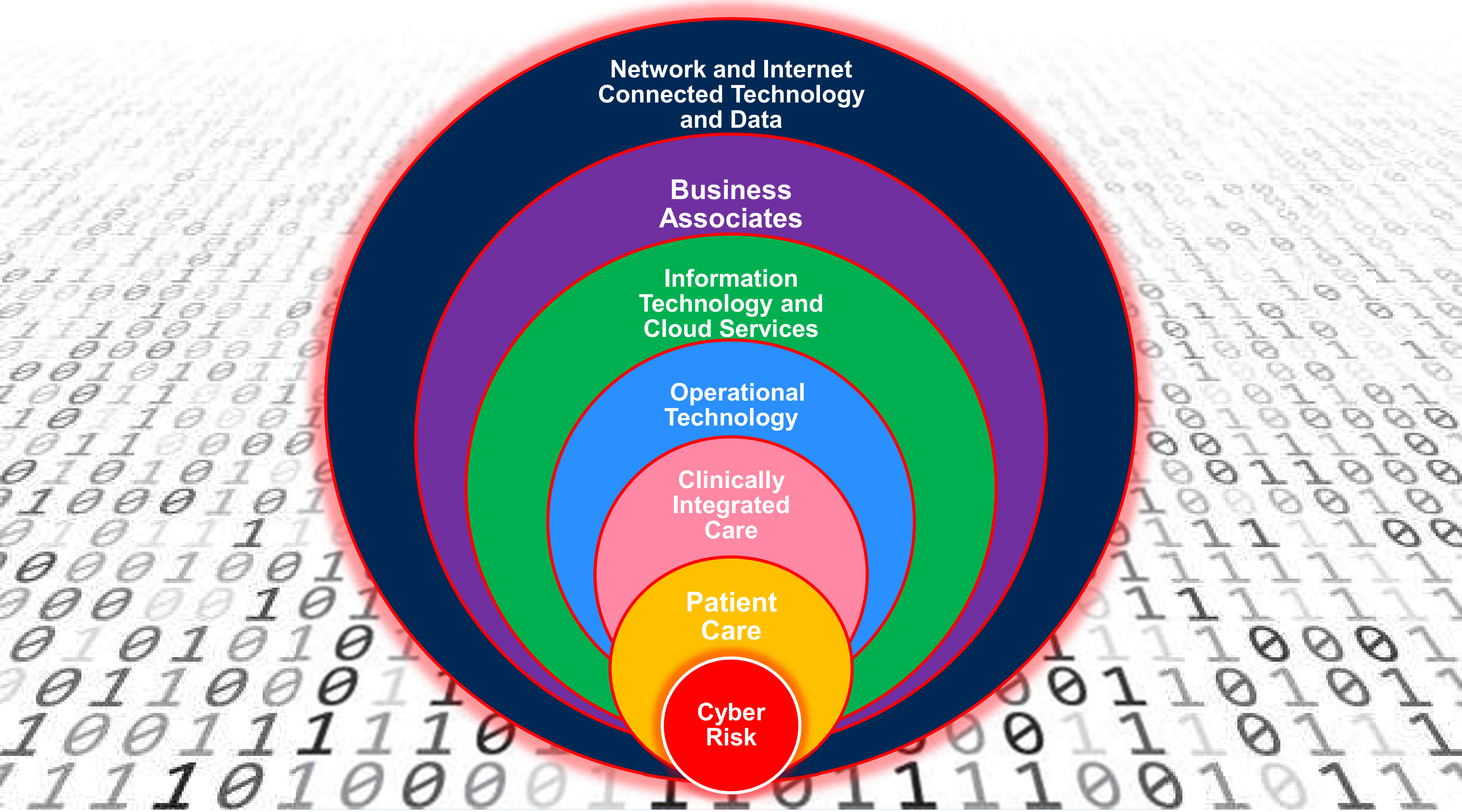
MIAMI-DADE COUNTY
HEALTHCARE PREPAREDNESS COALITION
EMERGENCY PREPAREDNESS

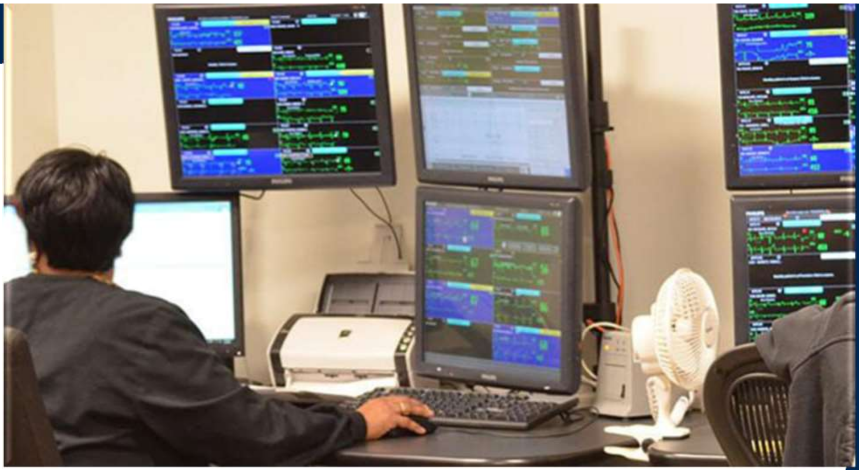
The Healthcare Cyber Threat Landscape: Ransomware Preparedness and Response

AMERICAN HOSPITAL ASSOCIATION
NISI DOMINUS FRUSTRA
FOUNDED 1898

American Hospital Association™
Advancing Health in America
Cybersecurity and Risk Advisory Services

Presented by John Riggi, National Advisor for Cybersecurity and Risk
American Hospital Association
04/11/2024


Network and Internet Connected Technology and Data
Business Associates
Information Technology and Cloud Services
Operational Technology
Clinically Integrated Care
Patient Care
Cyber Risk



Hacking Incidents Reported to HHS – Office of Civil Rights

2020 Total:
425 Hacks Impacting 27 Million Individuals

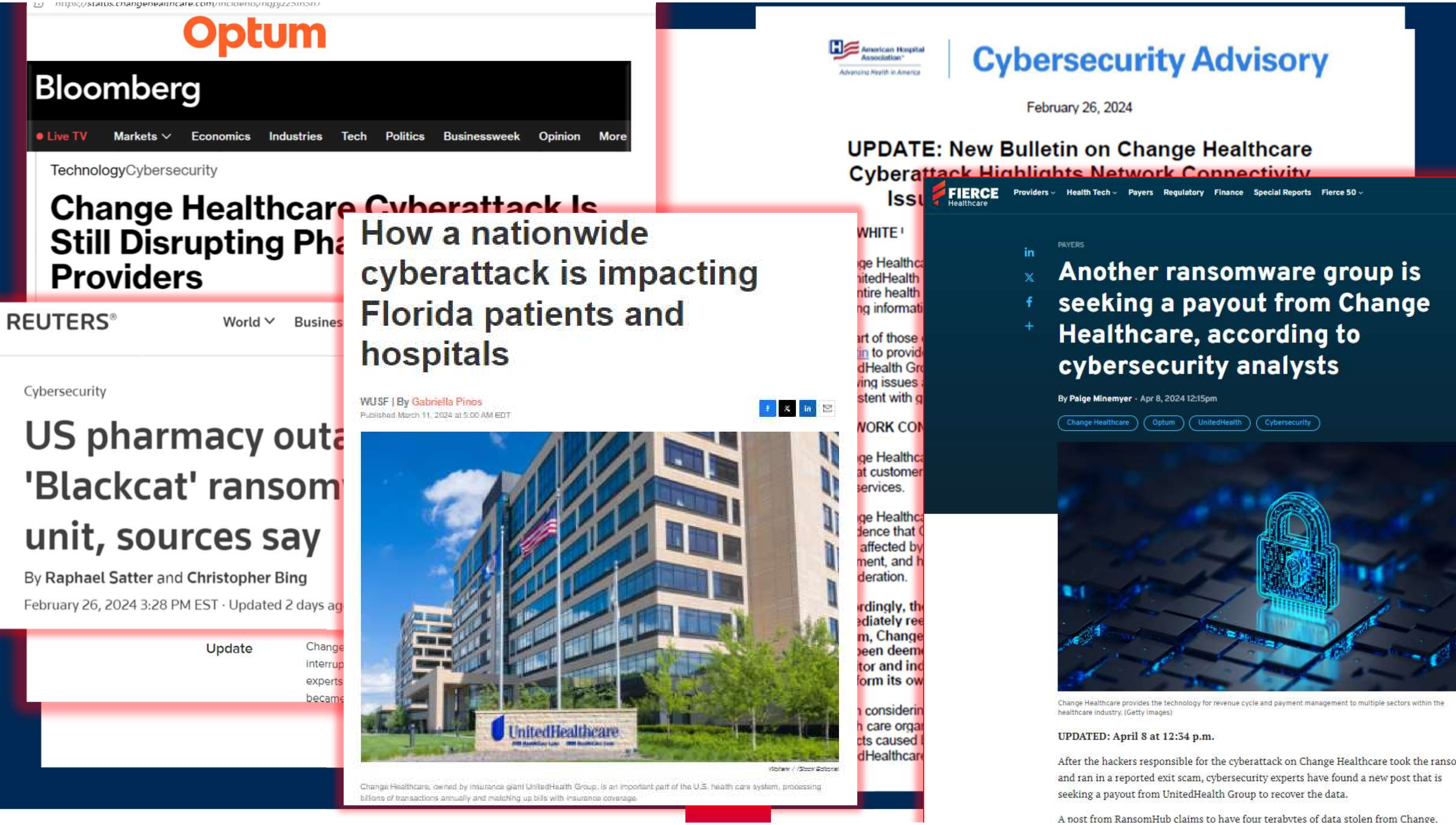
2021 Total:
518 Hacks Impacting 43 Million Individuals

2022 Total:
556 Hacks Impacting 44 Million Individuals

2023:
1/1/2023 – 12/31/2023 591 Hacks impacting A RECORD 135.9 Million individua

2024:
01/01/2024 - 03/22/2024 124 Hacks Impacting 15.6 Million Individuals

- 250 million people impacted by hacks of PHI since 2020 = ~ 72% of US population
- Ransomware attacks up 278% since 2020 per OCR
- Healthcare is the most attacked sector by ransomware per the FBI
- Sources : HHS, OCR website data accessed 01/11/2021, 01/15/2022, 01/15/2023 and 04/01/2024 www.ocrportal.hhs.gov. Active and arch breaches 2024 FBI Internet Crime Complaint Center 2022 Annual Report (March 2023)



https://status.changehealthcare.com/incidents/hqpjz25fn3n7

Optum

Bloomberg

TechnologyCybersecurity

Change Healthcare Cyberattack Is Still Disrupting Ph… Providers

Update

Change…
interrup…
experts…
becam…

REUTERS®

Cybersecurity

US pharmacy out… 'Blackcat' ransom… unit, sources say

By Raphael Satter and Christopher Bing

February 26, 2024 3:28 PM EST · Updated 2 days ag…

American Hospital Association®
Advancing Health in America

Cybersecurity Advisory

February 26, 2024

UPDATE: New Bulletin on Change Healthcare Cyberattack Highlights Network Connectivity Issu…

WHITE

…ge Healthc…
…itedHealth…
…ntire health…
…ng informati…

…rt of those…
…in to provid…
…dHealth Gr…
…ving issues…
…stent with g…

WORK CON…

…ge Healthc…
…at customer…
…services.

…ge Healthc…
…dence that C…
…affected by…
…ment, and h…
…deration.

…rdingly, th…
…ediately re…
…m, Change…
…been deem…
…itor and ind…
…form its ow…

…n considerin…
…h care orga…
…cts caused…
…dHealthcare…

How a nationwide cyberattack is impacting Florida patients and hospitals

WUSF | By Gabriella Pinos

Published March 11, 2024 at 5:00 AM EDT

Wolterk / iStock Editorial

Change Healthcare, owned by insurance giant UnitedHealth Group, is an important part of the U.S. health care system, processing billions of transactions annually and matching up bills with insurance coverage.

FIERCE Healthcare

PAYERS

Another ransomware group is seeking a payout from Change Healthcare, according to cybersecurity analysts

By Paige Minemyer · Apr 8, 2024 12:15pm

Change Healthcare provides the technology for revenue cycle and payment management to multiple sectors within the healthcare industry. (Getty Images)

UPDATED: April 8 at 12:34 p.m.

