# Monthly Cyber Briefing

September 5, 2024

Clearwater

# Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording, final slides, and resources shared within 24 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

# Agenda & Speakers

- Cyber & Regulatory Update
- Cloud Assumptions and Misconfigurations That Threaten Healthcare Security

**Steve Akers**

Chief Technology Officer &
Corporate CISO
**Clearwater**

**Steve Cagle**

Chief Executive Officer
**Clearwater**

Clearwater

# Cyber Update

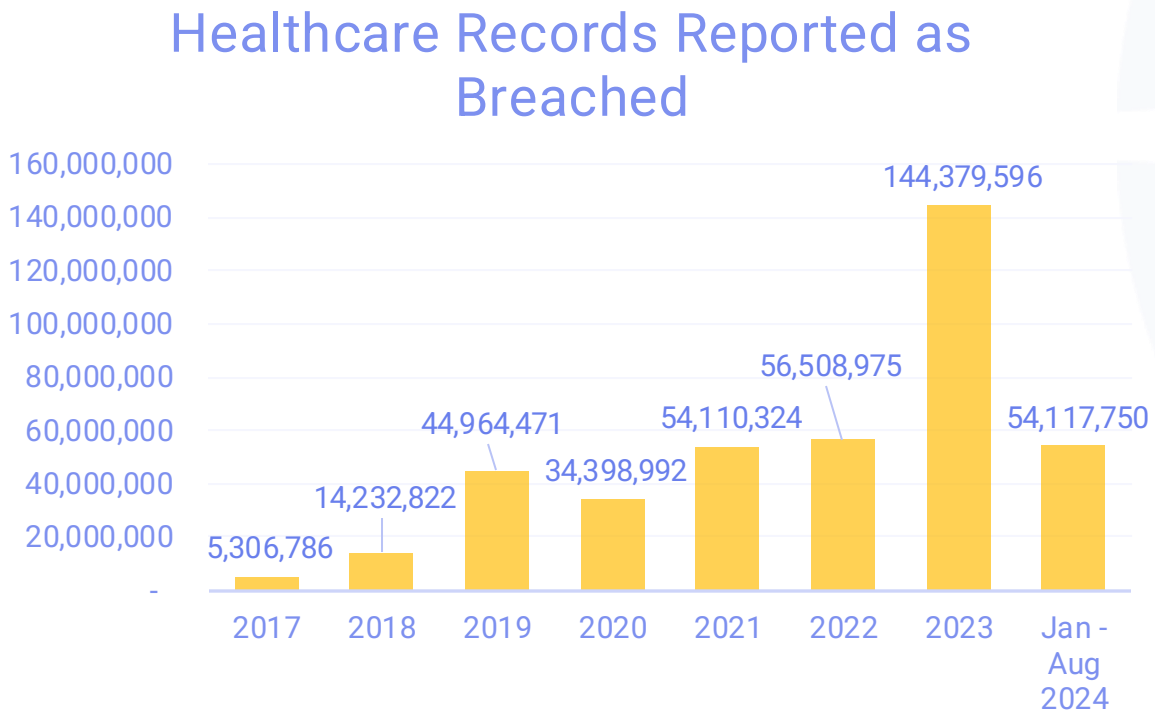
Steve Cagle

Clearwater

# Breach Reports via OCR Breach Portal and Other Sources

## OCR Breach Portal Data[1]

- 144.4M records reported breached in 2023, an increase of 156% vs 56.5 million in 2022
- 54M records from 471 breaches reported in 2024 vs 95M records and 472 breaches same period 2023




## Change Healthcare still reporting 500 records

## Notable in OCR Breach Portal

- Health Equity reported breach of 4.3 million records, second largest reported of 2024[2]

## National Public Data Breach

- Data breach involving 2.9B records, possibly largest of all time. Data goes back three decades and includes social security numbers[3]
- Recommended actions
  - Visit npd.pentester.com or npdbreach.com to see if your data was exposed
  - Change passwords
  - Run credit report and freeze your credit

Clearwater

1 The HHS Breach Portal (2024 data pulled on 8/31/24)
2 Health Equity SEC Filing hqy-20240702 (sec.gov)
3 NPD Security Incident Report (nationalpublicdata.com)

