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.

Monthly Cyber Briefing

March 2024

Clearwater

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda & Speakers

- Cyber update
- Quarterly Threat Review

Steve Cagle

CEO

Clearwater

Dave Bailey

VP, Consulting Services

Clearwater

Steve Akers

CTO, Managed Security Services,
CISO

Clearwater

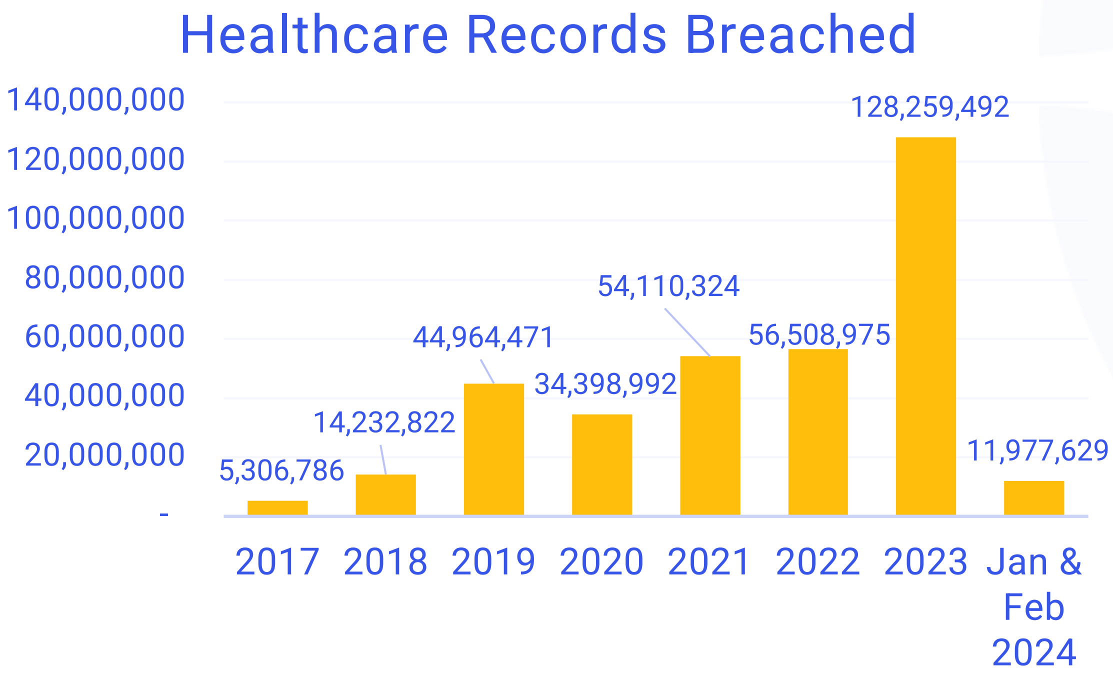
Cyber Update

Steve Cagle

Clearwater

Breach Reports via OCR Breach Portal[1]

- 135.3M records reported breached in 2023, and increase of 139% vs 56.5 million in 2022
- 734 breaches reported in 2023 vs 720 in 2022, a slight increase year over year
- About 12 million records (104 breaches) reported Jan – Feb 2024. Annual run Rate of 72M records … however, Change Healthcare Breach (not yet reported) has the potential to be one of largest of all time in healthcare



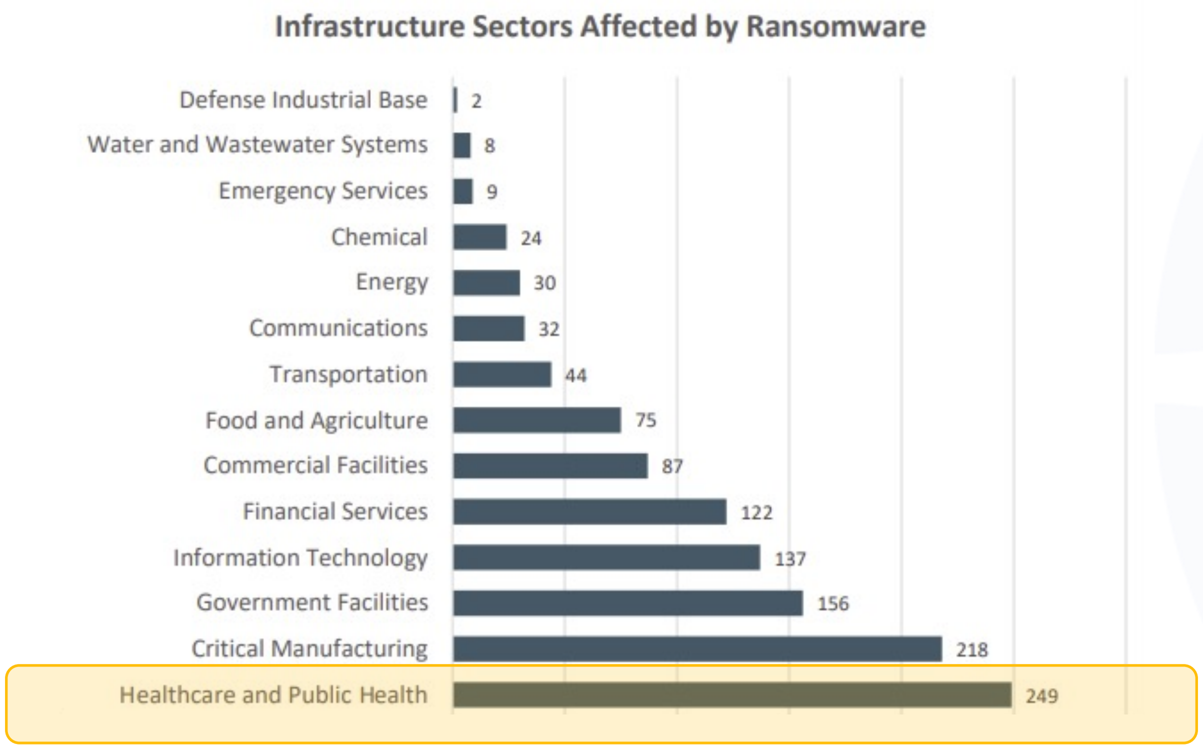
Top Breaches Reported to OCR in 2024

- Concentra Health Services, Inc. 4.0M (PJ&A)
- Integris Health 2.4M – Ransomware
- North Kansas City Hospital 502K (PJ&A)
- Medical Management Resource Group (dba American Vision Partners) 2.35M – Hacked Network

Clearwater

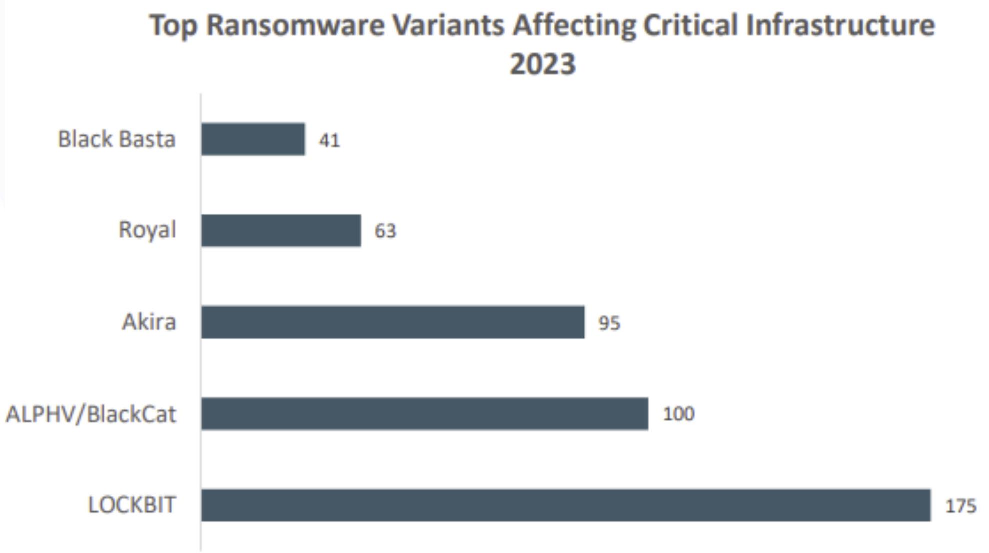
[1] HHS Breach Portal (data pulled March 3, 2024).

2023 FBI Internet Crime Report (just released)



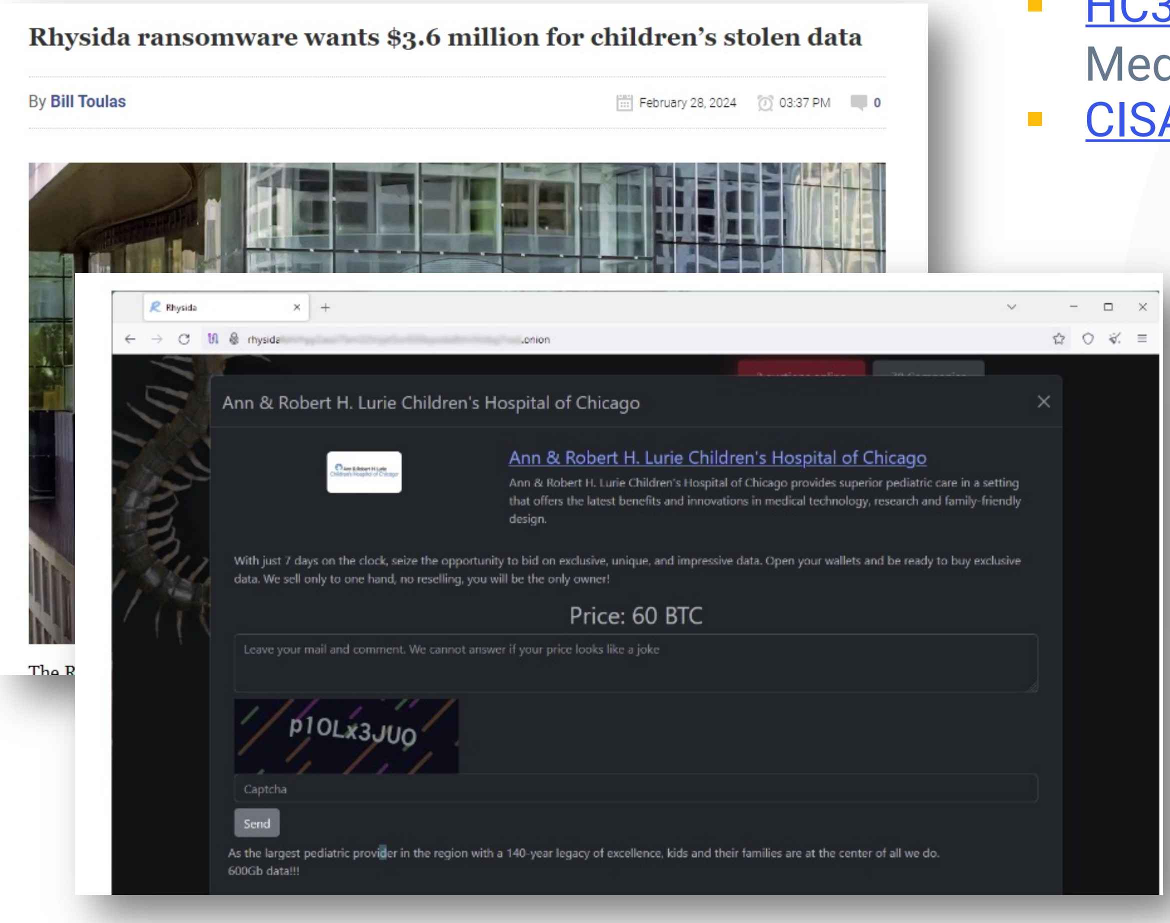
2023 FBI Internet Crime Report.pdf

- Healthcare continues to be the most targeted critical infrastructure industry by ransomware gangs
- Total losses from internet crime increased in the U.S. by 22% in 2023 to $12.5 Billion