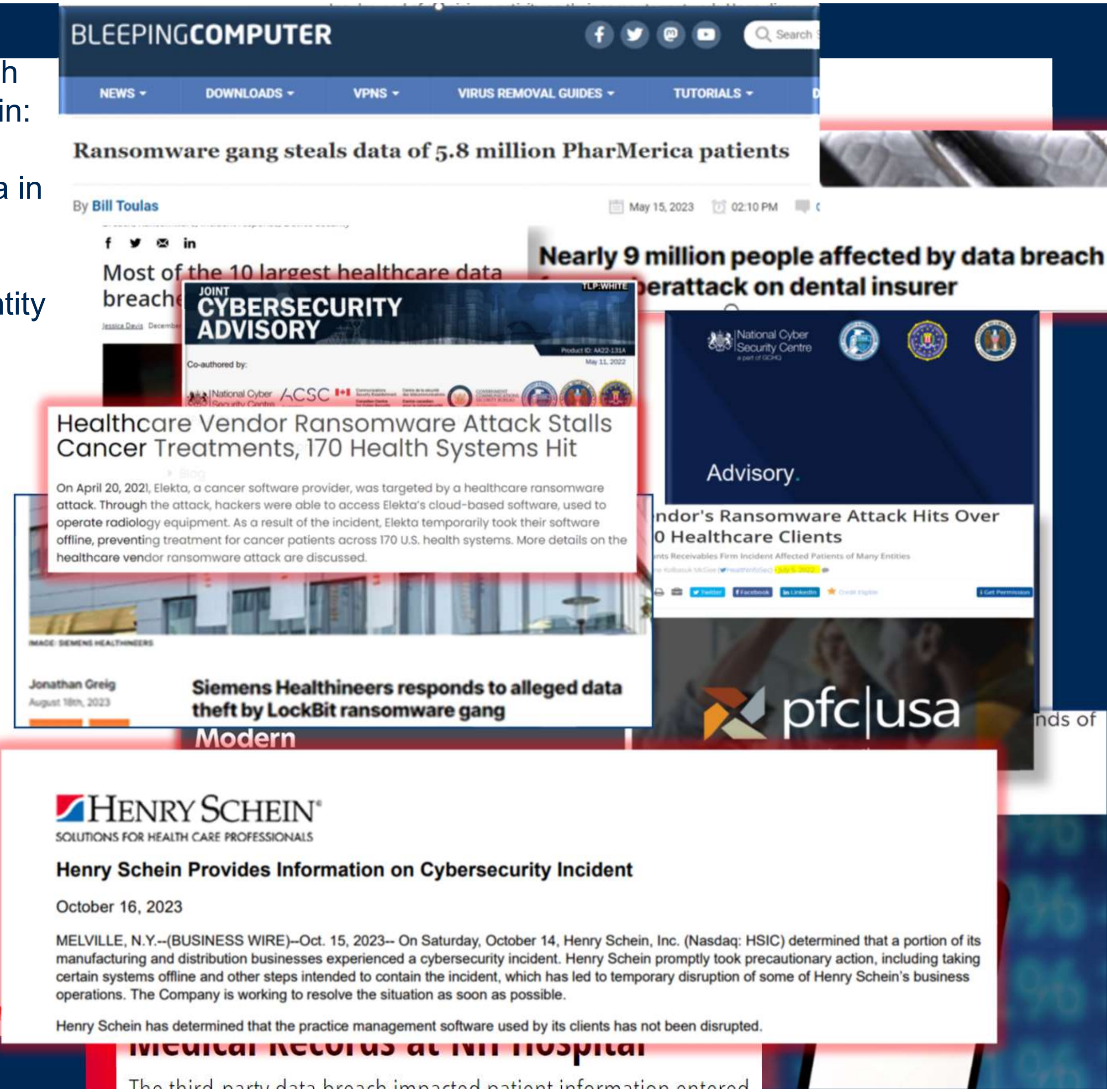
After the hackers responsible for the cyberattack on Change Healthcare took the ranso… and ran in a reported exit scam, cybersecurity experts have found a new post that is seeking a payout from UnitedHealth Group to recover the data.

A post from RansomHub claims to have four terabytes of data stolen from Change.

Primary Healthcare Cyber Threats

Third- and fourth-party cyber risk exposure through business associates, medical devices and supply chain:

- Theft of large quantities of covered entity data in possession of business associates –
- Third-party as digital pathway into covered entity
- Software and hardware supply chain attacks
- *Mission critical business associate becomes victim of ransomware attack*
- ***Dynamic*** *-Third Party Risk Management Program*
  - *Governance Committee - Include Privacy*
  - *Strategic risk identification*
  - *Risk stratification and prioritization*
  - ***Life, mission and business criticality***
  - ***Storage or access to sensitive data***
  - ***Network access –Privileged access?***
  - *Foreign operations and subcontractor risk*
  - *Technical cybersecurity posture*
  - *Consider aggregate risk from the 3rd party*
  - *Risk based cybersecurity requirements*
  - *Risk based cyber insurance requirements*
  - *Breach notification requirements*
  - ***Requirements Must be in BAA - Contractua***



Ransomware gang steals data of 5.8 million PharMerica patients

By Bill Toulas May 15, 2023 02:10 PM

Most of the 10 largest healthcare data breache

Jessica Davis Decembe

Nearly 9 million people affected by data breach …erattack on dental insurer

JOINT CYBERSECURITY ADVISORY

TLP:WHITE

Product ID: AA22-131A

May 11, 2022

Co-authored by:

National Cyber Security Centre ACSC

National Cyber Security Centre a part of GCHQ

Advisory.

Healthcare Vendor Ransomware Attack Stalls Cancer Treatments, 170 Health Systems Hit

On April 20, 2021, Elekta, a cancer software provider, was targeted by a healthcare ransomware attack. Through the attack, hackers were able to access Elekta's cloud-based software, used to operate radiology equipment. As a result of the incident, Elekta temporarily took their software offline, preventing treatment for cancer patients across 170 U.S. health systems. More details on the healthcare vendor ransomware attack are discussed.

…ndor's Ransomware Attack Hits Over …0 Healthcare Clients

…nts Receivables Firm Incident Affected Patients of Many Entities

IMAGE: SIEMENS HEALTHINEERS

Jonathan Greig
August 18th, 2023

Siemens Healthineers responds to alleged data theft by LockBit ransomware gang

Modern

pfc|usa

…nds of

HENRY SCHEIN®
SOLUTIONS FOR HEALTH CARE PROFESSIONALS

Henry Schein Provides Information on Cybersecurity Incident

October 16, 2023

MELVILLE, N.Y.--(BUSINESS WIRE)--Oct. 15, 2023-- On Saturday, October 14, Henry Schein, Inc. (Nasdaq: HSIC) determined that a portion of its manufacturing and distribution businesses experienced a cybersecurity incident. Henry Schein promptly took precautionary action, including taking certain systems offline and other steps intended to contain the incident, which has led to temporary disruption of some of Henry Schein's business operations. The Company is working to resolve the situation as soon as possible.

Henry Schein has determined that the practice management software used by its clients has not been disrupted.

Medical Records at NH Hospital

The third-party data breach impacted patient information entered

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

CNN politics SCOTUS Congress Facts First 2024 Elections

FBI director to warn that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure

By Hannah Rabinowitz, CNN
2 minute read · Published 5:00 AM EST, Wed January 31, 2024

agencies believe the actor could apply the same techniques against these and other

DIVE BRIEF

Cisco routers abused by China-linked hackers against US, Japan companies

A longstanding group, identified as BlackTech, uses custom malware to evade detection and hack into

Published Sept. 28, 2023

and network ac
would alert on t
amount of activ
tools this actor

Disclaimer: This document
risk of misuse, in accordanc
distributed without restrictio

U/OO/156893-23 | PP-

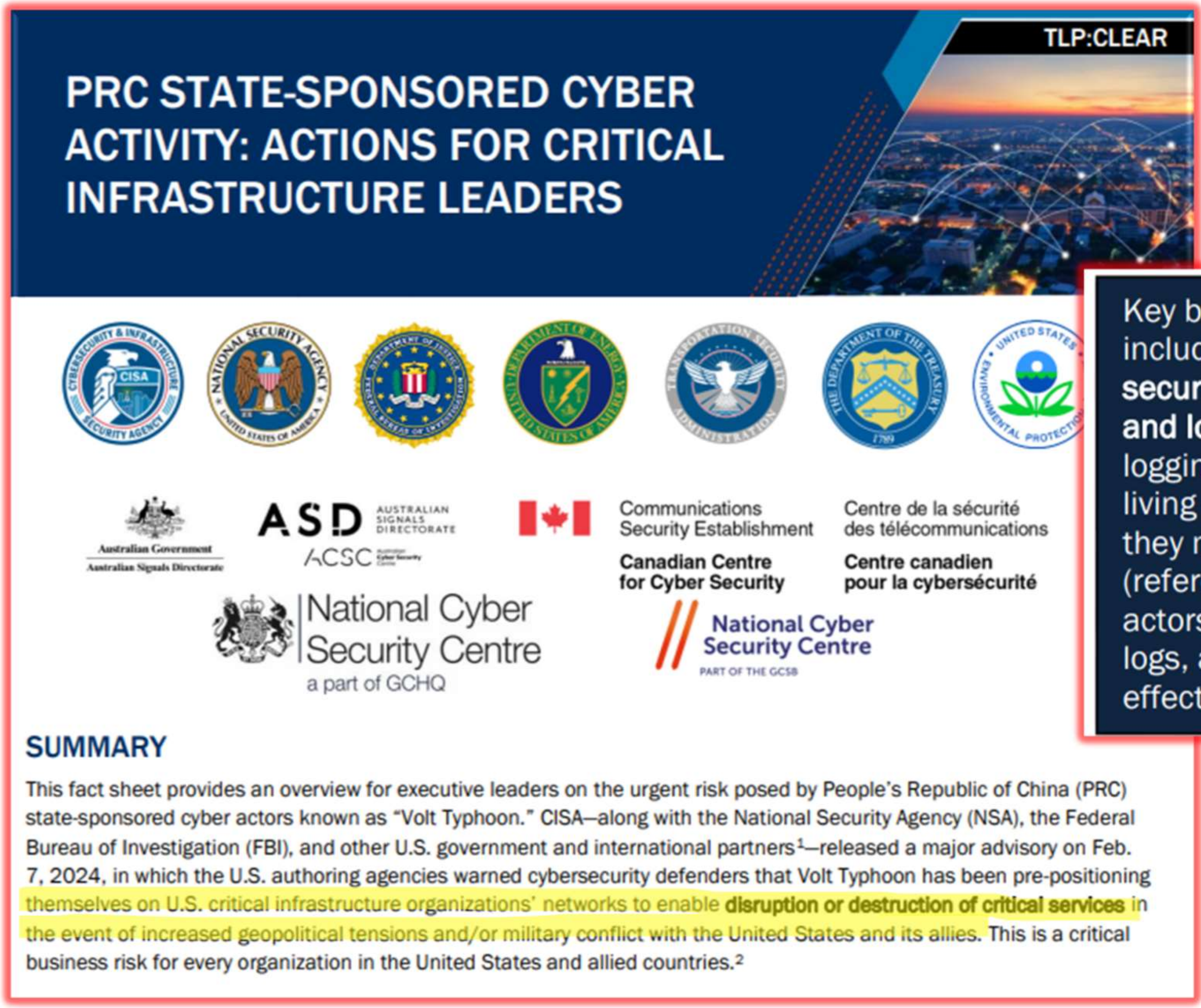
Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

UPDATE: Microsoft has released threat analysis on Storm-0558 activity here. Microsoft additionally released additional defense-in-depth security fixes to help customers improve token validation in their custom applications.

Microsoft has mitigated an attack by a China-based threat actor Microsoft tracks as Storm-0558 which targeted customer emails. Storm-0558 primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. Based on customer reported information on June 16, 2023, Microsoft began an investigation into anomalous mail activity. Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email accounts affecting approximately 25 organizations in the public cloud including government agencies as well as

*"Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure en the United States and Asia region **during future s."***



TLP:CLEAR

PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

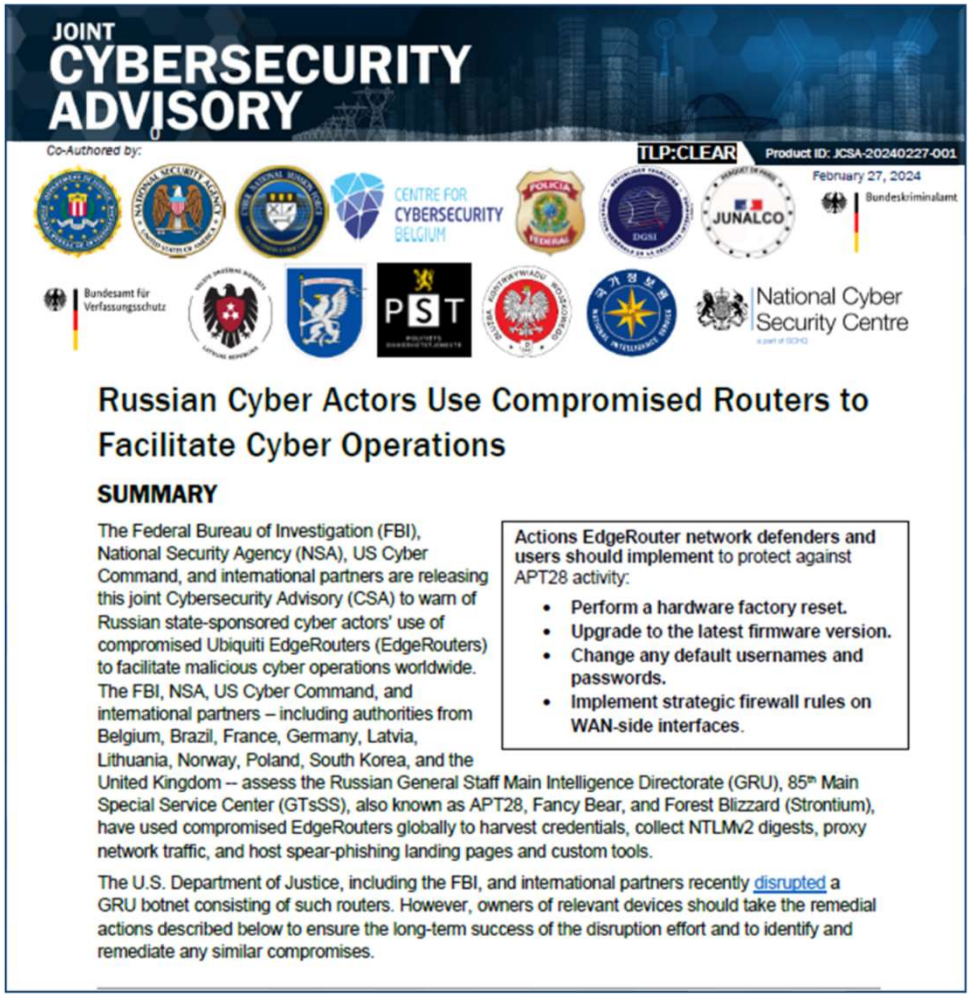
National Cyber Security Centre
PART OF THE GCSB