# Ransomware Key Trends H1

**57%** Increase the number of active ransomware criminal gangs

**$459M** In Ransomware payments

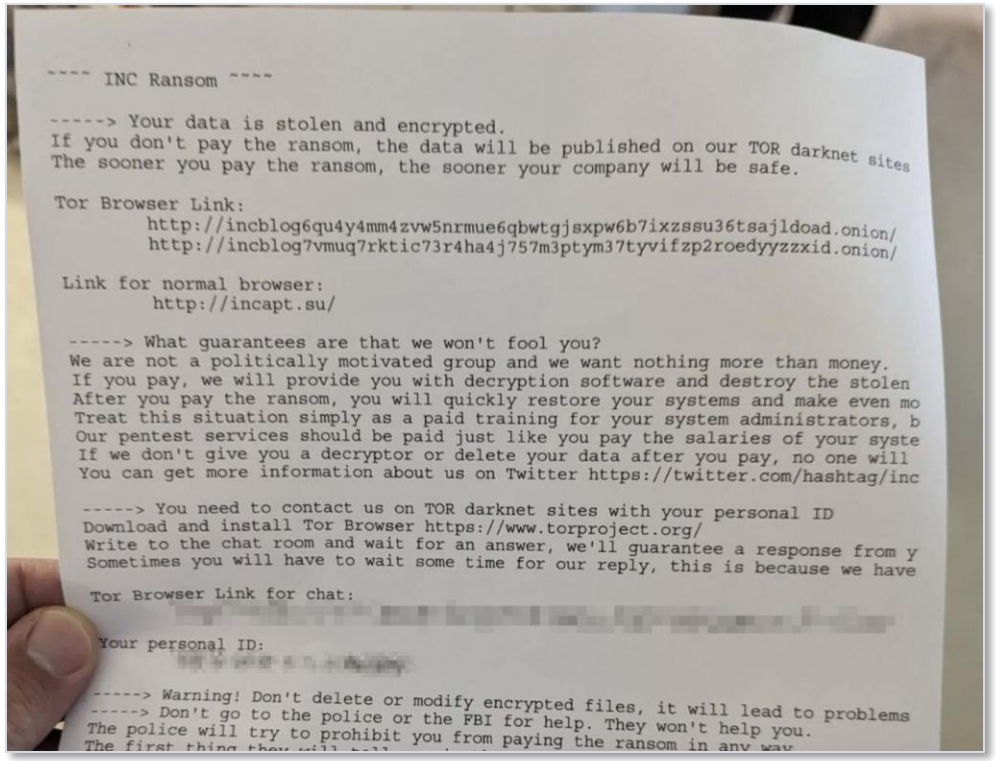
**72** Active ransomware groups

**21%** Attacks on the healthcare sector

Ransomware in H1 2024: Trends from the Dark Web (slcyber.io)
Ransomware Hit $1 Billion in 2023 (chainalysis.com)

# Ransomware: McLaren Healthcare – INC Ransomware

13-hospital McLaren Healthcare experienced a ransomware attack on August 5th impacting operations for several weeks before recently restoring them.



```
~~~~ INC Ransom ~~~~

-----> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites
The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Link:
        http://incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad.onion/
        http://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid.onion/

Link for normal browser:
        http://incapt.su/

-----> What guarantees are that we won't fool you?
We are not a politically motivated group and we want nothing more than money.
If you pay, we will provide you with decryption software and destroy the stolen
After you pay the ransom, you will quickly restore your systems and make even mo
Treat this situation simply as a paid training for your system administrators, b
Our pentest services should be paid just like you pay the salaries of your syste
If we don't give you a decryptor or delete your data after you pay, no one will
You can get more information about us on Twitter https://twitter.com/hashtag/inc

-----> You need to contact us on TOR darknet sites with your personal ID
Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from y
Sometimes you will have to wait some time for our reply, this is because we have

Tor Browser Link for chat:

Your personal ID:

-----> Warning! Don't delete or modify encrypted files, it will lead to problems
-----> Don't go to the police or the FBI for help. They won't help you.
The police will try to prohibit you from paying the ransom in any way
```

**McLaren Health Care systems restored after weeks of disruption from ransomware attack**

Kristen Jordan Shamus
Detroit Free Press

- Attack reported to have taken place August 5th
- Second ransomware attack on McLaren (previous ALPHV/Blackcat)
- Some services were canceled or delayed, including some diverted ambulance emergency services and cancer radiation treatments
- Systems restored, but data still needs to be input

McLaren hospitals disruption linked to INC ransomware attack (bleepingcomputer.com)

# Ransomware: BlackSuit (formerly Royal) Advisory

## New warnings from CISA on BlackSuit ransomware threat actor, following continued attacks on healthcare

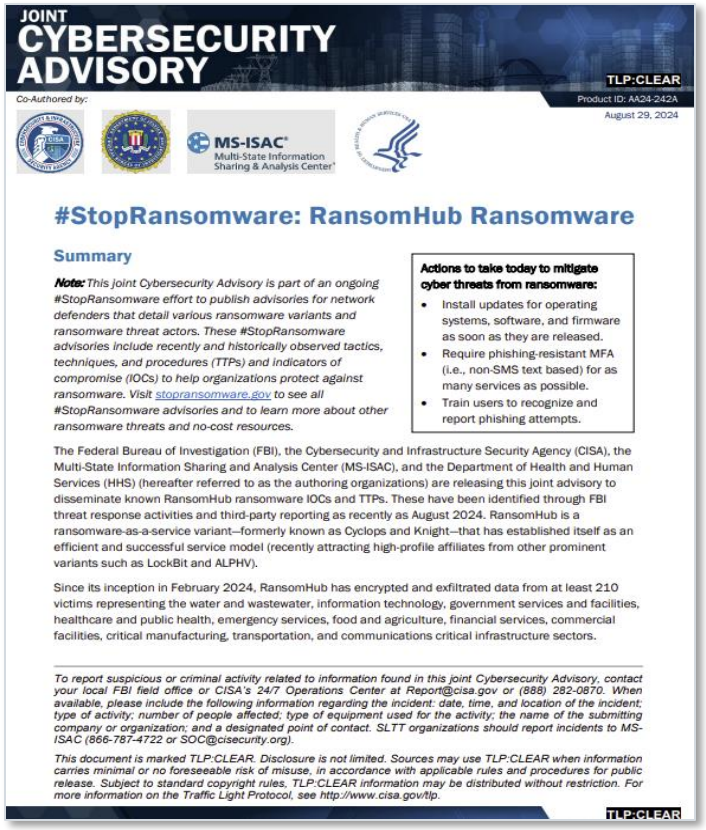

- Rebrand of Royal ransomware actors (formerly Conti), who notoriously targeted healthcare
- Ransom demands range from $1m - $10m with top demand of $60m
- Phishing email top vector of attack, followed by RDP compromise
- Evade detection by using native tools, move laterally
- After gaining access they disable antivirus software, exfiltrate data, and then deploy ransomware
- Typically use double extortion techniques

#StopRansomware: Blacksuit (Royal) Ransomware | CISA

Clearwater

# Ransomware: RansomHub

New Threat Advisory from CISA 8/29 on RansomHub ransomware threat actor, following attacks in August.



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA24-242A

August 29, 2024

Co-Authored by:

MS-ISAC Multi-State Information Sharing & Analysis Center

## #StopRansomware: RansomHub 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.*

**Actions to take today to mitigate cyber threats from ransomware:**

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Department of Health and Human Services (HHS) (hereafter referred to as the authoring organizations) are releasing this joint advisory to disseminate known RansomHub ransomware IOCs and TTPs. These have been identified through FBI threat response activities and third-party reporting as recently as August 2024. RansomHub is a ransomware-as-a-service variant—formerly known as Cyclops and Knight—that has established itself as an efficient and successful service model (recently attracting high-profile affiliates from other prominent variants such as LockBit and ALPHV).

Since its inception in February 2024, RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors.

*To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. 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. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).*



TLP:CLEAR

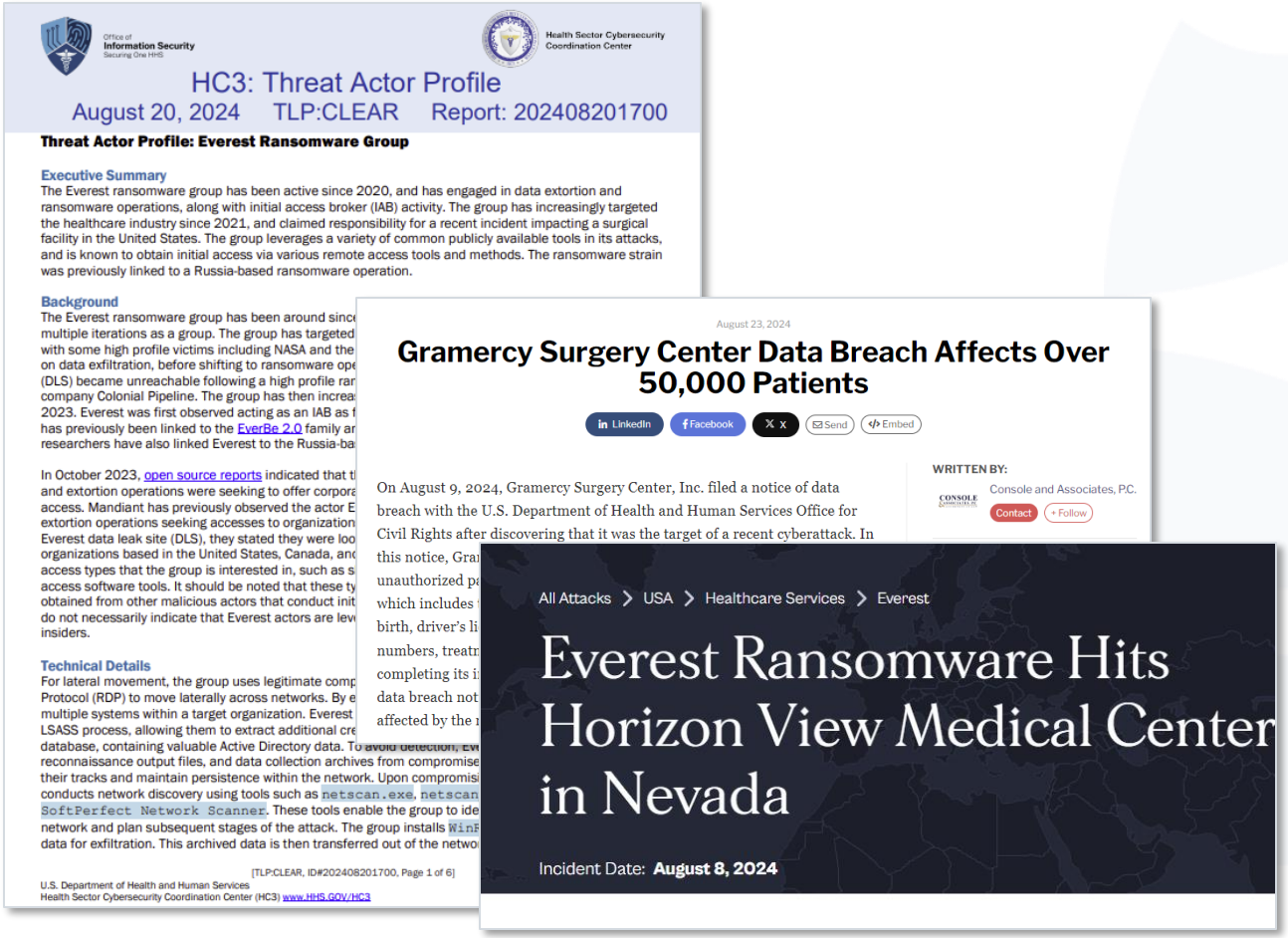
Please refer to our July 11th Cyber Briefing where I previously provided TTPs and recommended actions for RansomHub.

- Since inception in February 2024, RansomHub has encrypted and exfiltrated data from at least 210 victims in critical infrastructure including healthcare
- Attracting former affiliates of BlackCat/APLHV and Lockbit, paying 90% commission rate
- Initial access through phishing emails, exploitation of known vulnerabilities, and password spraying
- Particularly effective defense evasion techniques
- The affiliates leverage a double-extortion model by encrypting systems and exfiltrating data to extort victims

#StopRansomware: RansomHub Ransomware (cisa.gov)
Ransomware attackers introduce new EDR killer to their arsenal – Sophos News

# Everest Ransomware

## New Threat Actor Profile from HC3 following successful attacks on healthcare providers this summer.



Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Threat Actor Profile
August 20, 2024 TLP:CLEAR Report: 202408201700