Rysida Ransomware – Lurie Children’s Hospital, Chicago

- HC3 issued a sector alert 8/4/23 following Prospect Medical Attack.
- CISA issued a Rhysida Ransomware Advisory 11/15/23



Rhysida ransomware wants $3.6 million for children’s stolen data

By Bill Toulas   February 28, 2024   03:37 PM   0

The R

Ann & Robert H. Lurie Children's Hospital of Chicago

Ann & Robert H. Lurie Children's Hospital of Chicago

Ann & Robert H. Lurie Children's Hospital of Chicago provides superior pediatric care in a setting that offers the latest benefits and innovations in medical technology, research and family-friendly design.

With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data. Open your wallets and be ready to buy exclusive data. We sell only to one hand, no reselling, you will be the only owner!

Price: 60 BTC

Leave your mail and comment. We cannot answer if your price looks like a joke

p1OLx3JUQ

Captcha

Send

As the largest pediatric provider in the region with a 140-year legacy of excellence, kids and their families are at the center of all we do. 600Gb data!!!

Office of
Information Security
Securing One HHS
Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

August 4, 2023   TLP:CLEAR   Report: 202308041500

Rhysida Ransomware

Executive Summary

Rhysida is a new ransomware-as-a-service (RaaS) grou
drops an eponymous ransomware via phishing attacks
deploy their payloads. The group threatens to publicly
paid. Rhysida is still in early stages of development, as
program name Rhysida-0.1. The ransomware also leav
victims to contact the group via their portal and pay in
several countries across Western Europe, North and S
education, government, manufacturing, and technolog
there has been recent attacks against the Healthcare

Overview of Rhysida

First oberved on May 17, 2023, following the emergen
(.onion), Rhysida describes itself as a "cybersecurity te
security issues and secure their networks. While not m
affiliations, the name Rhysida is a reference to the Rhy
on their victim blog. The TOR page also shows the curr
group's website also serves as a portal for Rhysida-cer
how to contact the group should journalists, recovery f

Rhysida is a 64-bit Portable Executable (PE) Windows
using MINGW/GCC. In each sample analyzed, the appl
suggesting the tool is in early stages of development.
strings revealing registry modification commands.

Rhysida ransomware is deployed in multiple ways. Prin
via phishing attacks, and by dropping payloads across
Strike or similar command-and-control frameworks. Of
RaaS group, Black Basta, detailed how both threat gro
Group/Carbon Spider), share a TTP in their employmen

When Rhysida runs, one cybersecurity firm observed a
which apparently scans the files, runs the "file_to_cryp
extension to ".rhysida":

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR   Product ID: AA23-319A

November 15, 2023

#StopRansomware: Rhysida Ransomware

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders detailing 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 malicious cyber activity:

- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Segment networks to prevent the spread of ransomware.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known Rhysida ransomware IOCs and TTPs identified through investigations as recently as September 2023. Rhysida—an emerging ransomware variant—has predominately been deployed against the education, healthcare, manufacturing, information technology, and government sectors since May 2023. The information in this CSA is derived from related incident response investigations and malware analysis of samples discovered on victim networks.

FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of Rhysida ransomware and other ransomware incidents.

For a downloadable copy of IOCs, see:

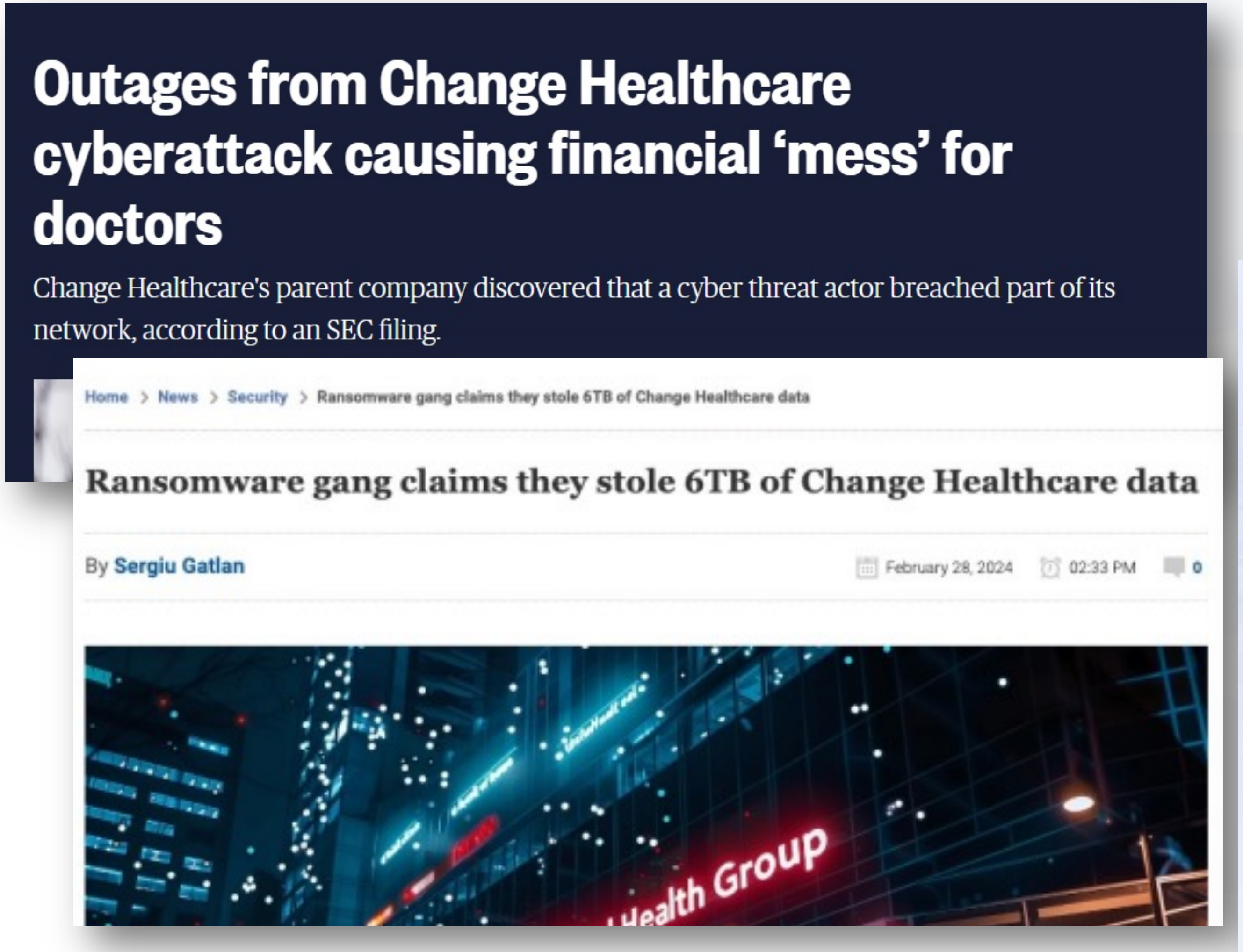
- AA23-319A.stix (XML, 116KB)
- AA23-319A.stix (JSON, 66KB)

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 the MS-ISAC (866-787-4722 or SOC@cisecurity.org).

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp

TLP:CLEAR

Blackcat/ALPHV Change Healthcare Ransomware



Outages from Change Healthcare cyberattack causing financial 'mess' for doctors

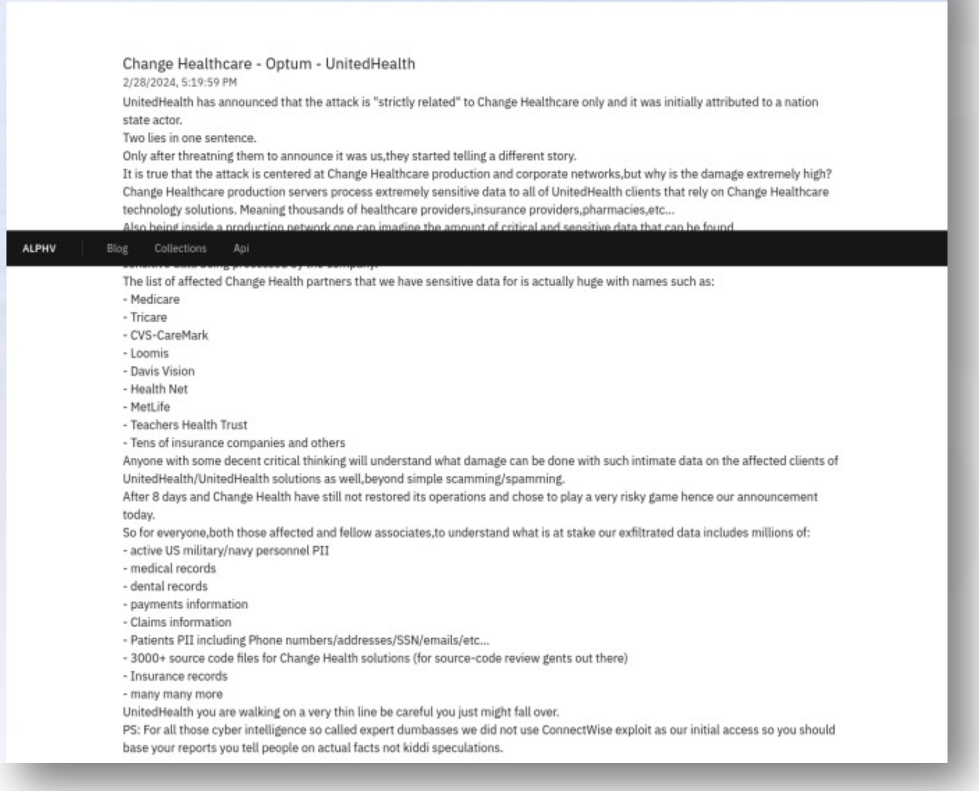
Change Healthcare's parent company discovered that a cyber threat actor breached part of its network, according to an SEC filing.

