100 | Monthly

Contact Us

FOR DEVELOPERS

\$550 | API Monthly

Contact Us

Lightning Fast

Lifetime Access

24/7 Support

Works On All Devices

Lightning Fast

24/7 Support

Works On All Devices

Monthly Access

Only Crypto Payments


Privacy Focused

No Limits

Lightning Fast

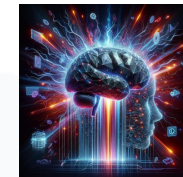
24/7 Support

Web API Support

 Clearwater

21

# Uncensored – Rapid Gains in Capability



- Same source code was provided to an uncensored AI at three intervals
- Source code was known to have five exploitable vulns
- Same starting prompts were used
- Measuring any progress in capabilities

Response Type	18 Months	12 Months	Current
Identified Vulns	2	3	5
Suggest Exploit Options	Generic	Specific	Exact
Write Exploit Paths	No	Generic	Exact
Support exploit execution	No	No	Full Toolkit Breakdown

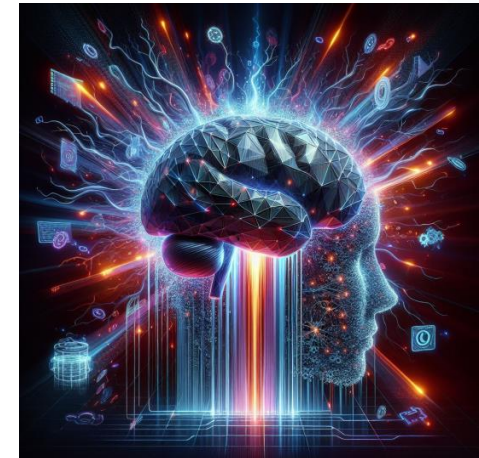




# Uncensored AI: What can be done?

# Guidance

- Recognize that change in the threat landscape has accelerated
  - Update Risk Analysis to include AI/LLM ideas and concepts
- AI/LLMs have two perspectives each with their own risks
  - Using them and building them
- Review areas for Grey Space
  - Is this in your threat model?
  - Has this been evaluated?
- Treat Data as Source Code
  - Protect it, Version Control, Integrity Checksums
- Don't Ignore the Physical Security Threats



# Guidance

- Training
  - Highlight Deepfakes – Image, Voice, and Video
- Use AI to combat AI
  - Monitor for Synthetic Content
  - Anomaly Detection to look for fake Artifacts
- Incident Response
  - How would we handle prompt injection? Data poisoning?
- Testing
- Like almost all things in Cybersecurity – not if, when
  - AI/LLMs – no different





Q&A



# Upcoming Events

**June 23-25, 2025**

Virtual Event

- Register once to attend any of the sessions.
- Featuring leading experts sharing insights and practical guidance on how to drive the responsible use of AI in healthcare
- Topics include governance, regulatory developments, compliance, risk management, and cybersecurity



[Click here to register](#)

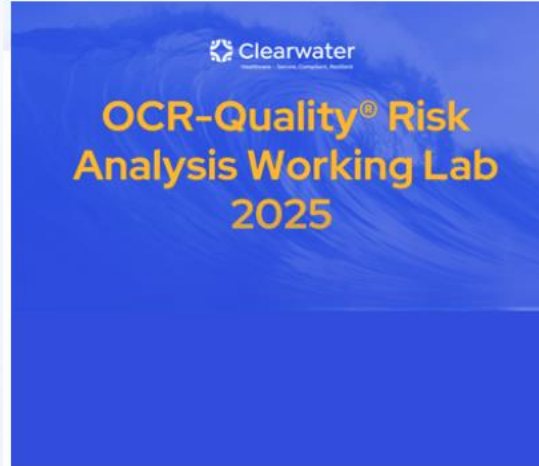


# Upcoming Webinars



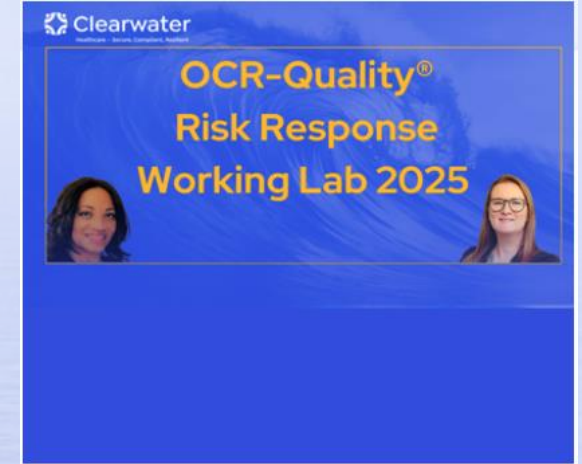
Clearwater's Monthly Cyber Briefing | 12pm – 1pm CT

- Enterprise Cyber Risk Management: Benchmarking Maturity, Prioritizing Risk, and Building a Resilient Program
- Next session July 10<sup>th</sup>
- 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](#)



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](http://www.ClearwaterSecurity.com)

800.704.3394

LinkedIn | [linkedin.com/company/clearwater-security-llc/](https://www.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

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

\*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.