**Threat Actor Profile: Everest Ransomware Group**

**Executive Summary**
The Everest ransomware group has been active since 2020, and has engaged in data extortion and ransomware operations, along with initial access broker (IAB) activity. The group has increasingly targeted the healthcare industry since 2021, and claimed responsibility for a recent incident impacting a surgical facility in the United States. The group leverages a variety of common publicly available tools in its attacks, and is known to obtain initial access via various remote access tools and methods. The ransomware strain was previously linked to a Russia-based ransomware operation.

**Background**
The Everest ransomware group has been around since
multiple iterations as a group. The group has targeted
with some high profile victims including NASA and the
on data exfiltration, before shifting to ransomware ope
(DLS) became unreachable following a high profile ran
company Colonial Pipeline. The group has then increa
2023. Everest was first observed acting as an IAB as f
has previously been linked to the EverBe 2.0 family ar
researchers have also linked Everest to the Russia-ba

In October 2023, open source reports indicated that t
and extortion operations were seeking to offer corpora
access. Mandiant has previously observed the actor E
extortion operations seeking accesses to organization
Everest data leak site (DLS), they stated they were loo
organizations based in the United States, Canada, and
access types that the group is interested in, such as s
access software tools. It should be noted that these ty
obtained from other malicious actors that conduct init
do not necessarily indicate that Everest actors are lev
insiders.

**Technical Details**
For lateral movement, the group uses legitimate comp
Protocol (RDP) to move laterally across networks. By e
multiple systems within a target organization. Everest
LSASS process, allowing them to extract additional cre
database, containing valuable Active Directory data. To avoid detection, Eve
reconnaissance output files, and data collection archives from compromise
their tracks and maintain persistence within the network. Upon compromisi
conducts network discovery using tools such as `netscan.exe`, `netscan`
`SoftPerfect Network Scanner`. These tools enable the group to ide
network and plan subsequent stages of the attack. The group installs `WinR`
data for exfiltration. This archived data is then transferred out of the netwo

[TLP:CLEAR, ID#202408201700, Page 1 of 6]
U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3

August 23, 2024

**Gramercy Surgery Center Data Breach Affects Over 50,000 Patients**

LinkedIn Facebook X Send Embed

On August 9, 2024, Gramercy Surgery Center, Inc. filed a notice of data breach with the U.S. Department of Health and Human Services Office for Civil Rights after discovering that it was the target of a recent cyberattack. In this notice, Gra
unauthorized pa
which includes
birth, driver's li
numbers, treatm
completing its i
data breach not
affected by the

WRITTEN BY:
Console and Associates, P.C.
Contact + Follow

All Attacks > USA > Healthcare Services > Everest

**Everest Ransomware Hits Horizon View Medical Center in Nevada**

Incident Date: **August 8, 2024**

- Russian speaking gang, active since 2020, may be related to Black Byte
- Attacks on healthcare increasing, especially in the Physician Practice Management space
- Engaged in data extortion and ransomware, and more recently initial access brokering
- Uses legitimate compromised user accounts and RDP to move laterally across networks
- Routinely removes tools, reconnaissance output files, and data collection archives from compromised hosts to cover tracks
- Recently began actively seeking access to corporate networks directly from employees

Clearwater