SUMMARY

This fact sheet provides an overview for executive leaders on the urgent risk posed by People's Republic of China (PRC) state-sponsored cyber actors known as "Volt Typhoon." CISA—along with the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and other U.S. government and international partners[1]—released a major advisory on Feb. 7, 2024, in which the U.S. authoring agencies warned cybersecurity defenders that Volt Typhoon has been pre-positioning themselves on U.S. critical infrastructure organizations' networks to enable **disruption or destruction of critical services** in the event of increased geopolitical tensions and/or military conflict with the United States and its allies. This is a critical business risk for every organization in the United States and allied countries.[2]

Key best practices for your cybersecurity teams includes **ensuring logging, including for access and security, is turned on for applications and systems and logs are stored in a central system**. Robust logging is necessary for detecting and mitigating living off the land. Ask your IT teams which logs they maintain as certain logs reveal commands (referenced in the CSA) used by Volt Typhoon actors. If your IT teams do not have the relevant logs, ask which resources they may need to effectively detect compromise.

American Hospital Association™
Advancing Health in America



JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR Product ID: JCSA-20240227-001

February 27, 2024

CENTRE FOR CYBERSECURITY BELGIUM

JUNALCO

Bundeskriminalamt

Bundesamt für Verfassungsschutz

PST

National Cyber Security Centre

Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations

SUMMARY

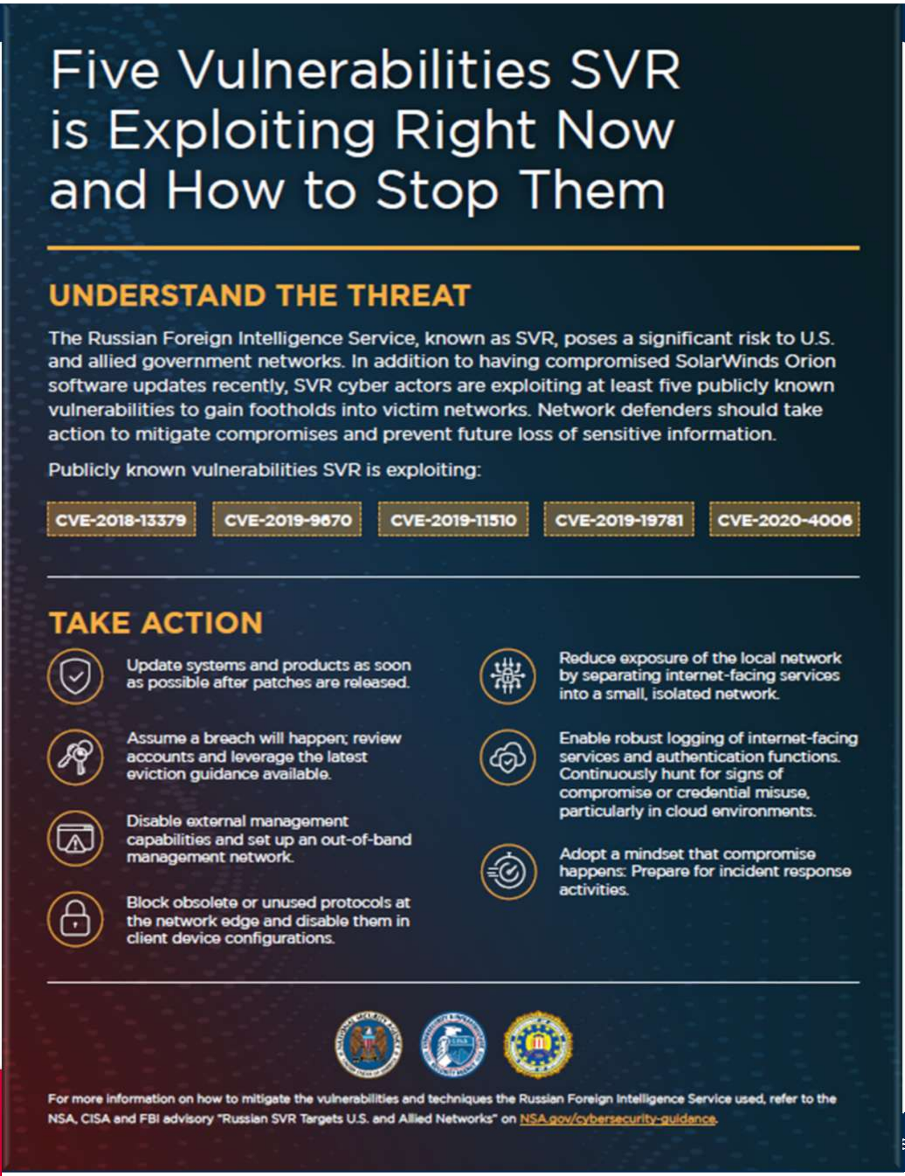
Actions EdgeRouter network defenders and users should implement to protect against APT28 activity:

- **Perform a hardware factory reset.**
- **Upgrade to the latest firmware version.**
- **Change any default usernames and passwords.**
- **Implement strategic firewall rules on WAN-side interfaces.**

The Federal Bureau of Investigation (FBI), National Security Agency (NSA), US Cyber Command, and international partners are releasing this joint Cybersecurity Advisory (CSA) to warn of Russian state-sponsored cyber actors' use of compromised Ubiquiti EdgeRouters (EdgeRouters) to facilitate malicious cyber operations worldwide.

The FBI, NSA, US Cyber Command, and international partners – including authorities from Belgium, Brazil, France, Germany, Latvia, Lithuania, Norway, Poland, South Korea, and the United Kingdom – assess the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS), also known as APT28, Fancy Bear, and Forest Blizzard (Strontium), have used compromised EdgeRouters globally to harvest credentials, collect NTLMv2 digests, proxy network traffic, and host spear-phishing landing pages and custom tools.

The U.S. Department of Justice, including the FBI, and international partners recently disrupted a GRU botnet consisting of such routers. However, owners of relevant devices should take the remedial actions described below to ensure the long-term success of the disruption effort and to identify and remediate any similar compromises.



Five Vulnerabilities SVR is Exploiting Right Now and How to Stop Them

UNDERSTAND THE THREAT

The Russian Foreign Intelligence Service, known as SVR, poses a significant risk to U.S. and allied government networks. In addition to having compromised SolarWinds Orion software updates recently, SVR cyber actors are exploiting at least five publicly known vulnerabilities to gain footholds into victim networks. Network defenders should take action to mitigate compromises and prevent future loss of sensitive information.

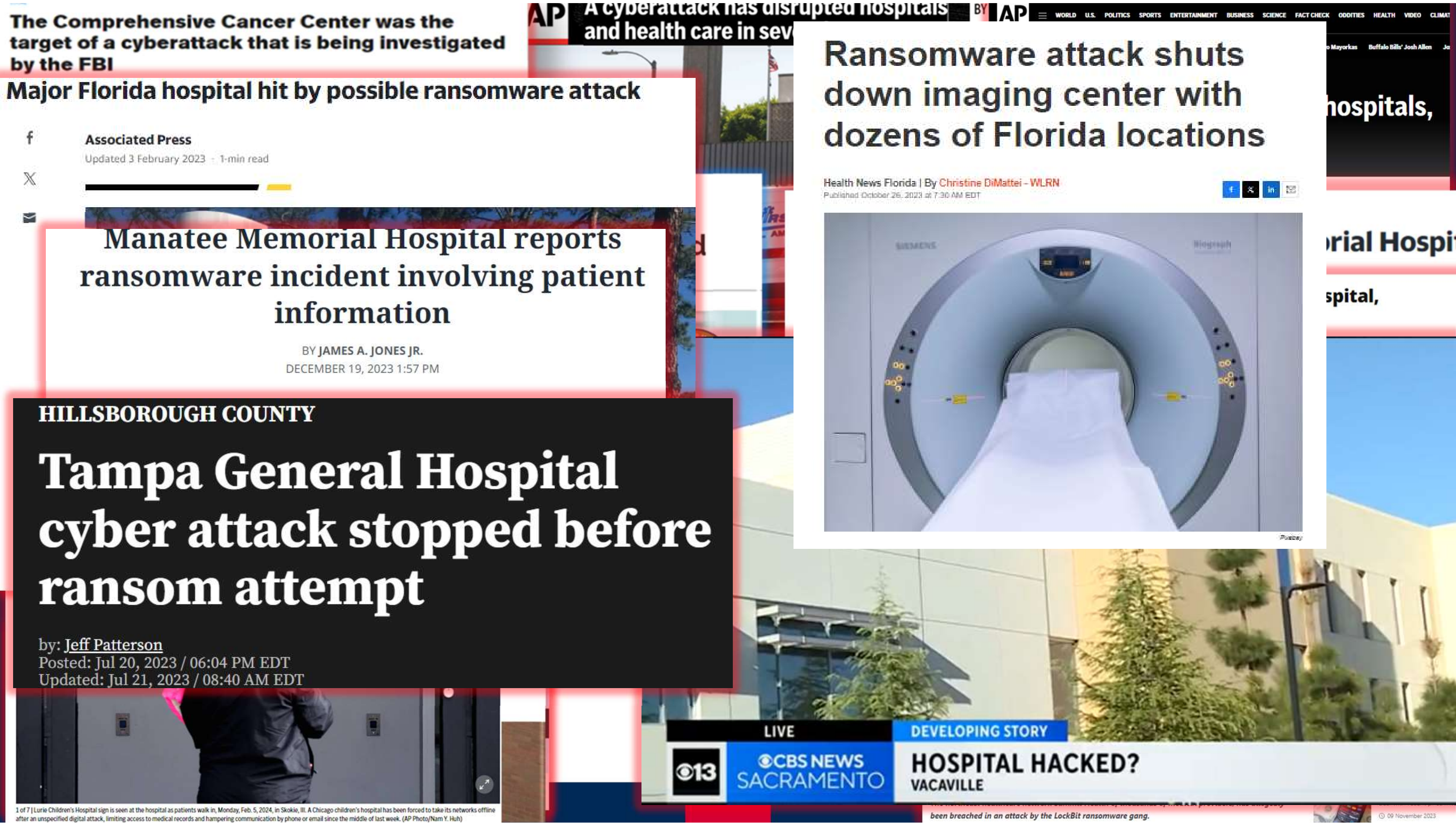
Publicly known vulnerabilities SVR is exploiting:

CVE-2018-13379 | CVE-2019-9670 | CVE-2019-11510 | CVE-2019-19781 | CVE-2020-4006

TAKE ACTION

- Update systems and products as soon as possible after patches are released.
- Assume a breach will happen; review accounts and leverage the latest eviction guidance available.
- Disable external management capabilities and set up an out-of-band management network.
- Block obsolete or unused protocols at the network edge and disable them in client device configurations.
- Reduce exposure of the local network by separating internet-facing services into a small, isolated network.
- Enable robust logging of internet-facing services and authentication functions. Continuously hunt for signs of compromise or credential misuse, particularly in cloud environments.
- Adopt a mindset that compromise happens: Prepare for incident response activities.

For more information on how to mitigate the vulnerabilities and techniques the Russian Foreign Intelligence Service used, refer to the NSA, CISA and FBI advisory "Russian SVR Targets U.S. and Allied Networks" on NSA.gov/cybersecurity-guidance.



The Comprehensive Cancer Center was the target of a cyberattack that is being investigated by the FBI

AP A cyberattack has disrupted hospitals and health care in sev

BY AP

hospitals,

Major Florida hospital hit by possible ransomware attack

Associated Press

Updated 3 February 2023 · 1-min read

Manatee Memorial Hospital reports ransomware incident involving patient information

BY JAMES A. JONES JR.