Home > News > Security > Ransomware gang claims they stole 6TB of Change Healthcare data

Ransomware gang claims they stole 6TB of Change Healthcare data

By Sergiu Gatlan February 28, 2024 02:33 PM 0

Darkweb BLOG POST from BlackCat



Change Healthcare - Optum - UnitedHealth

2/28/2024, 5:19:59 PM

UnitedHealth has announced that the attack is "strictly related" to Change Healthcare only and it was initially attributed to a nation state actor.

Two lies in one sentence.

Only after threatning them to announce it was us,they started telling a different story.

It is true that the attack is centered at Change Healthcare production and corporate networks,but why is the damage extremely high?

Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers,insurance providers,pharmacies,etc...

Also being inside a production network one can imagine the amount of critical and sensitive data that can be found

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well,beyond simple scamming/spamming.

After 8 days and Change Health have still not restored its operations and chose to play a very risky game hence our announcement today.

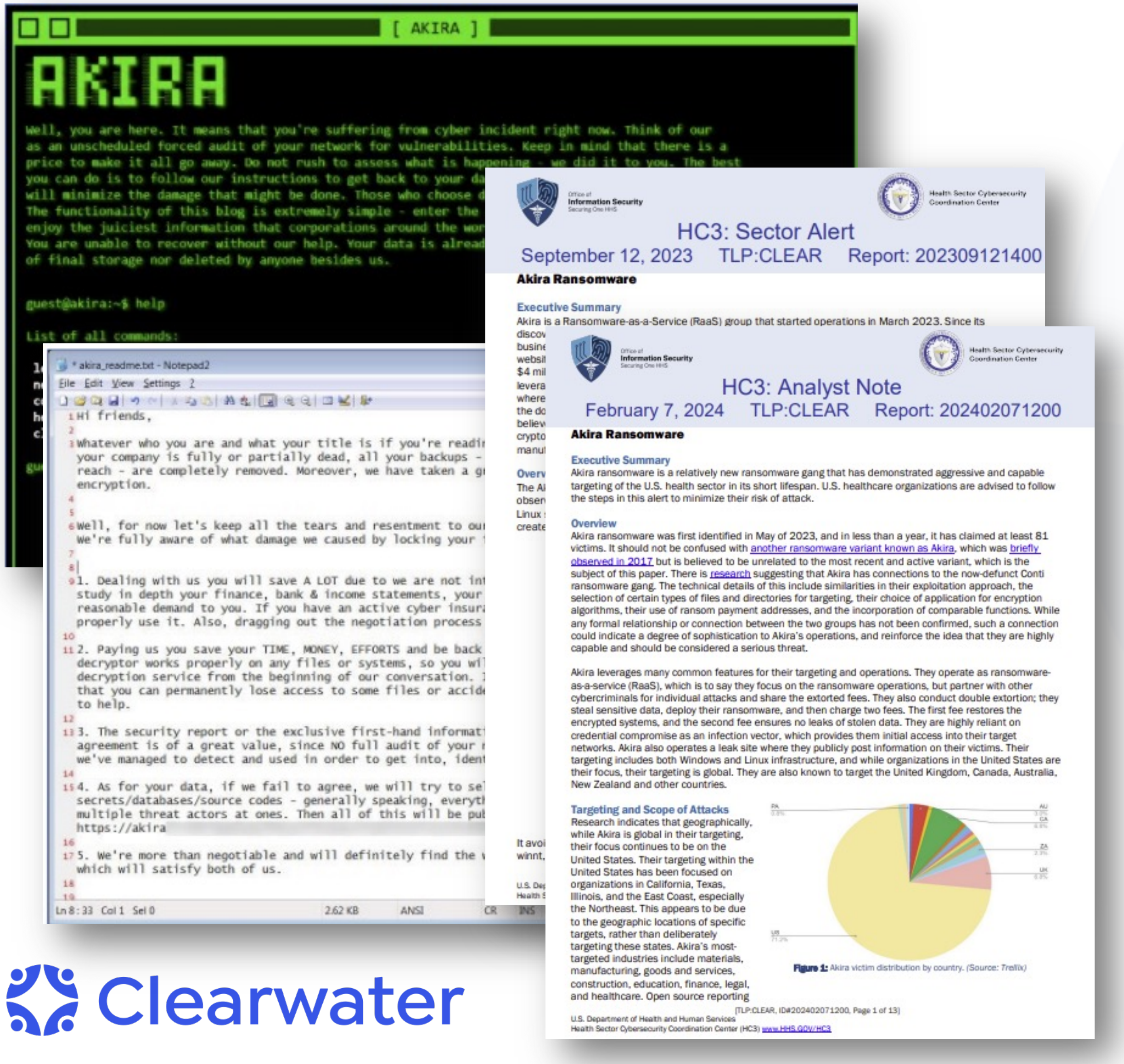
So for everyone,both those affected and fellow associates,to understand what is at stake our exfiltrated data includes millions of:

- active US military/navy personnel PII
- medical records
- dental records
- payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc...
- 3000+ source code files for Change Health solutions (for source-code review gents out there)
- Insurance records
- many many more

UnitedHealth you are walking on a very thin line be careful you just might fall over.

PS: For all those cyber intelligence so called expert dumbasses we did not use ConnectWise exploit as our initial access so you should base your reports you tell people on actual facts not kiddi speculations.

Akira Ransomware Advisory



```
[ AKIRA ]

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. The best
you can do is to follow our instructions to get back to your da
will minimize the damage that might be done. Those who choose d
The functionality of this blog is extremely simple - enter the
enjoy the juiciest information that corporations around the wor
You are unable to recover without our help. Your data is alread
of final storage nor deleted by anyone besides us.

guest@akira:~$ help

List of all commands:

 l
 n
 c
 h
 c

gu
```

```
Hi friends,

Whatever who you are and what your title is if you're readi
your company is fully or partially dead, all your backups -
reach - are completely removed. Moreover, we have taken a g
encryption.


Well, for now let's keep all the tears and resentment to ou
We're fully aware of what damage we caused by locking your


1. Dealing with us you will save A LOT due to we are not int
study in depth your finance, bank & income statements, your
reasonable demand to you. If you have an active cyber insur
properly use it. Also, dragging out the negotiation process

2. Paying us you save your TIME, MONEY, EFFORTS and be back
decryptor works properly on any files or systems, so you wi
decryption service from the beginning of our conversation. I
that you can permanently lose access to some files or accid
to help.

3. The security report or the exclusive first-hand informat
agreement is of a great value, since NO full audit of your
we've managed to detect and used in order to get into, iden

4. As for your data, if we fail to agree, we will try to se
secrets/databases/source codes - generally speaking, everyt
multiple threat actors at ones. Then all of this will be pub
https://akira[redacted]

5. We're more than negotiable and will definitely find the
which will satisfy both of us.
```

Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

September 12, 2023 TLP:CLEAR Report: 202309121400

Akira Ransomware

Executive Summary

Akira is a Ransomware-as-a-Service (RaaS) group that started operations in March 2023. Since its
discov
busine
websi
$4 mil
levera
where
the do
believ
crypto
manu

Overv
The A
obser
Linux
create

It avoi
winnt,

U.S. Dep
Health S

Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

February 7, 2024 TLP:CLEAR Report: 202402071200

Akira Ransomware

Executive Summary

Akira ransomware is a relatively new ransomware gang that has demonstrated aggressive and capable targeting of the U.S. health sector in its short lifespan. U.S. healthcare organizations are advised to follow the steps in this alert to minimize their risk of attack.

Overview

Akira ransomware was first identified in May of 2023, and in less than a year, it has claimed at least 81 victims. It should not be confused with another ransomware variant known as Akira, which was briefly observed in 2017 but is believed to be unrelated to the most recent and active variant, which is the subject of this paper. There is research suggesting that Akira has connections to the now-defunct Conti ransomware gang. The technical details of this include similarities in their exploitation approach, the selection of certain types of files and directories for targeting, their choice of application for encryption algorithms, their use of ransom payment addresses, and the incorporation of comparable functions. While any formal relationship or connection between the two groups has not been confirmed, such a connection could indicate a degree of sophistication to Akira's operations, and reinforce the idea that they are highly capable and should be considered a serious threat.

Akira leverages many common features for their targeting and operations. They operate as ransomware-as-a-service (RaaS), which is to say they focus on the ransomware operations, but partner with other cybercriminals for individual attacks and share the extorted fees. They also conduct double extortion; they steal sensitive data, deploy their ransomware, and then charge two fees. The first fee restores the encrypted systems, and the second fee ensures no leaks of stolen data. They are highly reliant on credential compromise as an infection vector, which provides them initial access into their target networks. Akira also operates a leak site where they publicly post information on their victims. Their targeting includes both Windows and Linux infrastructure, and while organizations in the United States are their focus, their targeting is global. They are also known to target the United Kingdom, Canada, Australia, New Zealand and other countries.