202408201700_Everest Ransomware Threat Actor Profile_TLPCLEAR (hipaajournal.com)
Dark Web Profile: Everest Ransomware - SOCRadar® Cyber Intelligence Inc.

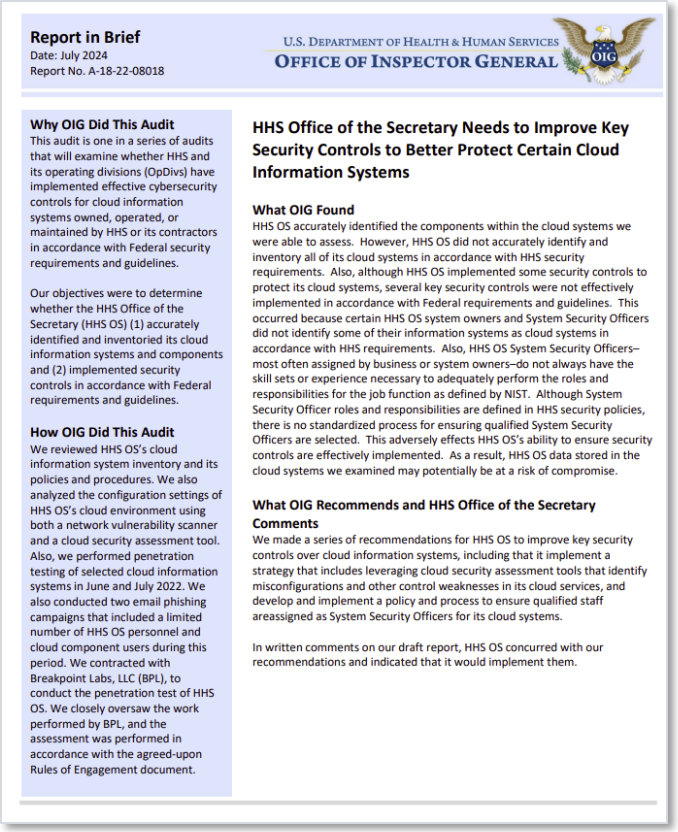
# Addressing Current Threat Environment

## Specific recommendations related to content in this briefing:

- Ensure you have a complete information asset inventory (you can't protect what you are not aware of)
- Conduct risk analysis at the information system and component level to address specific risks
- Require phishing-resistant non-SMS-based multi-factor authentication
- Educate users to both recognize and report more sophisticated phishing attempts
- Separate user and admin privileges
- Install updates for operating systems, software and firmware immediately
- Evaluate your monitoring, detection and response capabilities – are they sufficient?
- Assess third-party access. Limit as much as possible. Verify third-party controls are sufficiently followed.
- Validate security controls mapped to the MITRE ATT&CK framework (Security Controls Validation Assessment)

# Cloud Information System Security Concerns at HHS

## OIG found that HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems



**Report in Brief**
Date: July 2024
Report No. A-18-22-08018

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

**Why OIG Did This Audit**
This audit is one in a series of audits that will examine whether HHS and its operating divisions (OpDivs) have implemented effective cybersecurity controls for cloud information systems owned, operated, or maintained by HHS or its contractors in accordance with Federal security requirements and guidelines.

Our objectives were to determine whether the HHS Office of the Secretary (HHS OS) (1) accurately identified and inventoried its cloud information systems and components and (2) implemented security controls in accordance with Federal requirements and guidelines.

**How OIG Did This Audit**
We reviewed HHS OS's cloud information system inventory and its policies and procedures. We also analyzed the configuration settings of HHS OS's cloud environment using both a network vulnerability scanner and a cloud security assessment tool. Also, we performed penetration testing of selected cloud information systems in June and July 2022. We also conducted two email phishing campaigns that included a limited number of HHS OS personnel and cloud component users during this period. We contracted with Breakpoint Labs, LLC (BPL), to conduct the penetration test of HHS OS. We closely oversaw the work performed by BPL, and the assessment was performed in accordance with the agreed-upon Rules of Engagement document.

**HHS Office of the Secretary Needs to Improve Key Security Controls to Better Protect Certain Cloud Information Systems**

**What OIG Found**
HHS OS accurately identified the components within the cloud systems we were able to assess. However, HHS OS did not accurately identify and inventory all of its cloud systems in accordance with HHS security requirements. Also, although HHS OS implemented some security controls to protect its cloud systems, several key security controls were not effectively implemented in accordance with Federal requirements and guidelines. This occurred because certain HHS OS system owners and System Security Officers did not identify some of their information systems as cloud systems in accordance with HHS requirements. Also, HHS OS System Security Officers–most often assigned by business or system owners–do not always have the skill sets or experience necessary to adequately perform the roles and responsibilities for the job function as defined by NIST. Although System Security Officer roles and responsibilities are defined in HHS security policies, there is no standardized process for ensuring qualified System Security Officers are selected. This adversely effects HHS OS's ability to ensure security controls are effectively implemented. As a result, HHS OS data stored in the cloud systems we examined may potentially be at a risk of compromise.