DECEMBER 19, 2023 1:57 PM

Ransomware attack shuts down imaging center with dozens of Florida locations

Health News Florida | By Christine DiMattei - WLRN

Published October 26, 2023 at 7:30 AM EDT

Pixabay

rial Hospi

spital,

HILLSBOROUGH COUNTY

Tampa General Hospital cyber attack stopped before ransom attempt

by: Jeff Patterson

Posted: Jul 20, 2023 / 06:04 PM EDT

Updated: Jul 21, 2023 / 08:40 AM EDT

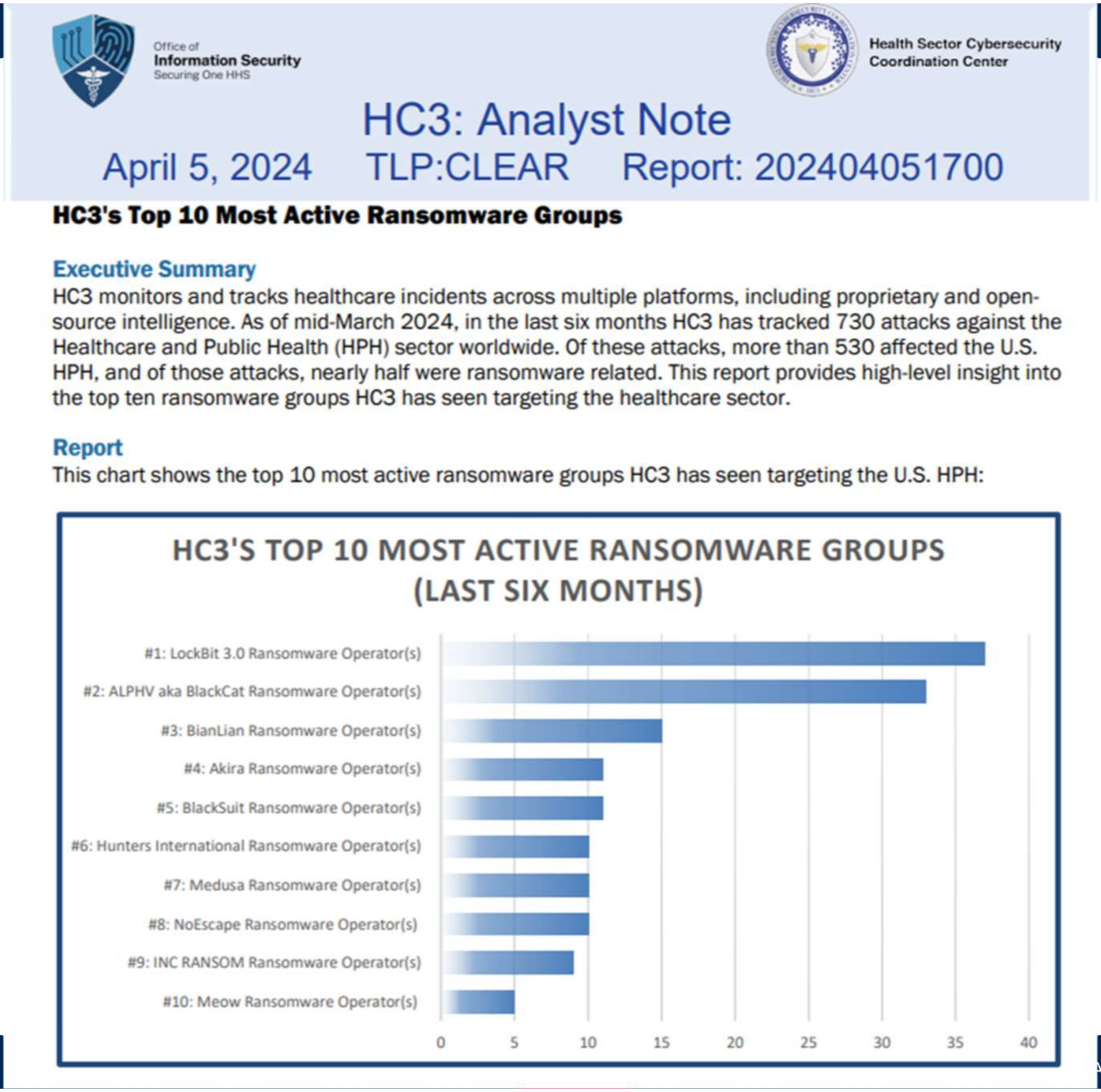
1 of 7 | Lurie Children's Hospital sign is seen at the hospital as patients walk in, Monday, Feb. 5, 2024, in Skokie, Ill. A Chicago children's hospital has been forced to take its networks offline after an unspecified digital attack, limiting access to medical records and hampering communication by phone or email since the middle of last week. (AP Photo/Nam Y. Huh)

HOSPITAL HACKED?

VACAVILLE

been breached in an attack by the LockBit ransomware gang.

09 November 2023



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Analyst Note

April 5, 2024 TLP:CLEAR Report: 202404051700

HC3's Top 10 Most Active Ransomware Groups

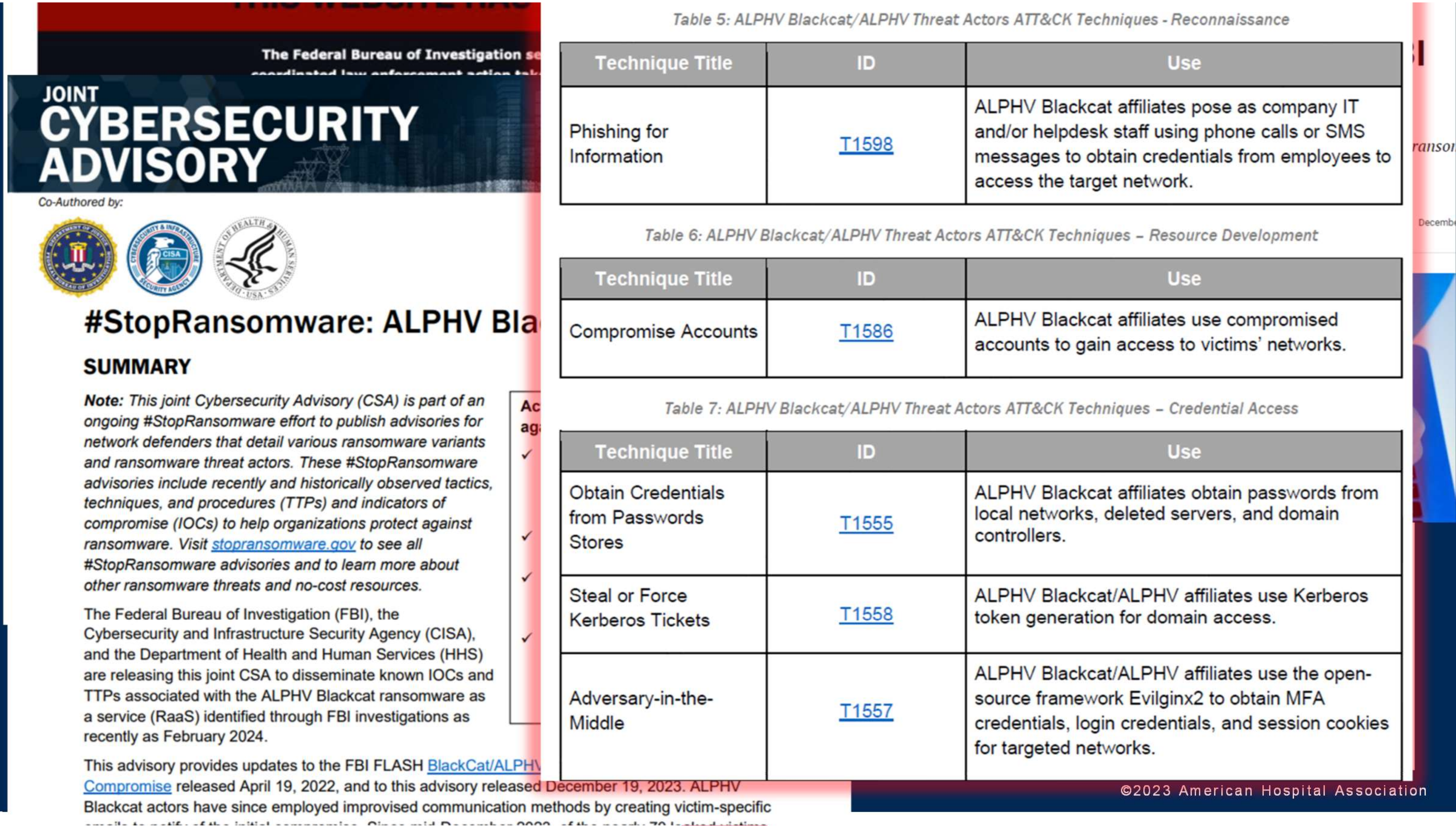
Executive Summary

HC3 monitors and tracks healthcare incidents across multiple platforms, including proprietary and open-source intelligence. As of mid-March 2024, in the last six months HC3 has tracked 730 attacks against the Healthcare and Public Health (HPH) sector worldwide. Of these attacks, more than 530 affected the U.S. HPH, and of those attacks, nearly half were ransomware related. This report provides high-level insight into the top ten ransomware groups HC3 has seen targeting the healthcare sector.

Report

This chart shows the top 10 most active ransomware groups HC3 has seen targeting the U.S. HPH:

HC3'S TOP 10 MOST ACTIVE RANSOMWARE GROUPS
(LAST SIX MONTHS)
#1: LockBit 3.0 Ransomware Operator(s)
#2: ALPHV aka BlackCat Ransomware Operator(s)
#3: BianLian Ransomware Operator(s)
#4: Akira Ransomware Operator(s)
#5: BlackSuit Ransomware Operator(s)
#6: Hunters International Ransomware Operator(s)
#7: Medusa Ransomware Operator(s)
#8: NoEscape Ransomware Operator(s)
#9: INC RANSOM Ransomware Operator(s)
#10: Meow Ransomware Operator(s)
0
5
10
15
20
25
30
35
40



The Federal Bureau of Investigation se

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

#StopRansomware: ALPHV Bla

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit* stopransomware.gov *to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) are releasing this joint CSA to disseminate known IOCs and TTPs associated with the ALPHV Blackcat ransomware as a service (RaaS) identified through FBI investigations as recently as February 2024.

Ac
ag
✓
✓
✓
✓

This advisory provides updates to the FBI FLASH BlackCat/ALPHV Compromise released April 19, 2022, and to this advisory released December 19, 2023. ALPHV Blackcat actors have since employed improvised communication methods by creating victim-specific

Table 5: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques - Reconnaissance

Technique Title	ID	Use
Phishing for Information	T1598	ALPHV Blackcat affiliates pose as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees to access the target network.

Table 6: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Resource Development

Technique Title	ID	Use
Compromise Accounts	T1586	ALPHV Blackcat affiliates use compromised accounts to gain access to victims' networks.

Table 7: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Credential Access

Technique Title	ID	Use
Obtain Credentials from Passwords Stores	T1555	ALPHV Blackcat affiliates obtain passwords from local networks, deleted servers, and domain controllers.
Steal or Force Kerberos Tickets	T1558	ALPHV Blackcat/ALPHV affiliates use Kerberos token generation for domain access.
Adversary-in-the-Middle	T1557	ALPHV Blackcat/ALPHV affiliates use the open-source framework Evilginx2 to obtain MFA credentials, login credentials, and session cookies for targeted networks.

ranso

Decemb

August 15, 2023

LockBit 3.0 Ransomware

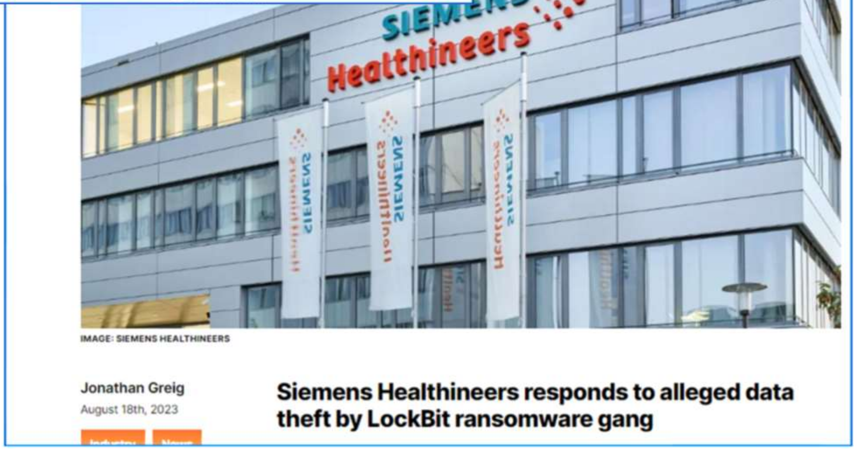


IMAGE: SIEMENS HEALTHINEERS

Jonathan Greig
August 18th, 2023

Siemens Healthineers responds to alleged data theft by LockBit ransomware gang

Co-Authored by:

TLP:CLEAR Product ID: AA23-165A

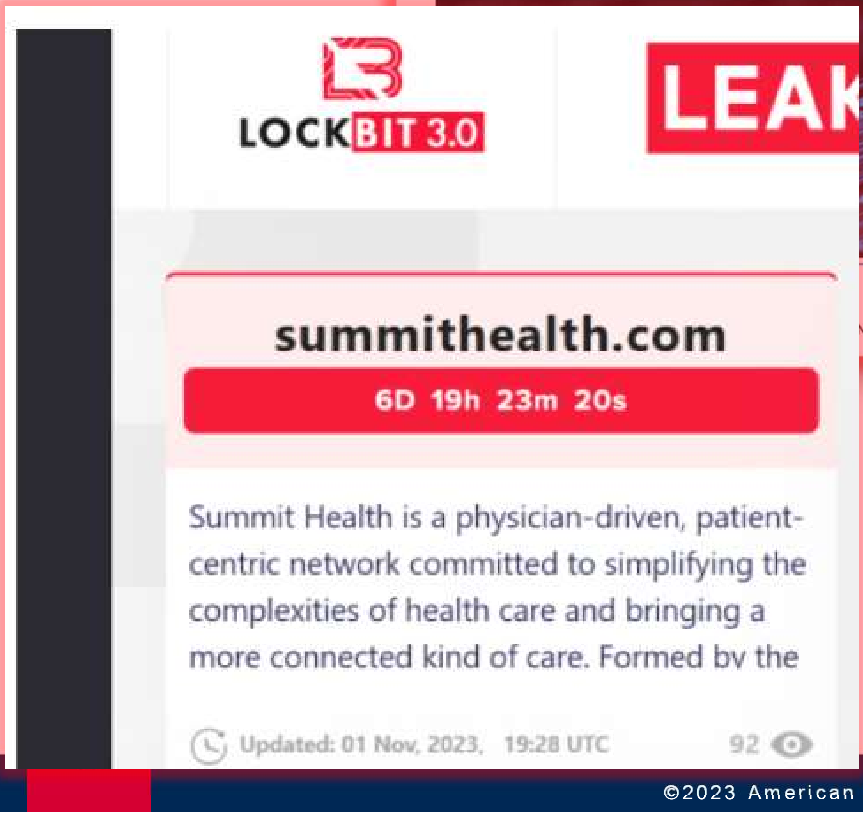
June 14, 2023

MS-ISAC®
Multi-State Information Sharing & Analysis Center®
Communications Security Establishment
Centre de la sécurité des télécommunications
Canadian Centre for Cyber Security
Centre canadien pour la cybersécurité
National Cyber Security Centre
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
RÉPUBLIQUE FRANÇAISE
Federal Office for Information Security
certnz
National Cyber Security Centre

UNDERSTANDING RANSOMWARE THREAT ACTORS:

LockBit

NZ | NCSC-NZ

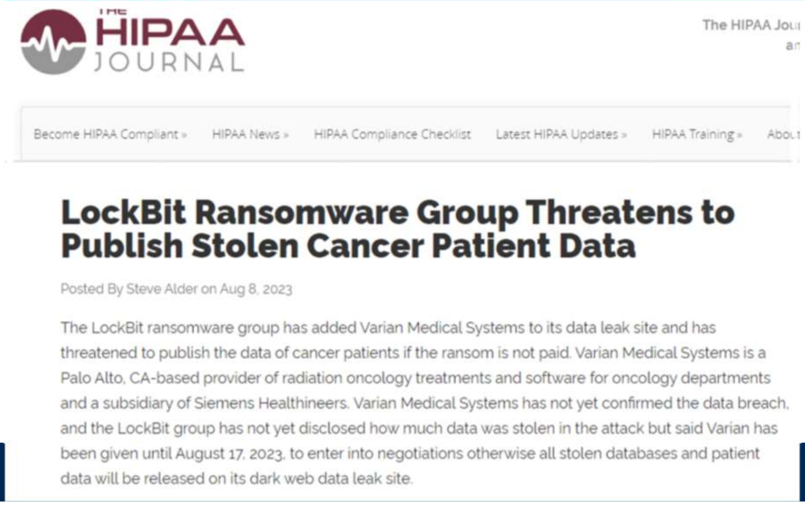


summithealth.com

6D 19h 23m 20s

Summit Health is a physician-driven, patient-centric network committed to simplifying the complexities of health care and bringing a more connected kind of care. Formed bv the

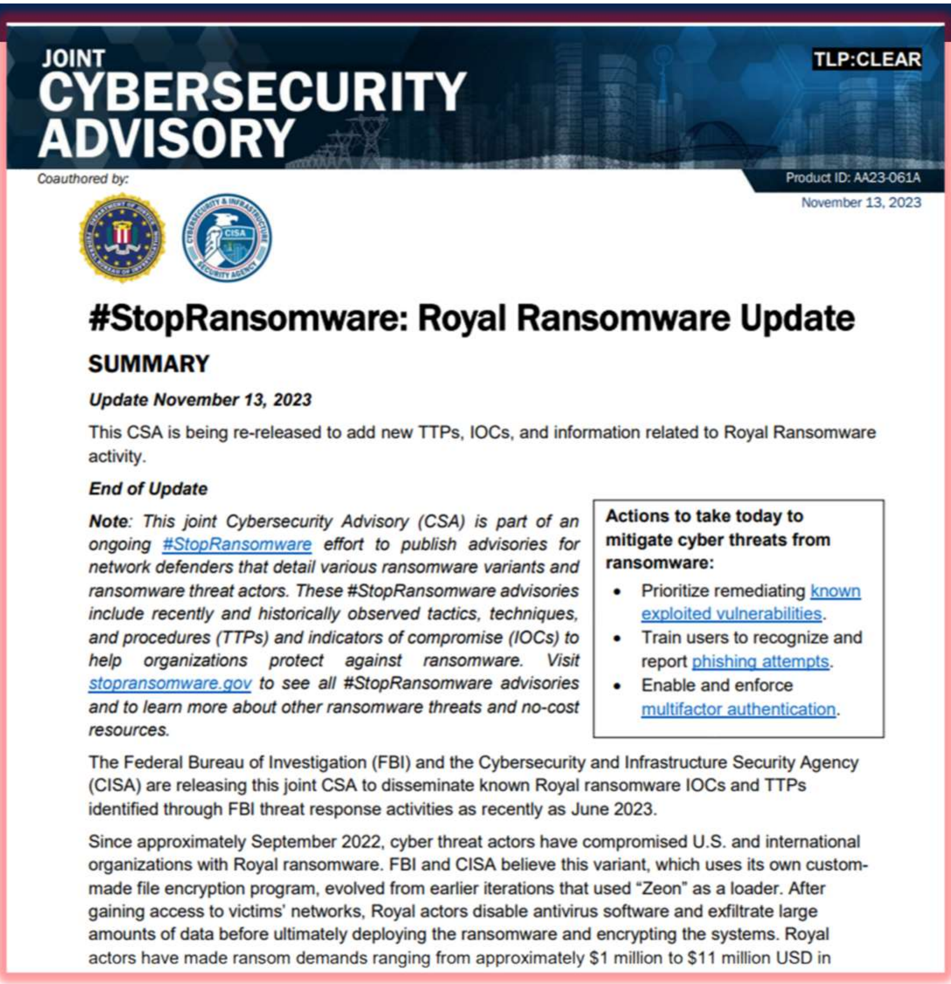
Updated: 01 Nov, 2023, 19:28 UTC 92



LockBit Ransomware Group Threatens to Publish Stolen Cancer Patient Data

Posted By Steve Alder on Aug 8, 2023

The LockBit ransomware group has added Varian Medical Systems to its data leak site and has threatened to publish the data of cancer patients if the ransom is not paid. Varian Medical Systems is a Palo Alto, CA-based provider of radiation oncology treatments and software for oncology departments and a subsidiary of Siemens Healthineers. Varian Medical Systems has not yet confirmed the data breach, and the LockBit group has not yet disclosed how much data was stolen in the attack but said Varian has been given until August 17, 2023, to enter into negotiations otherwise all stolen databases and patient data will be released on its dark web data leak site.



JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Coauthored by:

Product ID: AA23-061A

November 13, 2023

#StopRansomware: Royal Ransomware Update

SUMMARY

Update November 13, 2023

This CSA is being re-released to add new TTPs, IOCs, and information related to Royal Ransomware activity.

End of Update

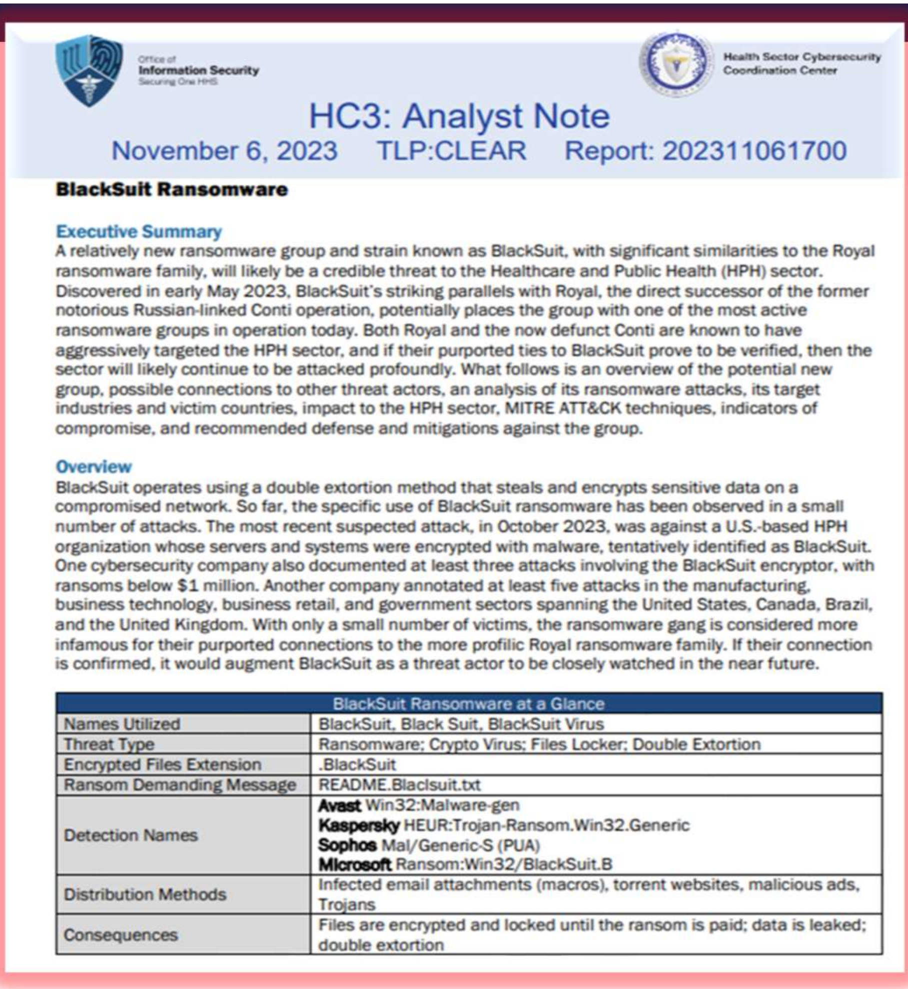
Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

***Note**: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as June 2023.

Since approximately September 2022, cyber threat actors have compromised U.S. and international organizations with Royal ransomware. FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader. After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems. Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in



Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

November 6, 2023 TLP:CLEAR Report: 202311061700

BlackSuit Ransomware

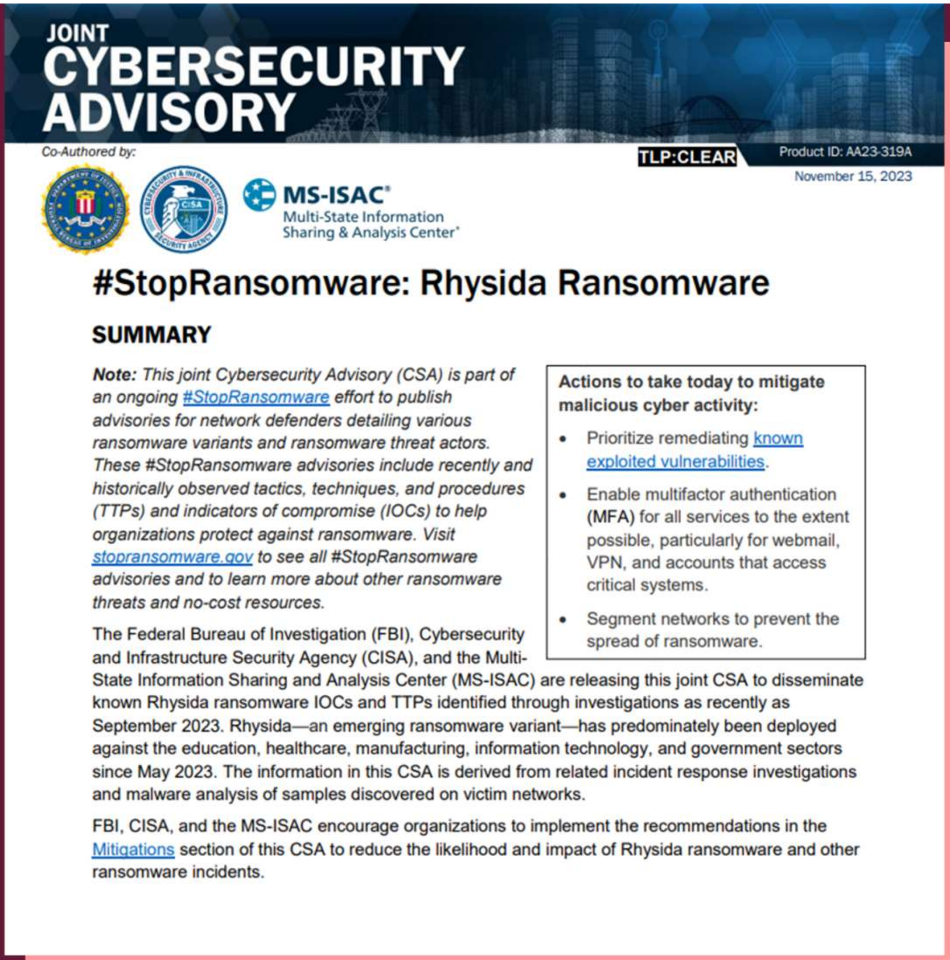
Executive Summary

A relatively new ransomware group and strain known as BlackSuit, with significant similarities to the Royal ransomware family, will likely be a credible threat to the Healthcare and Public Health (HPH) sector. Discovered in early May 2023, BlackSuit's striking parallels with Royal, the direct successor of the former notorious Russian-linked Conti operation, potentially places the group with one of the most active ransomware groups in operation today. Both Royal and the now defunct Conti are known to have aggressively targeted the HPH sector, and if their purported ties to BlackSuit prove to be verified, then the sector will likely continue to be attacked profoundly. What follows is an overview of the potential new group, possible connections to other threat actors, an analysis of its ransomware attacks, its target industries and victim countries, impact to the HPH sector, MITRE ATT&CK techniques, indicators of compromise, and recommended defense and mitigations against the group.