Targeting and Scope of Attacks

Research indicates that geographically, while Akira is global in their targeting, their focus continues to be on the United States. Their targeting within the United States has been focused on organizations in California, Texas, Illinois, and the East Coast, especially the Northeast. This appears to be due to the geographic locations of specific targets, rather than deliberately targeting these states. Akira's most-targeted industries include materials, manufacturing, goods and services, construction, education, finance, legal, and healthcare. Open source reporting

Figure 1: Akira victim distribution by country. *(Source: Trellix)*

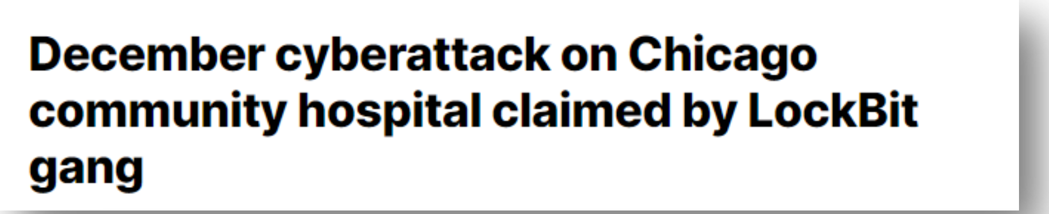
[TLP:CLEAR, ID#202402071200, Page 1 of 13]

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) www.HHS.GOV/HC3

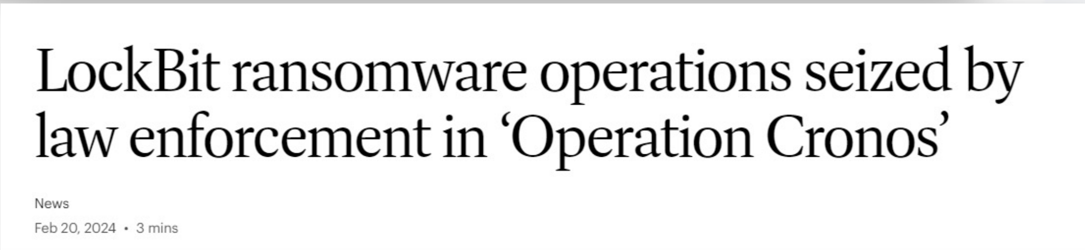
HC3 Alerts 9/12/23 & 2/7/24

- First identified in May of 2023 - has claimed at least 81 victims
- Relatively new but potentially former Conti ransomware group members
- Attacking U.S. focusing on Northeast U.S., CA, TX, IL
- Recent attack on Bucks County PA computer-aided dispatch system (911 services)
- Significant threat to healthcare industry per Health and Human Services' Health Sector Cybersecurity Coordination
- Double extortion techniques

Lockbit – Cat and Mouse Game

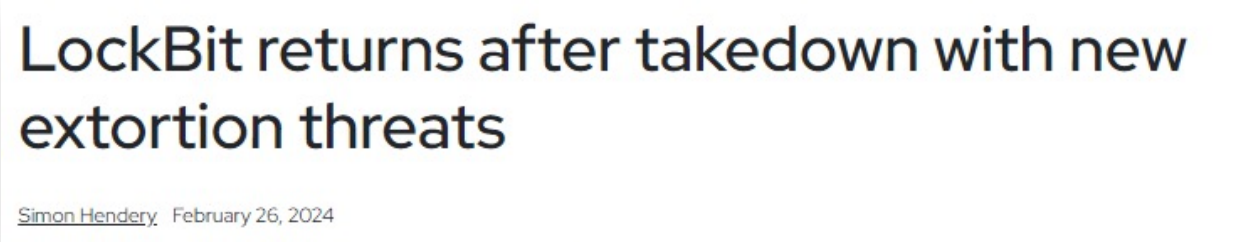


December cyberattack on Chicago community hospital claimed by LockBit gang



LockBit ransomware operations seized by law enforcement in 'Operation Cronos'

News
Feb 20, 2024 • 3 mins



LockBit returns after takedown with new extortion threats

Simon Hendery February 26, 2024

- More than 2,000 entities have been targeted in LockBit ransomware attacks, over $120 million in ransoms paid
- State Department offering $15 million for information leading to LockBit arrests
- Operation Cronos took down LockBit infrastructure ~Feb 19th
- Lockbit re-emerged several days later, promising to improve its own security while also increasing attacks against government sector

"I need to attack the .gov sector more often and more, it is after such attacks [by law enforcement/FBI]" - LockBitSupp posted in 2,800-word message

Continued Threats from Russian Threat Actors Expected

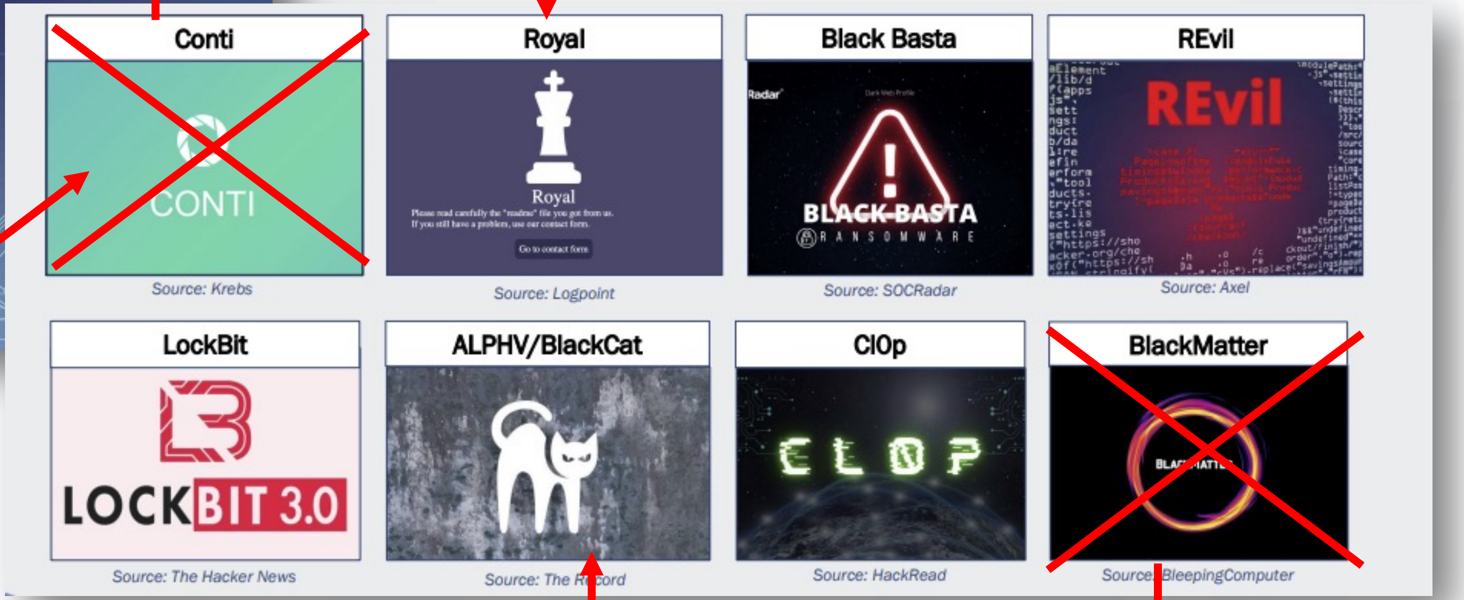
Russian Threat Actors Targeting the HPH Sector

February 15, 2024

TLP:CLEAR, ID# *202402151300*

Office of Information Security
Securing One HHS
Health Sector Cybersecurity Coordination Center
HC3

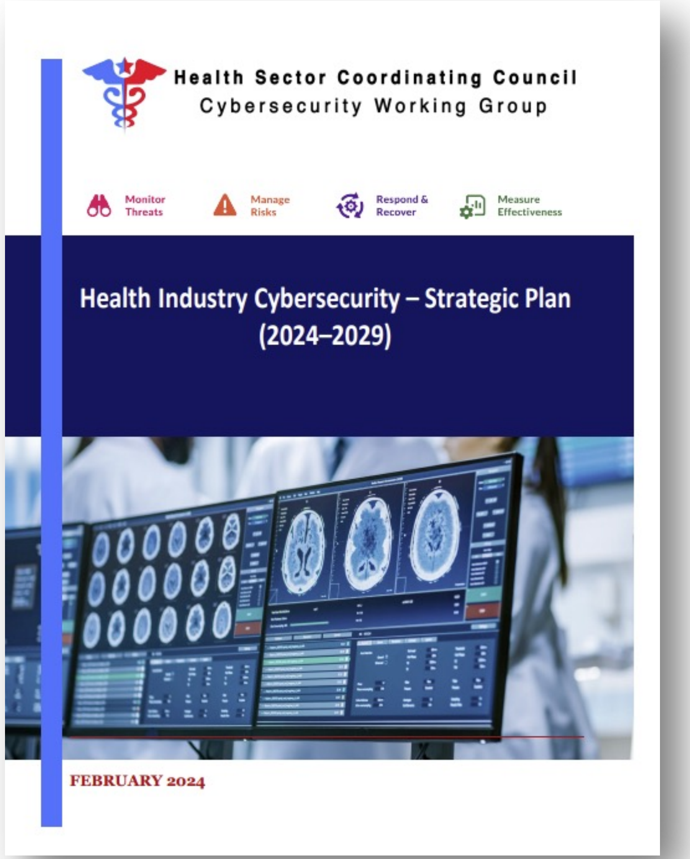
HC3 Threat Brief states that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities



Conti was taken down by law enforcement, re-emerged as Royal, Akira (not pictured) and Black Suit.

BlackMatter re-emerged as Blackcat

HSCC Health Industry Cybersecurity Strategic Plan (HIC-SP)



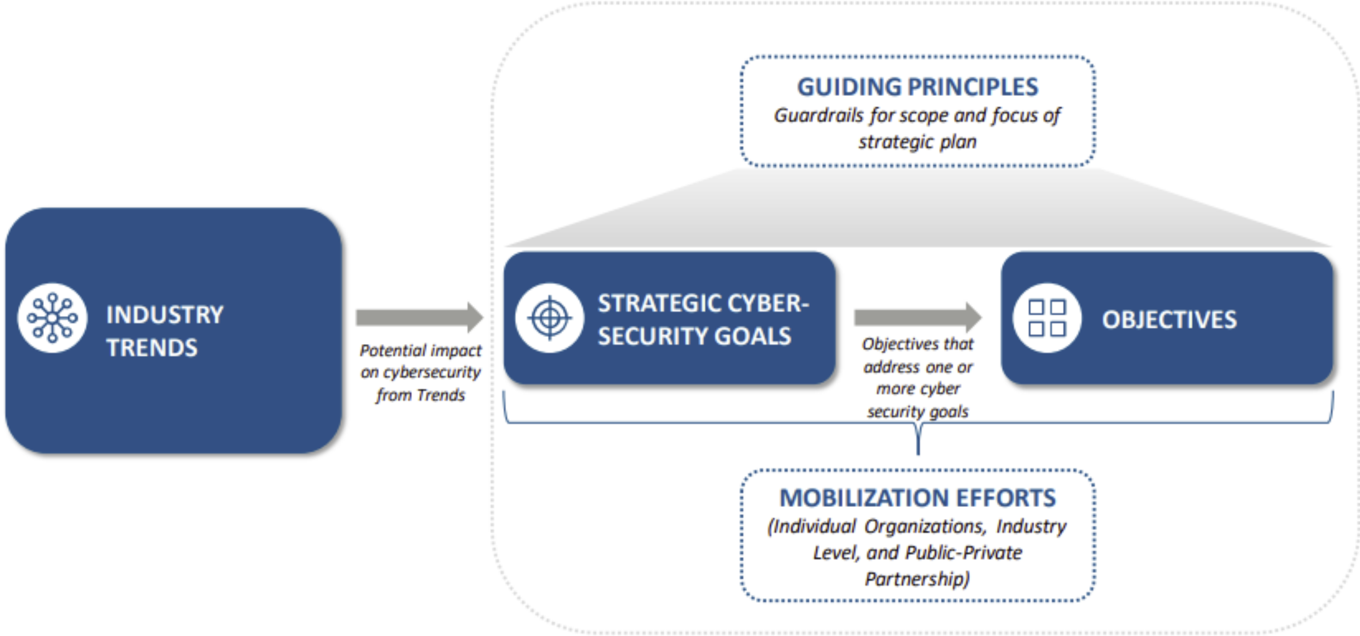
Health Sector Coordinating Council
Cybersecurity Working Group

Monitor Threats | Manage Risks | Respond & Recover | Measure Effectiveness

Health Industry Cybersecurity – Strategic Plan (2024–2029)

FEBRUARY 2024

Projected 5-year industry trends informed identification of broad cybersecurity goals realized by actionable implementing objectives to move the sector toward a more cyber-secure and resilient posture.