**What OIG Recommends and HHS Office of the Secretary Comments**
We made a series of recommendations for HHS OS to improve key security controls over cloud information systems, including that it implement a strategy that includes leveraging cloud security assessment tools that identify misconfigurations and other control weaknesses in its cloud services, and develop and implement a policy and process to ensure qualified staff areassigned as System Security Officers for its cloud systems.

In written comments on our draft report, HHS OS concurred with our recommendations and indicated that it would implement them.

- More than 30% of HHS' 1,555 systems were based in the cloud
- The audit, which included all cloud systems owned, operated and maintained by HHS OS or its managed service provider contractors
- **HHS did not accurately identify and inventory all its cloud systems** in accordance with HHS security requirements
- Security officers were not assigned to cloud systems in many cases, or if assigned were not qualified
- The audit also revealed **that at least 12 key security controls - including multifactor authentication for privileged accounts and web traffic encryption for one remote server - were not effectively implemented** in accordance with federal requirements and guidelines

# Cloud Assumptions and Misconfigurations That Threaten Healthcare Security

Steve Akers

Clearwater

# Common Cloud Themes During Investigations

- Cloud is significant player
- Gaps in understanding and skill
- Use of defaults
- Hybrid increased challenges
- Cloud would make things easier

# Cloud Security Stats

**45%**
Data Breaches happen in the cloud[1]

**82%**
Human error cause behind Cloud Breach[2]

**61%**
AI will have largest impact on Cloud Security[5]

**83%**
Experience Cloud Breach Last 18 Months[2]

**58%**
Developers predict orgs. will be breached in 1 year[2]

**45%**
Believe AI will benefit adversaries the most[4]

**75%**
Cloud environment intrusion increase[6]

**110%**
Increase in cloud-conscious incidents[6]

**25%**
Fear they have a cloud breach and don't know it[2]

**No. 1**
Misconfiguration and Poor Change Control[3]

**38%**
Misconfiguration – most common threat[4]

**35%**
Misconfiguration – most concerning threat[4]

Clearwater

[1]IBM Cost of Data Breach
[2]SentinelOne Cloud Breach Stats
[3]Cloud Security Alliance 2024 Top Threats
[4]Splunk State of Security 2024
[5]Dark Trace State of Security 2024
[6]Crowdstrike 2024 Global Threat Report

# Cloud Assumption No. 1

## A Cloud environment is just like a corporate network

| Underlying Premise | Reality of the Situation |
|---|---|
| The same skills apply to managing the Cloud as it does for on-premise | Cloud environments operate under different operational and technical rules |
| It is the Cloud, it already has segmentation | Just like on-premise, Cloud environments need proper segmentation |
| Deploying servers within the Cloud that were on premise | This often leads to excessive consumption costs, poor performance, and lack of scale |

Example: Deploying an MS-SQL Server, versus using Native Azure SQL Services

# Cloud Assumption No. 2

## The Cloud provider takes care of cybersecurity and compliance

| Underlying Premise | Reality of the Situation |
|---|---|
| In the Cloud they take care of security and compliance matters for their subscribers | Mostly inward. Good start – but like any tool, must be used properly to be effective |
| The access controls for the Cloud environment are the same as on-premise | Organizations can struggle using non-traditional firewall technologies |