Overview

BlackSuit operates using a double extortion method that steals and encrypts sensitive data on a compromised network. So far, the specific use of BlackSuit ransomware has been observed in a small number of attacks. The most recent suspected attack, in October 2023, was against a U.S.-based HPH organization whose servers and systems were encrypted with malware, tentatively identified as BlackSuit. One cybersecurity company also documented at least three attacks involving the BlackSuit encryptor, with ransoms below $1 million. Another company annotated at least five attacks in the manufacturing, business technology, business retail, and government sectors spanning the United States, Canada, Brazil, and the United Kingdom. With only a small number of victims, the ransomware gang is considered more infamous for their purported connections to the more profilic Royal ransomware family. If their connection is confirmed, it would augment BlackSuit as a threat actor to be closely watched in the near future.

BlackSuit Ransomware at a Glance	
Names Utilized	BlackSuit, Black Suit, BlackSuit Virus
Threat Type	Ransomware; Crypto Virus; Files Locker; Double Extortion
Encrypted Files Extension	.BlackSuit
Ransom Demanding Message	README.Blaclsuit.txt
Detection Names	**Avast** Win32:Malware-gen **Kaspersky** HEUR:Trojan-Ransom.Win32.Generic **Sophos** Mal/Generic-S (PUA) **Microsoft** Ransom:Win32/BlackSuit.B
Distribution Methods	Infected email attachments (macros), torrent websites, malicious ads, Trojans
Consequences	Files are encrypted and locked until the ransom is paid; data is leaked; double extortion



JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

TLP:CLEAR

Product ID: AA23-319A

November 15, 2023

#StopRansomware: Rhysida Ransomware

SUMMARY

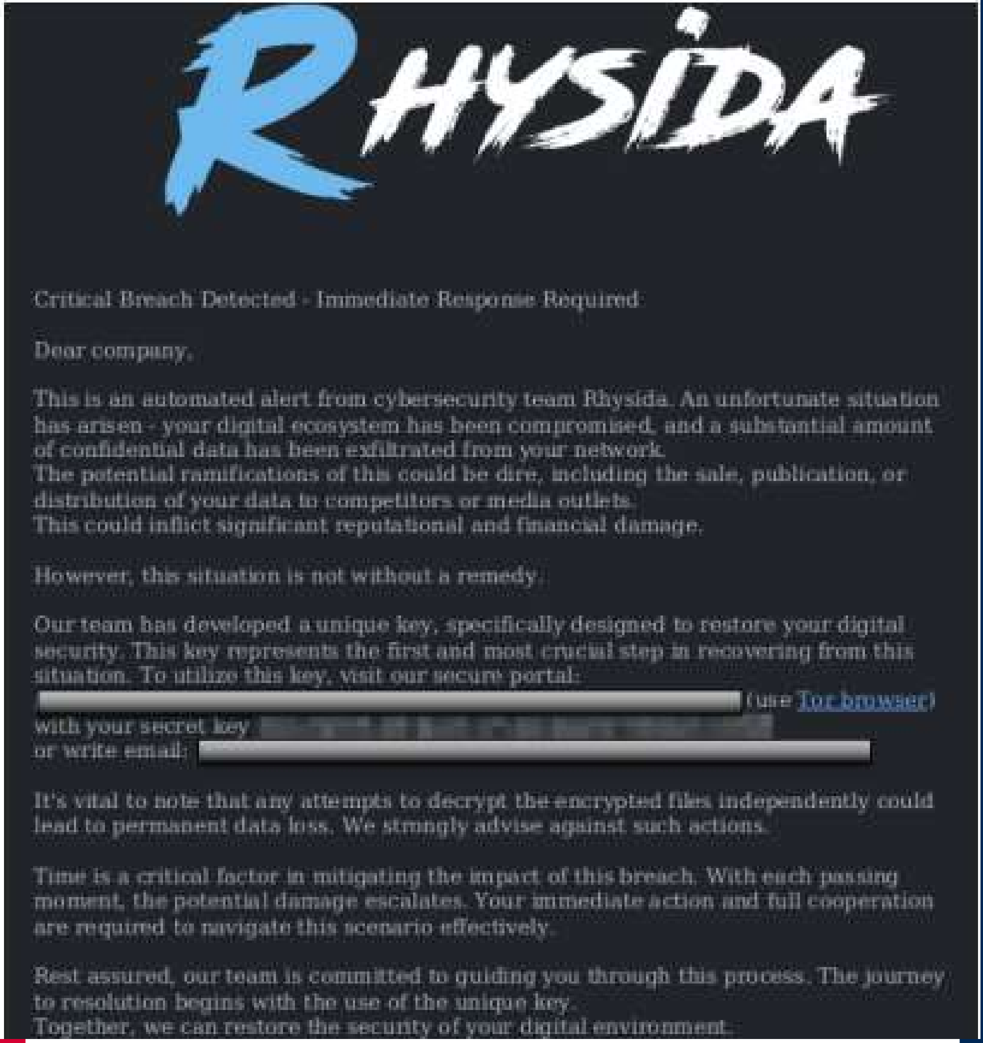
Actions to take today to mitigate malicious cyber activity:

- 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.

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.*

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.



Critical Breach Detected - Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen - your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network.
The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets.
This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal:
[redacted] (use Tor browser)
with your secret key [redacted]
or write email: [redacted]

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key.
Together, we can restore the security of your digital environment.

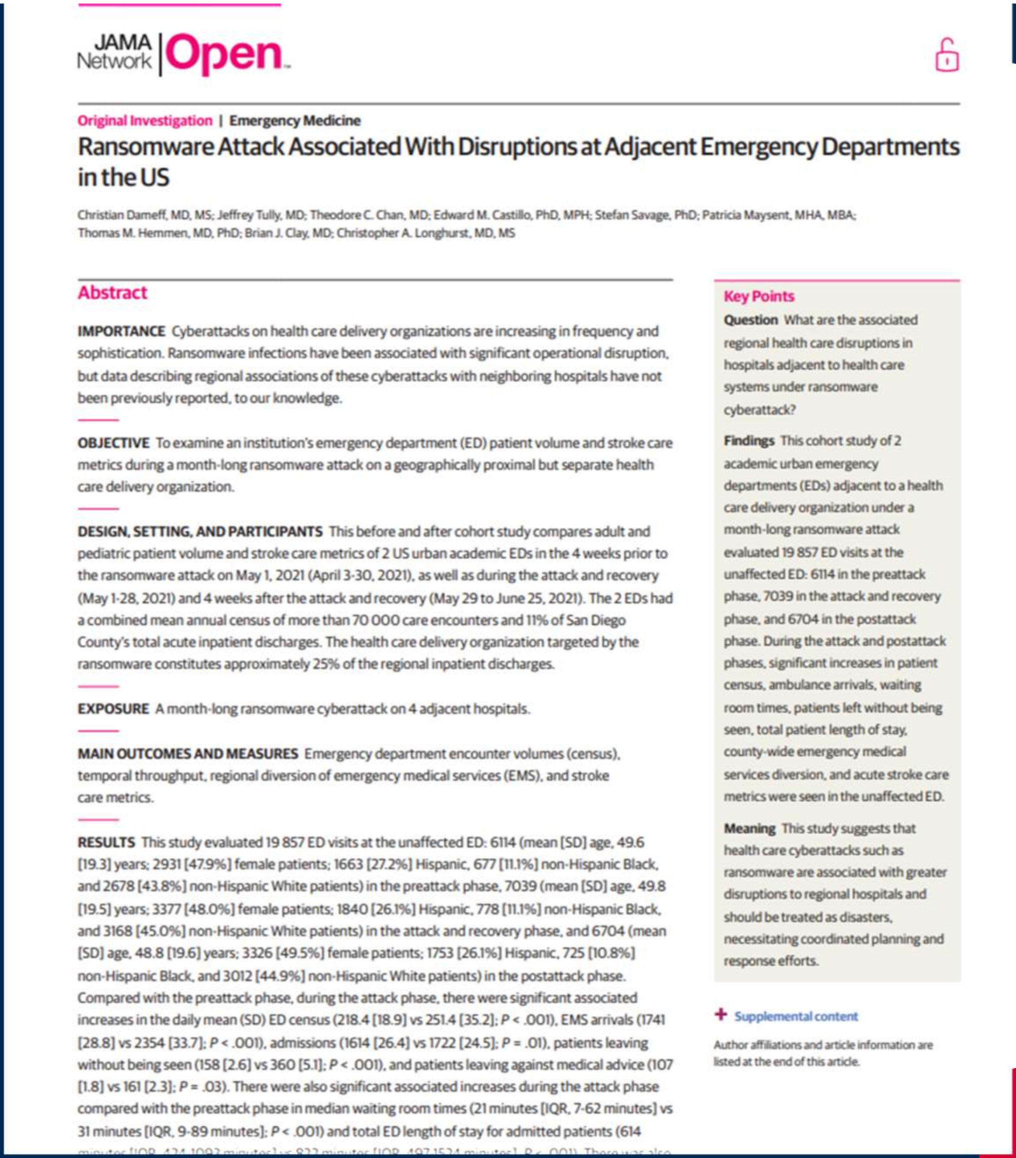
MIAMI-DADE COUNTY
HEALTHCARE PREPAREDNESS
COALITION
EMERGENCY
PREPAREDNESS

Cyber Risk Impact to Patient Safety

Reported Clinical and Business Impact of Ransomware Attacks on Hospitals 2020 – 2023

- **Radiology / Imaging / PACS down - other diagnostic technology lost. Remote radiology lost. All could lead to stroke and trauma diversion**
- **Cath lab down = heart attack diversion**
- ***Risk to patient safety*. ED's shutdown - Ambulances placed on full divert - rural distance** delay of emergency treatment. Trauma Center availability
- **Telemetry systems inoperable** – additional staff required for patient monitoring - Home health care telemetry. *Patients at home, greater risk?*
- **EHR rendered inaccessible**. Patient history, treatment protocols, drug allergies / interactions unknown – delay in rendering care

- **Lab** and **Pathology** disrupted
- Elective **surgeries** cancelled
- **ADT** forms and instructions unavailable
- **Drug cabinet**/ **pharmacy** systems down
- **Loss of VoIP phones and email systems**
- **Ransomware "blast radius"** – **effect on other providers who are dependent** for ED, EMR, labs, imaging, cancer treatment and other third parties also disrupted.
- **Regional impact** and stress based upon **capacity** of surrounding hospitals
- Simultaneous loss of all network and internet connected information, medical and operational technology – ***Downtime computers lost or limited data.***
- ***ED wait times significantly increased.***
- **Radiation oncology (RADONC)** treatment may be dependent upon network and internet connected technology.
- Extended delay of treatment when diverted to alternate RADONC treatment facilities.
- **Chemotherapy** and RADONC treatment plans may not be available.
- **Staff unprepared for extended clinical downtime procedures for *all functions* and paper EMR charting lasting up to three to four weeks**
- ***Three to four week recovery time*** *for mission critical systems, ransom paid or not,* ***residual impacts lasting 6 months - 2 years***
- **Backups corrupted or only 65% restoration from uncorrupted backups. RTO and RPO not fully understood.**
- Legacy systems unrecoverable
- **Revenue** interruption and revenue **loss** due to incomplete charts. **Need 60 days cash on hand – no income for 60 days.**
- **Scheduling, timekeeping and payroll systems disrupted**
- **Operational and physical security technology impact**, access control
- **Third parties** requesting independent certification before reconnection
- Increased **insurance** premiums or loss of coverage
- **Civil liability** for publicly released PHI or negative outcome
- State and federal **regulatory liability + Reputational Harm**



JAMA Network | Open

Original Investigation | Emergency Medicine

Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

Christian Dameff, MD, MS; Jeffrey Tully, MD; Theodore C. Chan, MD; Edward M. Castillo, PhD, MPH; Stefan Savage, PhD; Patricia Maysent, MHA, MBA; Thomas M. Hemmen, MD, PhD; Brian J. Clay, MD; Christopher A. Longhurst, MD, MS

Abstract

IMPORTANCE Cyberattacks on health care delivery organizations are increasing in frequency and sophistication. Ransomware infections have been associated with significant operational disruption, but data describing regional associations of these cyberattacks with neighboring hospitals have not been previously reported, to our knowledge.