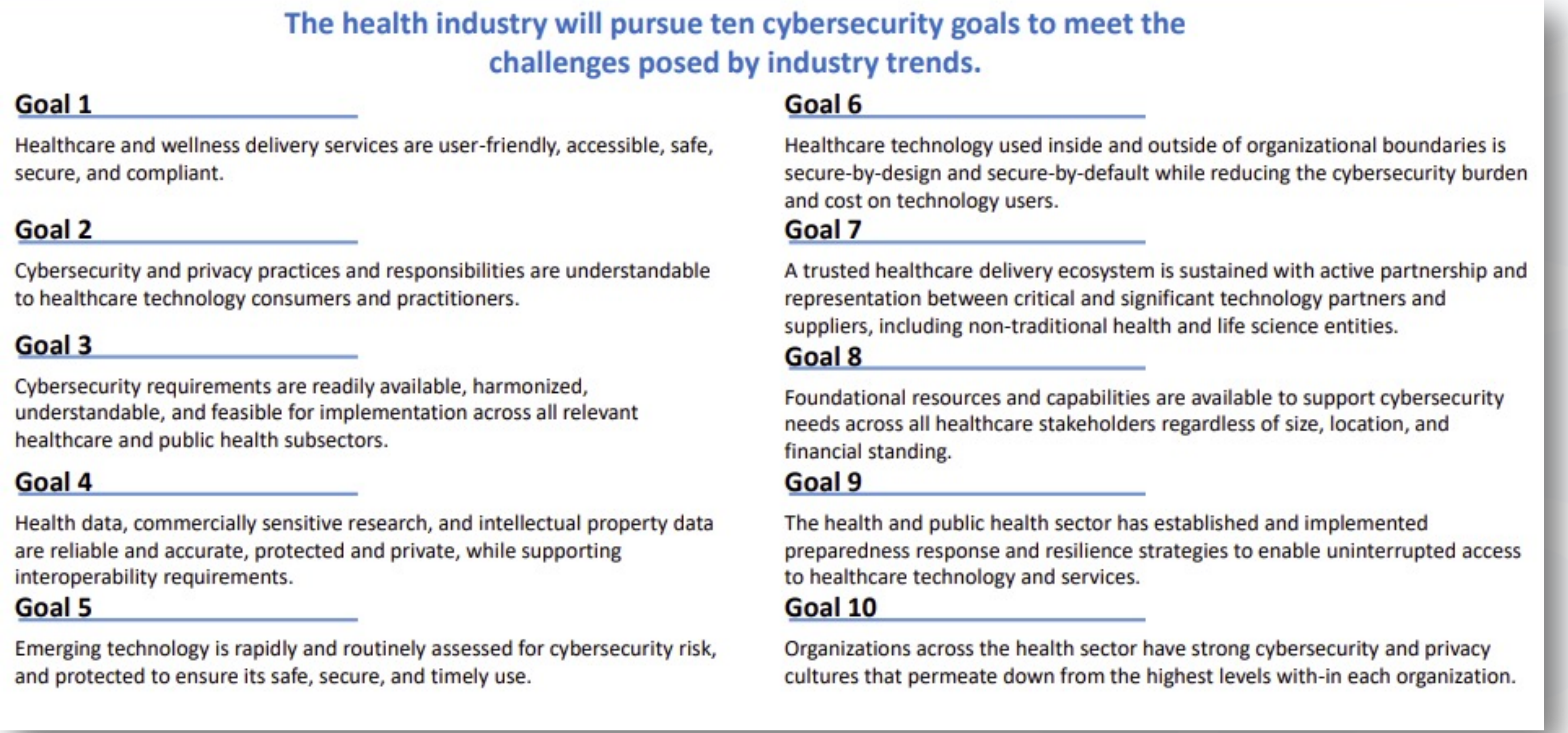


GUIDING PRINCIPLES
Guardrails for scope and focus of strategic plan
INDUSTRY TRENDS
Potential impact on cybersecurity from Trends
STRATEGIC CYBER-SECURITY GOALS
Objectives that address one or more cyber security goals
OBJECTIVES
MOBILIZATION EFFORTS
(Individual Organizations, Industry Level, and Public-Private Partnership)

Clearwater

Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf (healthsectorcouncil.org)

5-Year Cybersecurity Goals To Meet Industry Trends



The health industry will pursue ten cybersecurity goals to meet the challenges posed by industry trends.

Goal 1

Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant.

Goal 2

Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners.

Goal 3

Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors.

Goal 4

Health data, commercially sensitive research, and intellectual property data are reliable and accurate, protected and private, while supporting interoperability requirements.

Goal 5

Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use.

Goal 6

Healthcare technology used inside and outside of organizational boundaries is secure-by-design and secure-by-default while reducing the cybersecurity burden and cost on technology users.

Goal 7

A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non-traditional health and life science entities.

Goal 8

Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing.

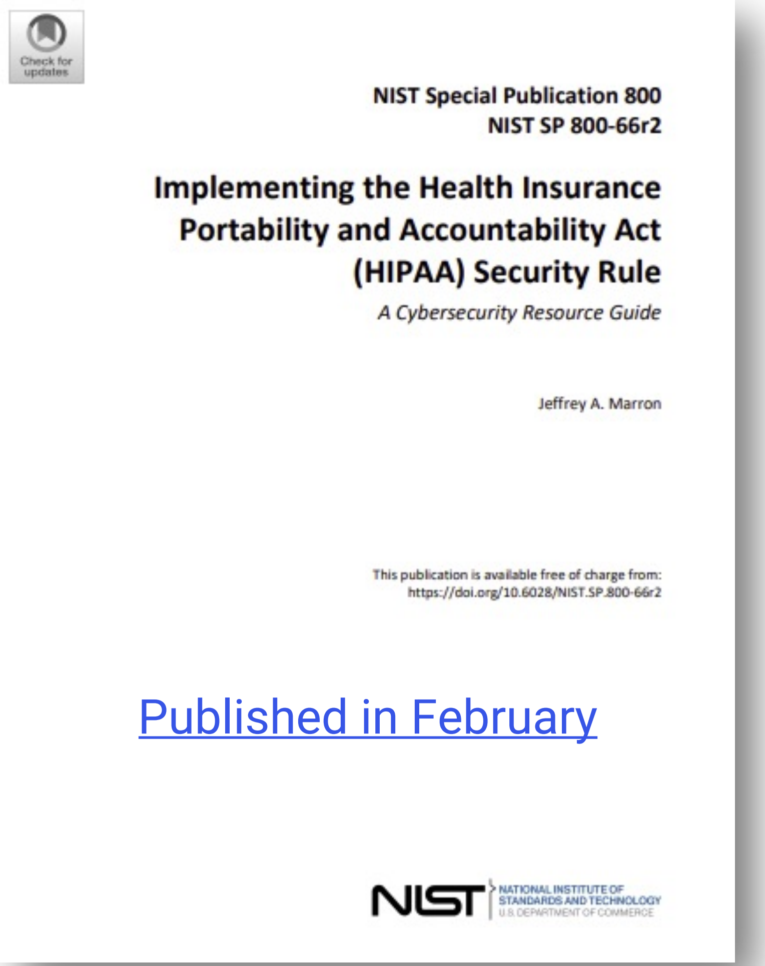
Goal 9

The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services.

Goal 10

Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels with-in each organization.

NIST SP 800-66 r2 Aligns with Asset Based Risk Analysis



Check for updates

NIST Special Publication 800
NIST SP 800-66r2

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

A Cybersecurity Resource Guide

Jeffrey A. Marron

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2

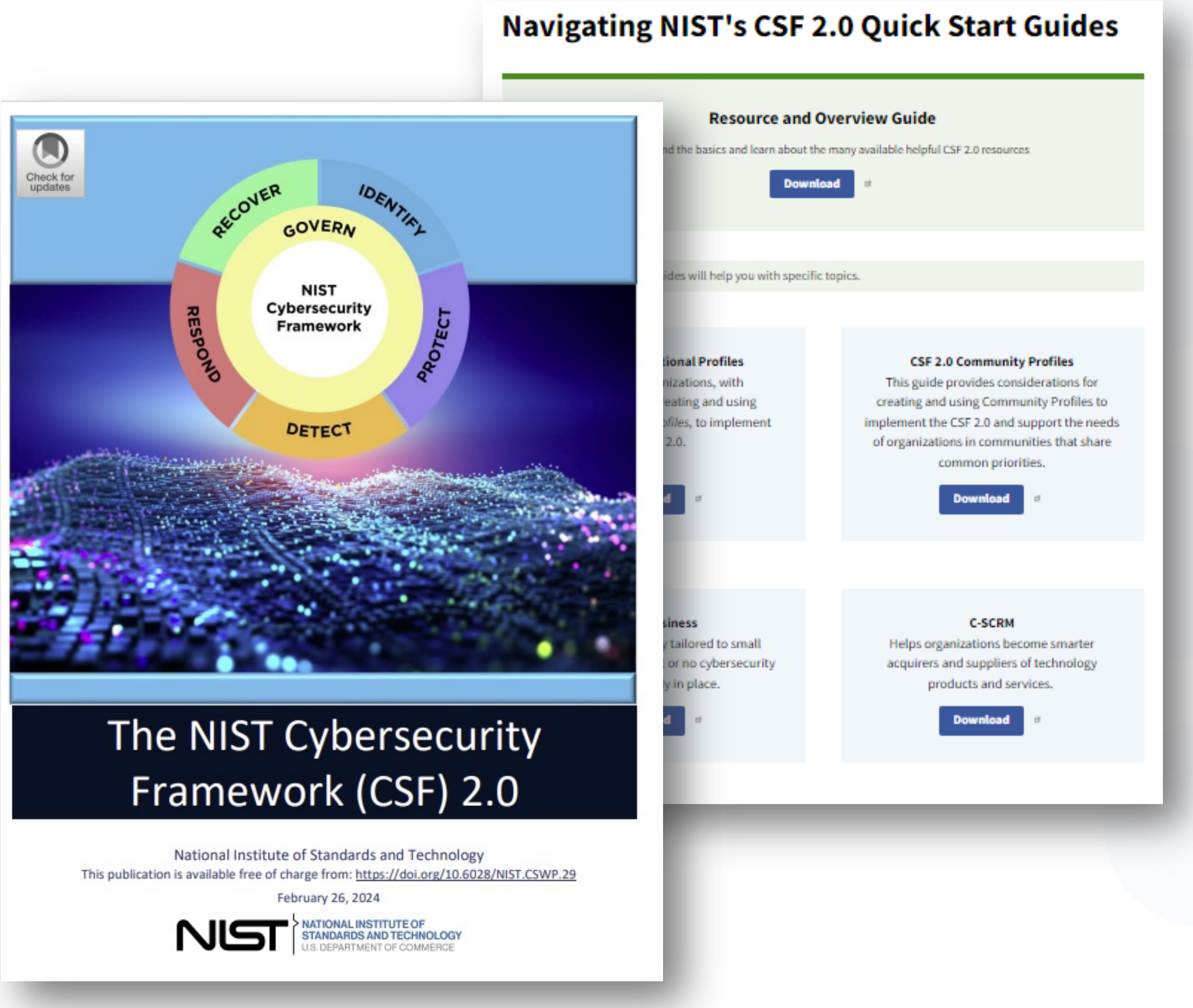
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Published in February