| Additional monitoring of the environment is not needed as the provider does this | Some, but limited. Need to setup proper monitoring and alerting |

Example: Showing all the compliance failures in Azure Compliance Manager for a new tenant
Realizing there are no default quarantine rules for Defender for Endpoint

# Cloud Assumption No. 3

## The Cloud environment's default settings are optimized

| Underlying Premise | Reality of the Situation |
|---|---|
| Leverage the defaults established by the Cloud provider | The defaults are optimized to deliver core features at the lowest cost to the provider |
| The Cloud provider has enabled all the logging needed for security and compliance | Most logging is limited in time, content, and not enabled |
| The retention periods for data and events are aligned with subscriber needs | Retention on many levels is simply below compliance requirements |
| Backups are handled by the Cloud provider | Backups must be enabled, and often are not comparable to third party tools |

Example: Defender Notifications, Alerting, and Sentinel Integrations not being fully enabled

# Cloud Assumption No. 4

## Operational formalities are not needed in the cloud

| Underlying Premise | Reality of the Situation |
|---|---|
| Everything is tracked in the Cloud, so change management/control is not needed | Poor controls in these areas lead to misconfigurations and unapproved changes |
| Configuration review, vuln mgmt., and pen tests are not needed for the Cloud | Without proper review, basic mistakes can lead to significant exposure and risks |
| User and Identity Management will become easier and less stringent in the Cloud | Users will end up with excessive privileges, stale and dormant accounts will exist |
| Third-party integrations in the Cloud will be secure and require less overhead | Third parties will end up with unmanaged access to critical data and resources |

Example: Endpoints and Servers not being added to a patch and update policy

# Cloud Assumption No. 5

## The choices made in the development environment won't be in production

| Underlying Premise | Reality of the Situation |
|---|---|
| Insecure API configuration will be addressed prior to go live | Many APIs remain insecure, are never tested, and remain "On" 24x7 |
| Broad access rights will be limited before production roll out | Developers maintain access to production, rights are not removed/limited |
| Backend configurations enabled to make work easier will be disabled | Configurations stay enabled |
| Enable Encryption and Conditional Access as part of go live preparations | Enabling these at the last minute creates problems, and are delayed or deferred |

Example: Encrypt data at rest in Azure Storage Accounts is not on be default

# Supporting Information

- Assumptions align with threats
- Slight changes in two years
- Need for cloud-specific skills
- Dive In vs. Formal Strategy
  - Often driven by Development

| 2024 | | 2022 |
|---|---|---|
| Misconfiguration & Inadequate Change Control | 1 | Identity & Access Mgmt (IAM) |
| Identity & Access Mgmt (IAM) | 2 | Insecure Interfaces and APIs |
| Insecure Interfaces and APIs | 3 | Misconfiguration & Inadequate Change Control |
| Inadequate Selection/ Implementation of Cloud Security Strategy | 4 | Inadequate Selection/ Implementation of Cloud Security Strategy |
| Insecure Third-Pary Resources | 5 | Insecure Software Development |
| Insecure Software Development | 6 | Insecure Third-Party Resources |
| Accidental Cloud Disclosure | 7 | System Vulnerabilities |
| System Vulnerabilities | 8 | Accidental Cloud Disclosure |
| Limited Cloud Visibility/ Observability | 9 | Misconfiguration & Exploitation of Serverless & Container Workloads* |
| Unauthenticated Resource Sharing | 10 | Advanced Persistent Threats |