OBJECTIVE To examine an institution's emergency department (ED) patient volume and stroke care metrics during a month-long ransomware attack on a geographically proximal but separate health care delivery organization.

DESIGN, SETTING, AND PARTICIPANTS This before and after cohort study compares adult and pediatric patient volume and stroke care metrics of 2 US urban academic EDs in the 4 weeks prior to the ransomware attack on May 1, 2021 (April 3-30, 2021), as well as during the attack and recovery (May 1-28, 2021) and 4 weeks after the attack and recovery (May 29 to June 25, 2021). The 2 EDs had a combined mean annual census of more than 70 000 care encounters and 11% of San Diego County's total acute inpatient discharges. The health care delivery organization targeted by the ransomware constitutes approximately 25% of the regional inpatient discharges.

EXPOSURE A month-long ransomware cyberattack on 4 adjacent hospitals.

MAIN OUTCOMES AND MEASURES Emergency department encounter volumes (census), temporal throughput, regional diversion of emergency medical services (EMS), and stroke care metrics.

RESULTS This study evaluated 19 857 ED visits at the unaffected ED: 6114 (mean [SD] age, 49.6 [19.3] years; 2931 [47.9%] female patients; 1663 [27.2%] Hispanic, 677 [11.1%] non-Hispanic Black, and 2678 [43.8%] non-Hispanic White patients) in the preattack phase, 7039 (mean [SD] age, 49.8 [19.5] years; 3377 [48.0%] female patients; 1840 [26.1%] Hispanic, 778 [11.1%] non-Hispanic Black, and 3168 [45.0%] non-Hispanic White patients) in the attack and recovery phase, and 6704 (mean [SD] age, 48.8 [19.6] years; 3326 [49.5%] female patients; 1753 [26.1%] Hispanic, 725 [10.8%] non-Hispanic Black, and 3012 [44.9%] non-Hispanic White patients) in the postattack phase. Compared with the preattack phase, during the attack phase, there were significant associated increases in the daily mean (SD) ED census (218.4 [18.9] vs 251.4 [35.2]; *P* < .001), EMS arrivals (1741 [28.8] vs 2354 [33.7]; *P* < .001), admissions (1614 [26.4] vs 1722 [24.5]; *P* = .01), patients leaving without being seen (158 [2.6] vs 360 [5.1]; *P* < .001), and patients leaving against medical advice (107 [1.8] vs 161 [2.3]; *P* = .03). There were also significant associated increases during the attack phase compared with the preattack phase in median waiting room times (21 minutes [IQR, 7-62 minutes] vs 31 minutes [IQR, 9-89 minutes]; *P* < .001) and total ED length of stay for admitted patients (614 minutes [IQR, 424-1093 minutes] vs 822 minutes [IQR, 497-1524 minutes]; *P* < .001). There was also

Key Points

Question What are the associated regional health care disruptions in hospitals adjacent to health care systems under ransomware cyberattack?

Findings This cohort study of 2 academic urban emergency departments (EDs) adjacent to a health care delivery organization under a month-long ransomware attack evaluated 19 857 ED visits at the unaffected ED: 6114 in the preattack phase, 7039 in the attack and recovery phase, and 6704 in the postattack phase. During the attack and postattack phases, significant increases in patient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics were seen in the unaffected ED.

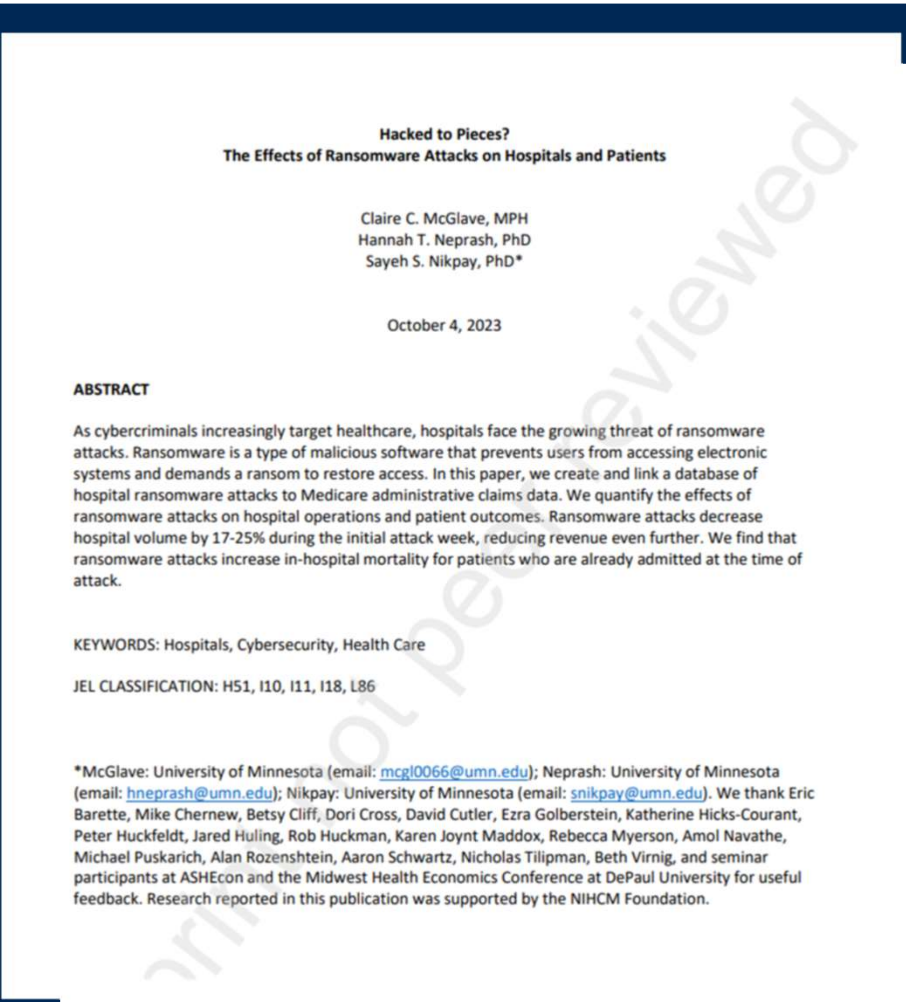
Meaning This study suggests that health care cyberattacks such as ransomware are associated with greater disruptions to regional hospitals and should be treated as disasters, necessitating coordinated planning and response efforts.

+ Supplemental content

Author affiliations and article information are listed at the end of this article.

- *The data showed "significant increases in patient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics were seen in the unaffected emergency department… during the attack and postattack phases."*
- The study showed a "significant increase in stroke code activations during the attack phase compared with the pre-attack phase, as well as confirmed strokes."
- "Increasing cyberattack prevention efforts and operational resiliency across all health care systems should be a high national priority."

Cyberattacks against hospitals should be treated as regional disasters since patients have to be diverted to other hospital to receive care, a new JAMA study concluded. (Getty Images)



Hacked to Pieces?
The Effects of Ransomware Attacks on Hospitals and Patients

Claire C. McGlave, MPH
Hannah T. Neprash, PhD
Sayeh S. Nikpay, PhD*

October 4, 2023

ABSTRACT

As cybercriminals increasingly target healthcare, hospitals face the growing threat of ransomware attacks. Ransomware is a type of malicious software that prevents users from accessing electronic systems and demands a ransom to restore access. In this paper, we create and link a database of hospital ransomware attacks to Medicare administrative claims data. We quantify the effects of ransomware attacks on hospital operations and patient outcomes. Ransomware attacks decrease hospital volume by 17-25% during the initial attack week, reducing revenue even further. We find that ransomware attacks increase in-hospital mortality for patients who are already admitted at the time of attack.

KEYWORDS: Hospitals, Cybersecurity, Health Care

JEL CLASSIFICATION: H51, I10, I11, I18, L86

*McGlave: University of Minnesota (email: mcgl0066@umn.edu); Neprash: University of Minnesota (email: hneprash@umn.edu); Nikpay: University of Minnesota (email: snikpay@umn.edu). We thank Eric Barette, Mike Chernew, Betsy Cliff, Dori Cross, David Cutler, Ezra Golberstein, Katherine Hicks-Courant, Peter Huckfeldt, Jared Huling, Rob Huckman, Karen Joynt Maddox, Rebecca Myerson, Amol Navathe, Michael Puskarich, Alan Rozenshtein, Aaron Schwartz, Nicholas Tilipman, Beth Virnig, and seminar participants at ASHEcon and the Midwest Health Economics Conference at DePaul University for useful feedback. Research reported in this publication was supported by the NIHCM Foundation.

October 4, 2023

- "In this paper, we create and link a database of hospital ransomware attacks to Medicare administrative claims data.
- We quantify the effects of ransomware attacks on hospital operations and patient outcomes.
- Ransomware attacks decrease hospital volume by 17-25% during the initial attack week, reducing revenue even further.
- *We find that ransomware attacks increase in-hospital mortality for patients who are already admitted at the time of attack*
- The mortality consequences of ransomware attacks will not surprise some in the cybersecurity and law enforcement communities, where ransomware attacks are viewed as "threat to life" crimes. "

FBI Director Wray talks cyberattacks, workplace violence

Apr 25, 2023 - 03:49 PM

More than 1,000 executive leaders from the nation's top hospitals and health systems convened at the 2023 AHA Annual Membership Meeting, April 23-25 in Washington, D.C.

FBI Director Wray talks cyberattacks, workplace violence

Apr 25, 2023 - 03:49 PM

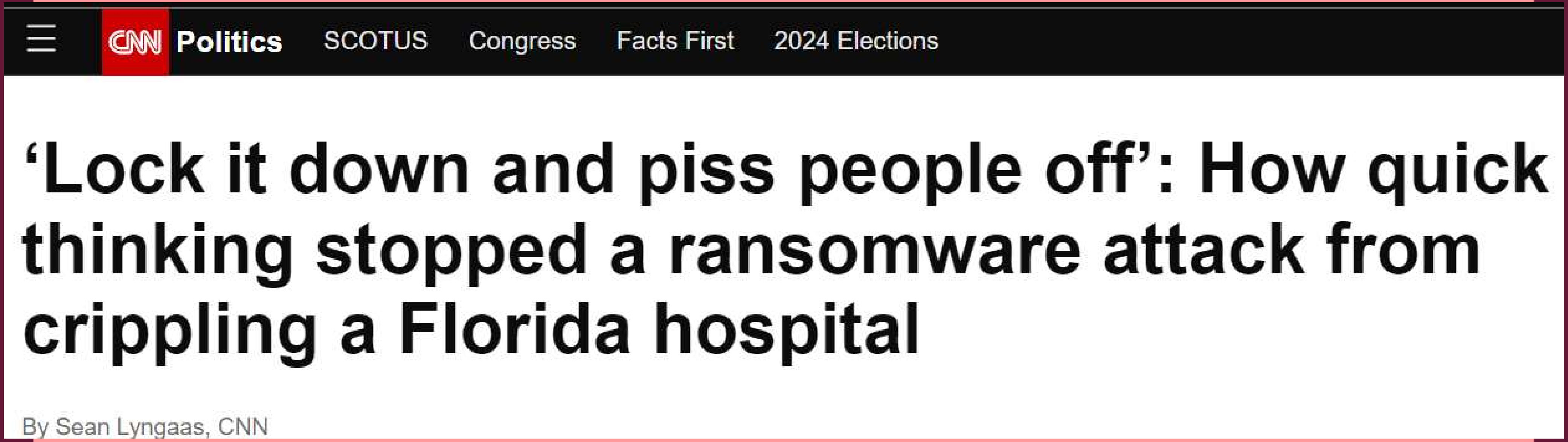
More than 1,000 executive leaders from the nation's top hospitals and health systems convened at the 2023 AHA Annual Membership Meeting, April 23-25 in Washington, D.C.

"What it comes down to is that cyber risk is business risk, and cyber-attacks on hospitals specifically, are really threats to life."