Risk Assessment, initially part of Appendix E in rev 1, is now distinctly outlined as Section 3 in rev 2. The content aligns with SP 800-30 and the NIST IR 8286 series of documents.

- States the need to identify all systems and components with ePHI
- Risk assessment is the process by which an must include all systems and processes, including remote workers or systems that are managed by service providers
- Risk tolerance and risk appetite should be clearly defined and weighted. Risk mitigation and management efforts must be tailored appropriately.
- Regulated entities should not view risk assessment as a one-time, static task but as an ongoing activity

NIST Cybersecurity Framework 2.0 Released



Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

nd the basics and learn about the many available helpful CSF 2.0 resources

Download

ides will help you with specific topics.

ional Profiles
nizations, with
eating and using
files, to implement
2.0.

CSF 2.0 Community Profiles

This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.

Download

iness
tailored to small
or no cybersecurity
in place.

C-SCRM

Helps organizations become smarter acquirers and suppliers of technology products and services.

Download

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

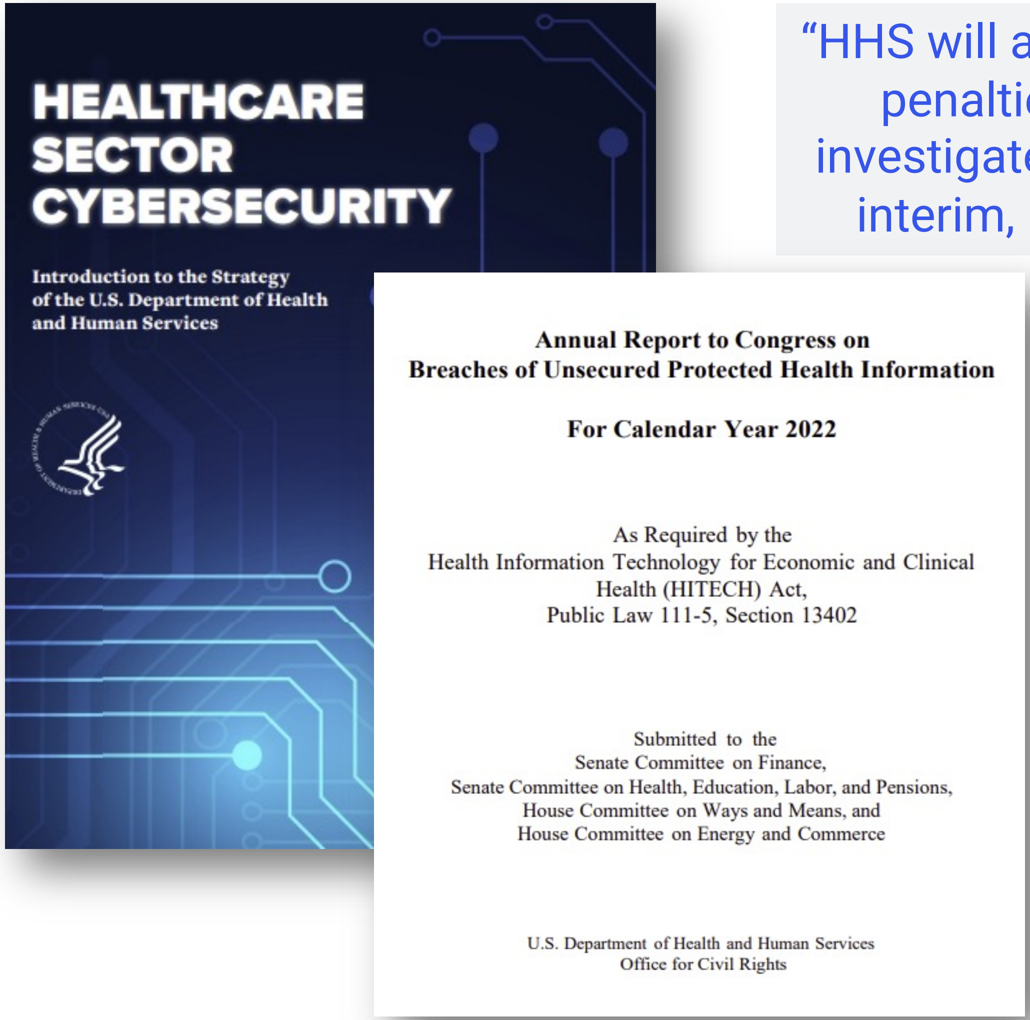
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST CSF 2.0 just released…

- New Govern function to emphasize cybersecurity risk management outcomes
- Broadens the scope to any sector
- Number of tools for “quick start” to help smaller businesses
- Advice for creating profiles tailored to an organization's unique risk posture

Please refer to our July Cyber Briefing featuring Dave Bailey’s presentation on NIST 2.0.

Expect OCR Enforcement to Increase if Funding is Provided



HEALTHCARE SECTOR CYBERSECURITY

Introduction to the Strategy of the U.S. Department of Health and Human Services

Annual Report to Congress on
Breaches of Unsecured Protected Health Information

For Calendar Year 2022

As Required by the
Health Information Technology for Economic and Clinical Health (HITECH) Act,
Public Law 111-5, Section 13402

Submitted to the
Senate Committee on Finance,
Senate Committee on Health, Education, Labor, and Pensions,
House Committee on Ways and Means, and
House Committee on Energy and Commerce

U.S. Department of Health and Human Services
Office for Civil Rights

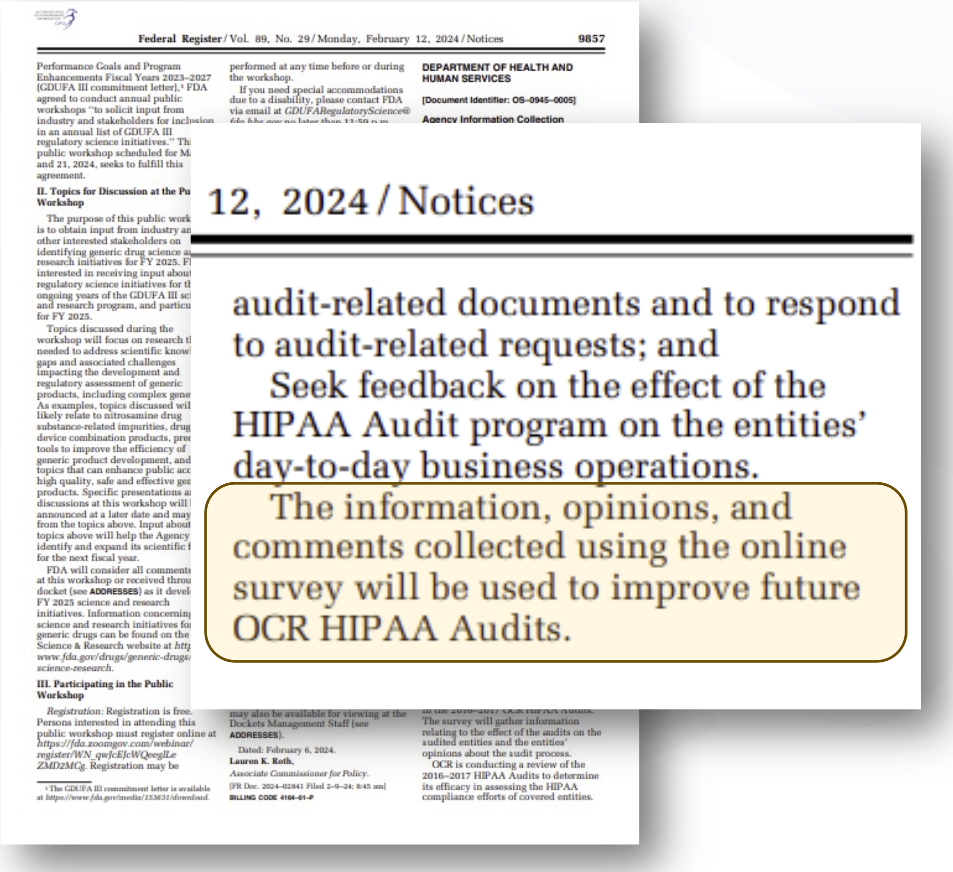
> “HHS will also continue to work with Congress to increase civil monetary penalties for HIPAA violations and increase resources for HHS to investigate potential HIPAA violations, conduct proactive audits….in the interim, HHS will continue to investigate potential HIPAA violations.

- Two Resolution agreements (Corrective Action Plans) announced in last 30 days, including one for $4.75 Million.
- HHS Strategic Plan released in December outlines additional regulations and resources for enforcement
- 2022 OCR Compliance Report to Congress (published Feb 2024) called out multiple times it needs more funding for enforcement
- Asked Congress to increase HITECH civil monetary penalty caps be increased
- HHS plans to update HIPAA Security Rule – process beginning this spring

OCR Auditing Program Likely to Resume

Audits have not been conducted since 2016 - 2017 however the expectation is that auditing program will go into effect at end of 2024

- OCR published in Federal Register that it is surveying previous auditees to learn from the previous program and improve future program
- In Annual Report to Congress OCR noted that "..it is currently developing the criteria for implementing future audits should financial resources become available."
- Funding discussions underway with Congress per HHS ViVE presentation



Federal Register / Vol. 89, No. 29 / Monday, February 12, 2024 / Notices 9857

Performance Goals and Program
Enhancements Fiscal Years 2023–2027
(GDUFA III commitment letter),[1] FDA
agreed to conduct annual public
workshops "to solicit input from
industry and stakeholders for inclusion
in an annual list of GDUFA III
regulatory science initiatives." Thi
public workshop scheduled for M
and 21, 2024, seeks to fulfill this
agreement.