| Advanced Persistent Threats | 11 | Cloud Storage Data Exfiltration* |

[1]Cloud Security Alliance Top Threat to Cloud 2024

Clearwater

# Key Take Aways - Operational

- Assess risk – Ensure Cloud environments are included
- Understand internal skills – Training and Certs
- Clouds are and can be very complex – seek a trusted third party
- Evaluate Partners / MSP and CSP – Are they Cloud skilled?
  - Ask these important questions:
    - Do they understand security and compliance?
      - Be prepared with detailed questions that would indicate the MSSPs understanding
    - Can they explain in detail how they get you to your end goal without generic responses?
    - Is there a focus on end user experience, versus cookie cutter solutions?

# Key Take Aways - Technical

- Trust but verify – Third-Party Cloud Assessment, Pen Testing
  - Ensure assessor has deep cloud experience
- Implement Zero Trust/Zero Trust Network Access
  - Never Trust, Always Verify
  - Authenticate First, Connect Second
- Enable Conditional Access
- Use Security as design constraint, versus obstacle to overcome

# Q&A

# Upcoming Webinars

**Making the Move to Proactive Patient Privacy Monitoring | September 10**

- Experts from Clearwater and Protenus will team up for a discussion of how to make the move to proactive patient privacy monitoring that extends across and beyond your organization and helps minimize the risk of a breach.
- Register Here

**OCR-Quality Risk Response Working Lab | September 18**

- 2-part series
- Hands-On, Interactive E-Learning Series to Help You Minimize Cyber Risk Exposures and Meet Compliance Requirements.
- Register Here

**View from Washington: How Cybersecurity Legislative Activity May Impact Healthcare Organizations | Monthly Cyber Briefing on October 3**

- Clearwater's CEO, Steve Cagle and Mari Savickis, VP, Public Policy with CHiME
- Register Here (Cyber Briefing attendees are already registered)

# Upcoming Industry Events


## Healthtech Leader 3.0 | Sept 18-20 | Cleveland, OH

- Clearwater is a proud sponsor.
- Join our CEO, Steve Cagle, Director of Partnerships, Robyn Ewers, and Account Executive, Laura Martin, and connect with influential leaders in security, technology, and data & analytics.
- Register Here


## HHA Governance Retreat | Sept 19-20 | Lincoln, NE

- Clearwater Chief Risk Officer and Head of Consulting Services and Client Success Jon Moore will be presenting "Protecting Patients in an Age of Robots & Outlaws: Governance Strategies for Small Hospitals in AI and Cybersecurity".
- Register Here


## McGuireWoods Healthcare Finance & Growth Conference | Sept 25-26 | Charlotte, NC

- Join our session at 2:20pm on Thursday, Sept 26, and hear insights from Clearwater CFO Baxter Lee and our CRO and Head of Consulting and Client Success Jon Moore as well as Colin McCarthy, Counsel with McGuireWoods' Healthcare team for PE Firms and investors active in healthcare.
- Register Here


## SCALE Healthcare Leadership Conference | Oct 1 | New York, NY

- Clearwater is a platinum level sponsor. Join us for a fireside chat at 11:00 am featuring our CEO, Steve Cagle, and Gen4 Dental Partner's CIO, Scott Dever.
- Register Here


## HITRUST Collaborate | Oct 1-3 | Frisco, TX

- Clearwater Senior Principal Consultant John Santana is teaming with our client James Polanco, CTO for ForeSee Medical, Inc to deliver the presentation "Turning Your Security-First Approach into a Competitive Advantage". Breakout session is slated on Tuesday, Oct. 2, at 10:30am.
- Register Here


## Nashville Healthcare Sessions | Oct 7-9 | Nashville, TN

- Clearwater is hosting a dynamic collaboration with cybersecurity experts from Jarrard and 1stReponder for an exclusive live cybersecurity incident response simulation. Join us Tuesday, Oct 8 at 10:45 am.
- 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.