II. Topics for Discussion at the Pu
Workshop

The purpose of this public work
is to obtain input from industry an
other interested stakeholders on
identifying generic drug science a
research initiatives for FY 2025. F
interested in receiving input about
regulatory science initiatives for t
ongoing years of the GDUFA III sci
and research program, and particu
for FY 2025.

Topics discussed during the
workshop will focus on research t
needed to address scientific know
gaps and associated challenges
impacting the development and
regulatory assessment of generic
products, including complex gene
As examples, topics discussed wil
likely relate to nitrosamine drug
substance-related impurities, drug
device combination products, pre
tools to improve the efficiency of
generic product development, and
topics that can enhance public acc
high quality, safe and effective ge
products. Specific presentations a
discussions at this workshop will
announced at a later date and may
from the topics above. Input about
topics above will help the Agency
identify and expand its scientific f
for the next fiscal year.

FDA will consider all comments
at this workshop or received throu
docket (see ADDRESSES) as it devel
FY 2025 science and research
initiatives. Information concernin
science and research initiatives fo
generic drugs can be found on the
Science & Research website at *htt*
www.fda.gov/drugs/generic-drugs/
science-research.

III. Participating in the Public Workshop

Registration: Registration is free. Persons interested in attending this public workshop must register online at *https://fda.zoomgov.com/webinar/register/WN_qwfcEJcWQeeglLeZMDzMCg*. Registration may be

[1] The GDUFA III commitment letter is available at *https://www.fda.gov/media/153631/download*.

performed at any time before or during the workshop.

If you need special accommodations due to a disability, please contact FDA via email at *GDUFARegulatoryScience@*
fda.hhs.gov no later than 11:59 p.m.

may also be available for viewing at the Dockets Management Staff (see ADDRESSES).

Dated: February 6, 2024.

Lauren K. Roth,

Associate Commissioner for Policy.

[FR Doc. 2024–02841 Filed 2–9–24; 8:45 am]

BILLING CODE 4164–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

[Document Identifier: OS–0945–0005]

Agency Information Collection

in the 2016–2017 OCR HIPAA Audits. The survey will gather information relating to the effect of the audits on the audited entities and the entities' opinions about the audit process.

OCR is conducting a review of the 2016–2017 HIPAA Audits to determine its efficacy in assessing the HIPAA compliance efforts of covered entities.

12, 2024 / Notices

audit-related documents and to respond to audit-related requests; and

Seek feedback on the effect of the HIPAA Audit program on the entities' day-to-day business operations.

The information, opinions, and comments collected using the online survey will be used to improve future OCR HIPAA Audits.

Clearwater

HIPAA Audits On the Way – Clearwater Free Education

Register to attend Clearwater's 5 Part Series to Prepare for Anticipated Audits

March 13, 12-1 CT

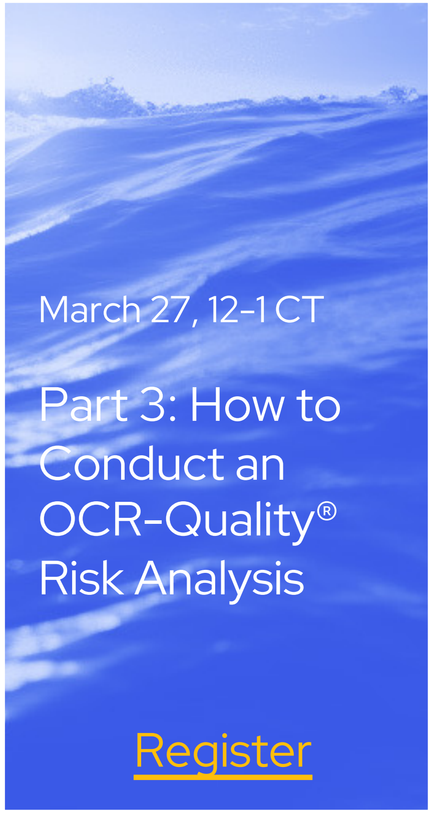
Part 1: What We Learned from the Last Round of HIPAA Audits

Register

March 20, 12-1 CT

Part 2: Keys to Implementing an OCR-Quality® Compliance Program

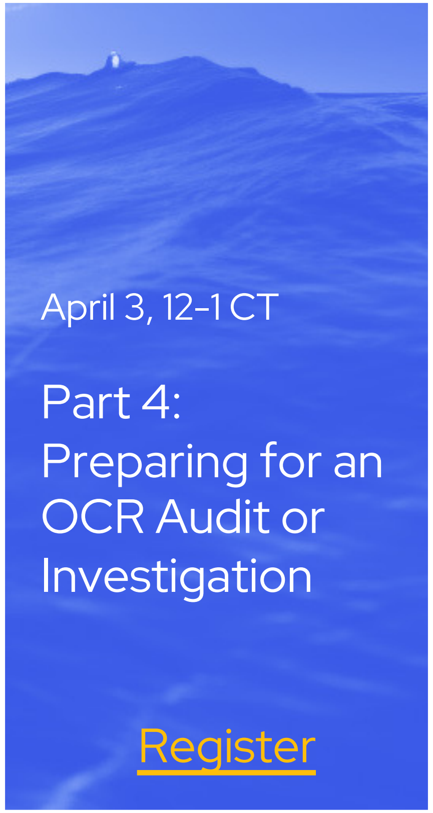
Register



March 27, 12-1 CT

Part 3: How to Conduct an OCR-Quality® Risk Analysis

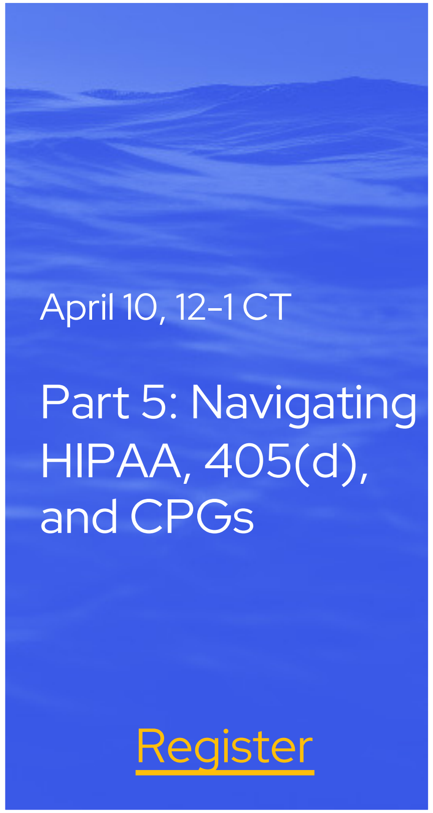
Register



April 3, 12-1 CT

Part 4: Preparing for an OCR Audit or Investigation

Register



April 10, 12-1 CT

Part 5: Navigating HIPAA, 405(d), and CPGs

Register

Recommendations

- Continue to monitor threat alerts from CISA, Health Sector Cybersecurity Coordination Center (HC3)
- Relatively immature? Leverage the 405(d) Health Industry Cybersecurity Practices (HCIP)
- Review scope and cadence of vulnerability management program, and ensure capabilities are in place for rapid patching or implementing other mitigating controls
- Ability to detect, respond, and contain an attack is critical
- Conduct on going threat hunting, and perform a compromise assessment
- Update and test incident response plans
- Conduct a Business Impact Analysis to feed into risk analysis and risk management programs
  - Review impact of each system based on business or clinical process
  - Include all systems, locations and technologies in scope of Risk Analysis
  - Assess unique risks for each information system
  - Make sure you keep it up to date

Quarterly Threat Review

Dave Bailey

Steve Akers

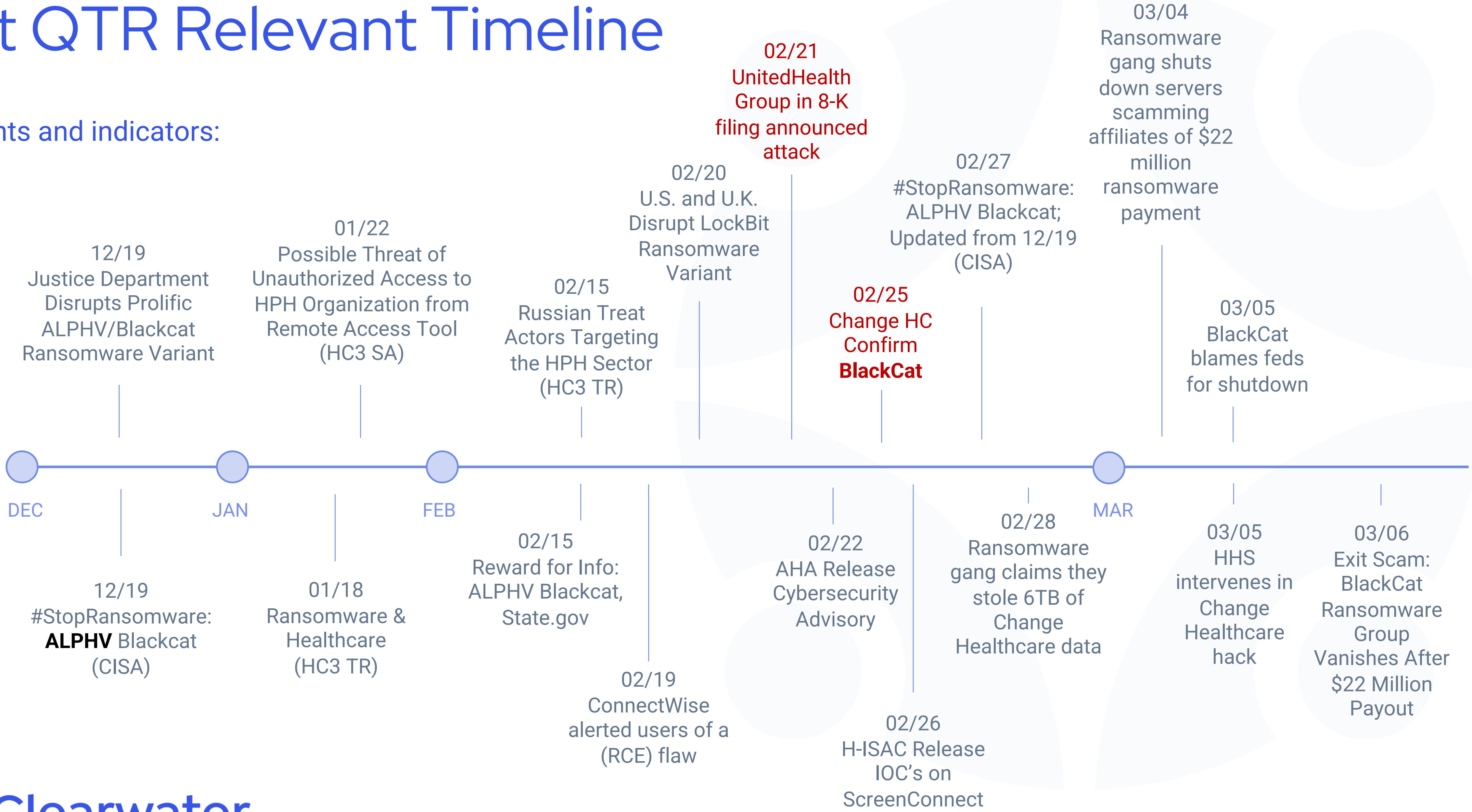
Clearwater

Change Healthcare Incident Update

- Mandiant and Palo Alto Networks working incident response: initial phase complete
  - The initial attack vector is defined, and all IOC's captured
- Shifting efforts to full data center rebuild/restoration; ETA of EOW
  - Offline Data Center is "quarantined"
- Change will provide documentation for systems coming back on-line
  - 3rd party penetration testing attestation
  - Attestation new system is not connected to the quarantine area
- **BlackCat shuts down servers scamming affiliates of $22 million payment: blames feds**
  - **Reports of BlackCat vanishing or pulling off the "exit-scam" & selling the source code for the malware for the hefty price of $5 million.**
- **Be aware of scams taking advantage of the Change Incident**

1st QTR Relevant Timeline

Events and indicators:



12/19
Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant

12/19
#StopRansomware: **ALPHV** Blackcat (CISA)

01/18
Ransomware & Healthcare (HC3 TR)

01/22
Possible Threat of Unauthorized Access to HPH Organization from Remote Access Tool (HC3 SA)

02/15
Russian Treat Actors Targeting the HPH Sector (HC3 TR)

02/15
Reward for Info: ALPHV Blackcat, State.gov

02/19
ConnectWise alerted users of a (RCE) flaw

02/20
U.S. and U.K. Disrupt LockBit Ransomware Variant

02/21
UnitedHealth Group in 8-K filing announced attack

02/22
AHA Release Cybersecurity Advisory

02/25
Change HC Confirm **BlackCat**

02/26
H-ISAC Release IOC's on ScreenConnect

02/27
#StopRansomware: ALPHV Blackcat; Updated from 12/19 (CISA)

02/28
Ransomware gang claims they stole 6TB of Change Healthcare data

03/04
Ransomware gang shuts down servers scamming affiliates of $22 million ransomware payment

03/05
BlackCat blames feds for shutdown

03/05
HHS intervenes in Change Healthcare hack

03/06
Exit Scam: BlackCat Ransomware Group Vanishes After $22 Million Payout

Clearwater

Relevant Threat Reports

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
HC3

Russian Threat Actors Targeting the HPH Sector

February 15, 2024

TLP:CLEAR, ID# *202402151300*

1

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
HC3

Ransomware & Healthcare

January 18, 2024

TLP:CLEAR, ID# *202401181300*

1

RHYSIDA

Clearwater

Threat Actor Spotlight: Characteristics of ALPHV/BlackCat

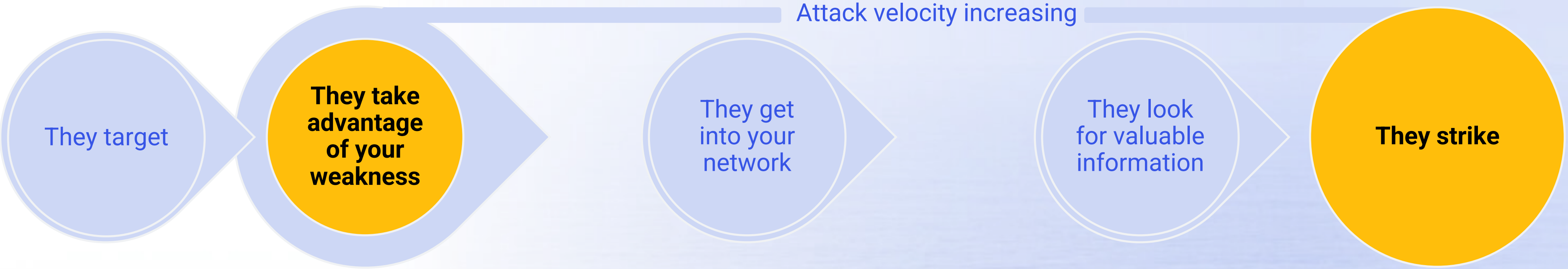
CAPABILITY	Very Low	Low	Moderate	High	[✓ Very High]	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.	▪ Ransomware as a Service ▪ Associated with other advanced-persistent threat (APT) groups like Conti, DarkSide, Revil, and BlackMatter.
INTENT	Very Low	Low	Moderate	[✓ High]	Very High	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.	▪ Demanded over $500 million and received nearly $300 million in ransom payments (CISA)
TARGETING	Very Low	Low	Moderate	[✓ High]	Very High	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.	▪ ALPHV Blackcat affiliates have compromised over 750 United States entities (CISA)
RELEVANCE	Possible	Predicted	Anticipated	[✓ Expected]	Confirmed	The threat event or TTP has been seen by the organization's peers or partners.	▪ Change Healthcare ▪ HHS H3C Threat Alerts ▪ Multiple media reports and other HC orgs impacted by BlackCat
LIKELIHOOD	Very Low	Low	Moderate	[✓ High]	Very High	Adversary is almost certain to initiate the threat event.	▪ Unpatched Vulnerabilities (ScreenConnect) ▪ Connections to Change/Optum ▪ Lack of reasonable and appropriate controls (EDR, monitoring, email protections, MFA, etc)

Threat Actor Spotlight: Characteristics of Rhysida

CAPABILITY	Very Low	Low	Moderate	High	[✓ Very High]	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.	▪ Ransomware as a Service ▪ Related to threat actor group Vice Society
INTENT	Very Low	Low	Moderate	[✓ High]	Very High	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.	▪ The group threatens to publicly distribute the exfiltrated data if the ransom is not paid.
TARGETING	Very Low	Low	Moderate	[✓ High]	Very High	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.	▪ The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads
RELEVANCE	Possible	Predicted	Anticipated	[✓ Expected]	Confirmed	The threat event or TTP has been seen by the organization's peers or partners.	▪ Linked with Lurie Children's, Prospect Medical Holdings, & Singing River Health System
LIKELIHOOD	Very Low	Low	Moderate	[✓ High]	Very High	Adversary is almost certain to initiate the threat event.	▪ Vulnerable to living off the land techniques ▪ Exploited vulnerabilities in remote access & compromised accounts ▪ Lack of reasonable and appropriate controls (EDR, monitoring, email protections, MFA, etc.)

Clearwater

Typical Ransomware: How They Attack


Attack velocity increasing
They target
They take advantage of your weakness
They get into your network
They look for valuable information
They strike

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
10	7	9	12	19	13	40	16	29	9	17	16	9	13

# of techniques

MITRE ATT&CK Enterprise Tactics

Dwell Times Decreasing

- Improved Coverage
- Better Detection Capabilities
- Use of MSSPs
- External Notifications
  - Partners
  - Gov't / ISACs
  - Bad Actors

15-21	10-16	8-13
2021[3,4]	2022[3,4]	2023[1,3]

Median Dwell Time in Days

5-11	4.5-9	<1-8
2021[3,4]	2022[2,3,4]	2023[2,3]

Ransomware Median Dwell Time in Days

[1] Palo Alto Unit 42 2024 Incident response Report
[2] Secureworks annual State of The Threat Report Dec 2023
[3] Sophos Active Advisory Report 2023
[4] Mandiant M-Trends 2023 Report

Attack Velocity Increasing

- Speed and Stealth reduces chance of detection
- Focused on simpler/quicker
  - Grab and Go, versus targeted
- Top Paths – Scan and Exploit and Stolen Creds Tied (32%)
  - Record Zero Days in 2023
- Initial Access Brokers

9
2022[1]

2
2023[1]

Median Time from Compromise to Exfil in Days

81%
Outside Business Hours[3]

43%
Friday or Saturday[3]

45%
Exfil in under 1 Day[1]

50%
Deployed in Under 24 Hours[2]

10%
Deployed in Under 5 Hours[2]

16
Hours to Breach Active Directory

Ransomware 2023 Stats

[1] Palo Alto Unit 42 2024 Incident response Report
[2] Secureworks annual State of The Threat Report Dec 2023
[3] Sophos Active Advisory Report 2023
[4] Mandiant M-Trends 2023 Report

Recommended Actions and Response

Response Actions

- Disconnect and/or Block Change Healthcare/Optum connections
- Continually check your environment for IOC's: ScreenConnect and Blackcat
- Formally initiate Incident Response if you discover any IOCs & conduct a Compromise Assessment
- Provide workforce awareness on potential scams

Risk Management

- Determine criteria and establish risk tolerance to restore/unblock Change Healthcare/Optum connections
- IT/Security provide decision-makers with:
  - Current Security Posture
  - Known relevant information on incident

Cyber Resilience

- Validate and rehearse your plans
- Validate the effectiveness of your controls; Security Control Validation
- Provide continuous awareness to the workforce

Assumptions

- The following capabilities are in place (at a minimum):
- Security Continuous Monitoring
  - SOC, EDR
  - Logging
- Vulnerability Management Program
- Vendor Risk Management
- MFA and PAM

Q&A

Steve Akers
Dave Bailey
Steve Cagle

Clearwater

We are here to help.

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

Upcoming Events

CREATING TOMORROW'S HEALTH
HIMSS Global Health Conference & Exhibition
March 11-15, 2024

HIMSS | March 11-15
Booth #1618, Cybersecurity
Command Center

HIPAA Audits 5 Part Webinar Series:

1. March 13
2. March 20
3. March 27
4. April 3
5. April 10

RECORD SHOP
ALL TYPES OF RECORDS SHIPPED ROUND THE WORLD
REAL COUNTRY MUSIC LIVES HERE
28th Annual
Compliance Institute
April 14–17, 2024 • Nashville or Virtual

HCCA | April 14-17
Andrew Mahler presenting "How Safe Is 'Safe Harbor'? Balancing De-identification, Anonymization, and Pseudonymization of Health Data with Privacy Risks"

Clearwater

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Twitter | @clearwaterhipaa