FBI Director Wray at the AHA Annual Conference - 4/25/2023

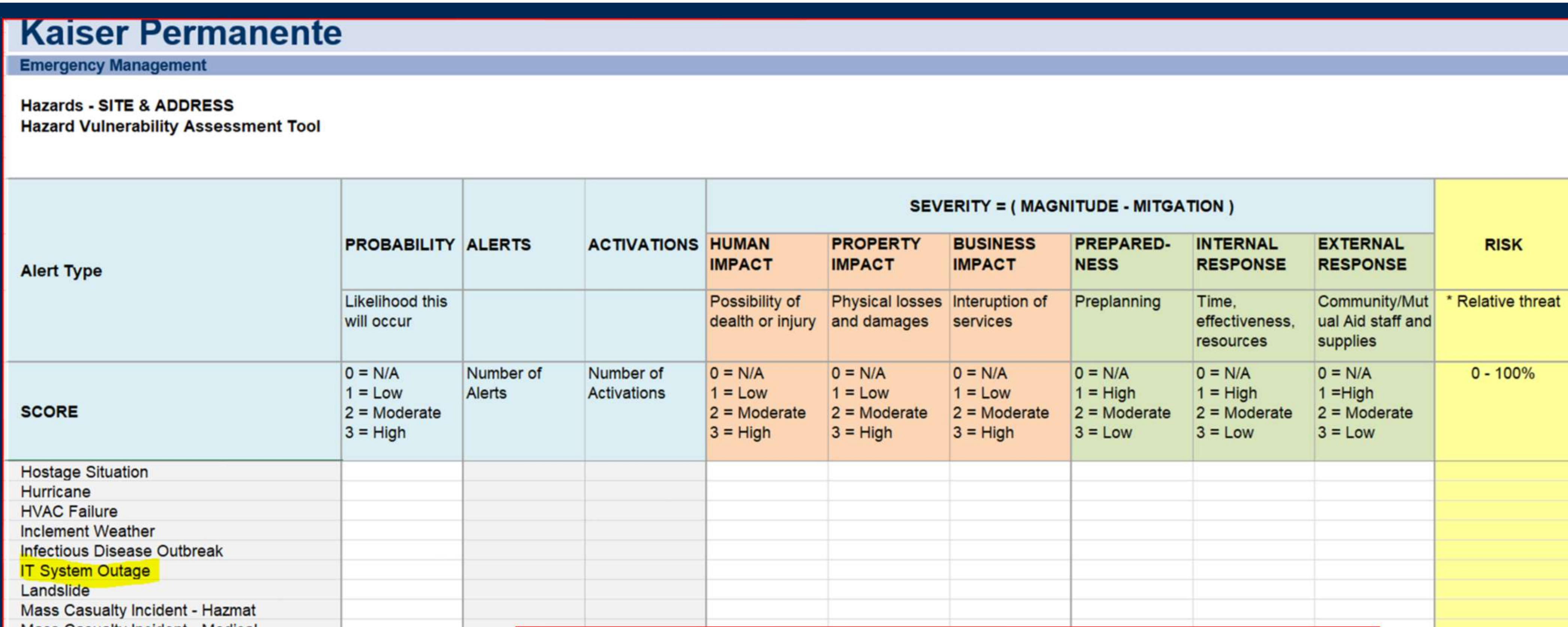
Summary of National Findings:

Hospital Ransomware Attacks and Exercises: Readiness, Response, Resiliency and Recovery



‘Lock it down and piss people off’: How quick thinking stopped a ransomware attack from crippling a Florida hospital

By Sean Lyngaas, CNN



Kaiser Permanente

Emergency Management

Hazards - SITE & ADDRESS
Hazard Vulnerability Assessment Tool

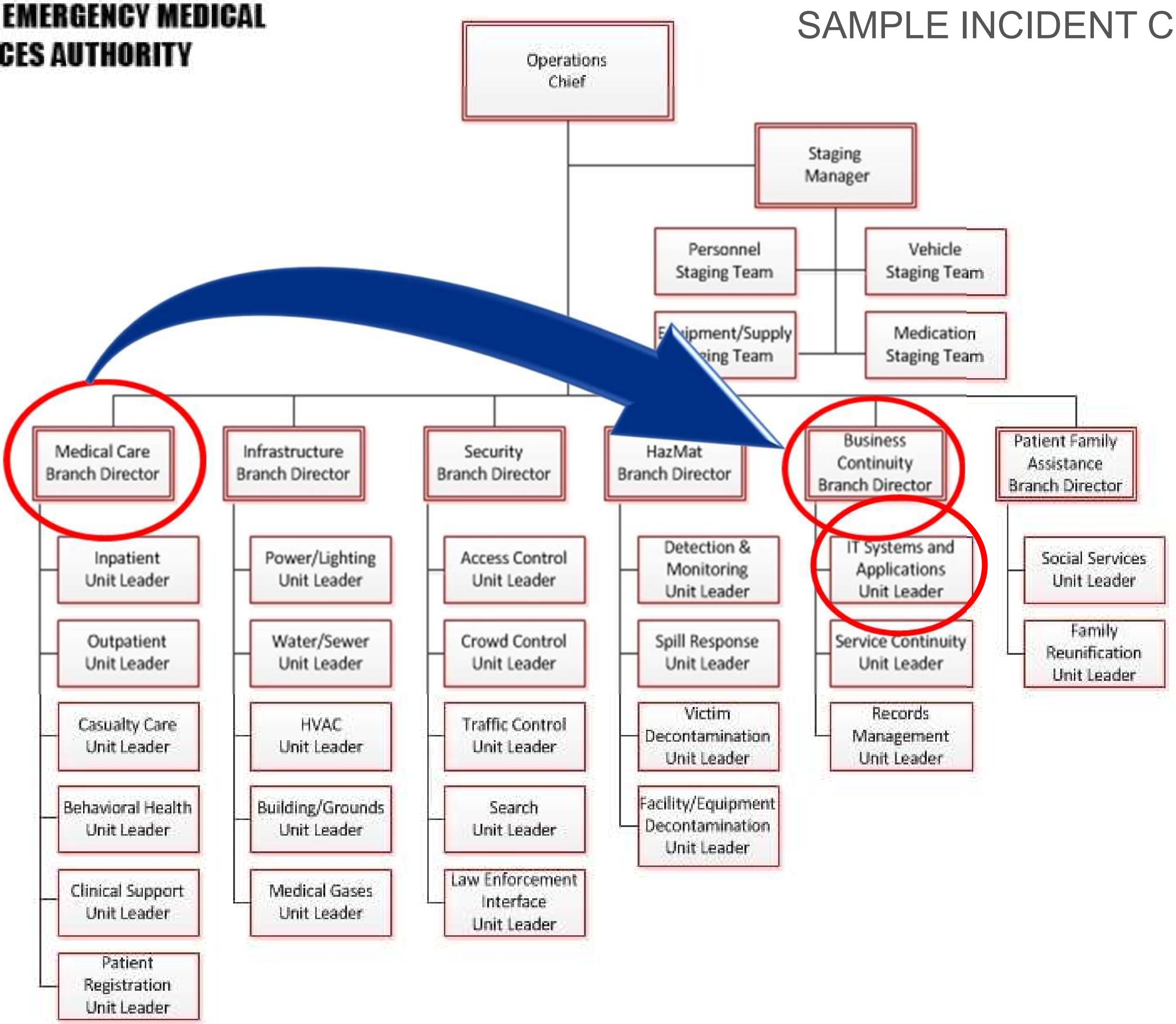
Alert Type				SEVERITY = (MAGNITUDE - MITGATION)						RISK
	PROBABILITY	ALERTS	ACTIVATIONS	HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	PREPARED-NESS	INTERNAL RESPONSE	EXTERNAL RESPONSE	
	Likelihood this will occur			Possibility of death or injury	Physical losses and damages	Interuption of services	Preplanning	Time, effectiveness, resources	Community/Mutual Aid staff and supplies	* Relative threat
SCORE	0 = N/A 1 = Low 2 = Moderate 3 = High	Number of Alerts	Number of Activations	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = Low 2 = Moderate 3 = High	0 = N/A 1 = High 2 = Moderate 3 = Low	0 = N/A 1 = High 2 = Moderate 3 = Low	0 = N/A 1 =High 2 = Moderate 3 = Low	0 - 100%
Hostage Situation										
Hurricane										
HVAC Failure										
Inclement Weather										
Infectious Disease Outbreak										
IT System Outage										
Landslide										
Mass Casualty Incident - Hazmat										
Mass Casualty Incident - Medical										
Mass Casualty Incident - Trauma										
Medical Gas Disruption										

CALIFORNIA EMERGENCY MEDICAL SERVICES AUTHORITY
Home
About ▾
Responders ▾
EMS Systems ▾
Disaster ▾
HOSPITAL INCIDENT COMMAND SYSTEM

Hospital Incident Command System – Welcome!

CALIFORNIA EMERGENCY MEDICAL SERVICES AUTHORITY

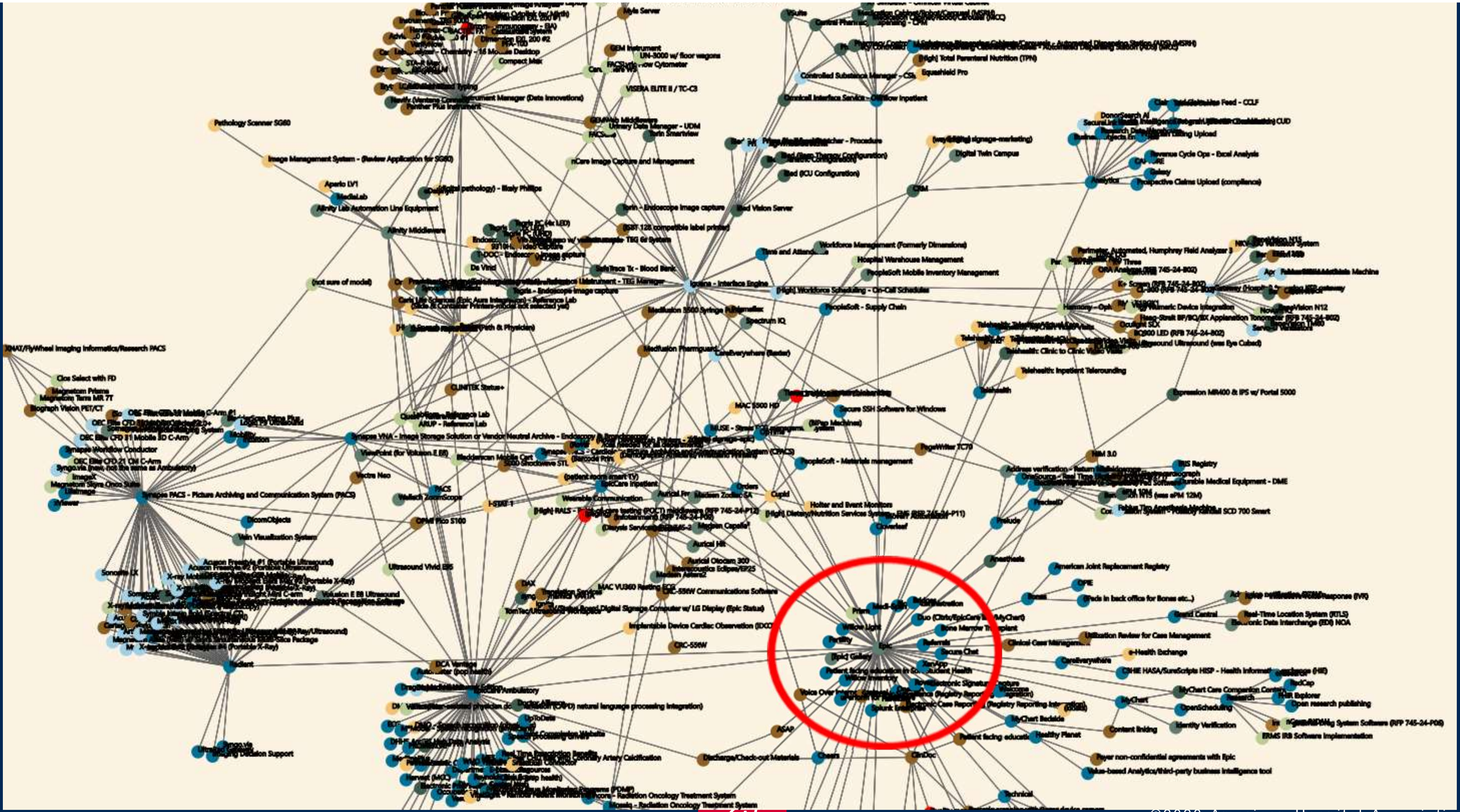
SAMPLE INCIDENT COMMAND CHART



- Operations Chief
  - Staging Manager
    - Personnel Staging Team
    - Vehicle Staging Team
    - Equipment/Supply Staging Team
    - Medication Staging Team
  - Medical Care Branch Director
    - Inpatient Unit Leader
    - Outpatient Unit Leader
    - Casualty Care Unit Leader
    - Behavioral Health Unit Leader
    - Clinical Support Unit Leader
    - Patient Registration Unit Leader
  - Infrastructure Branch Director
    - Power/Lighting Unit Leader
    - Water/Sewer Unit Leader
    - HVAC Unit Leader
    - Building/Grounds Unit Leader
    - Medical Gases Unit Leader
  - Security Branch Director
    - Access Control Unit Leader
    - Crowd Control Unit Leader
    - Traffic Control Unit Leader
    - Search Unit Leader
    - Law Enforcement Interface Unit Leader
  - HazMat Branch Director
    - Detection & Monitoring Unit Leader
    - Spill Response Unit Leader
    - Victim Decontamination Unit Leader
    - Facility/Equipment Decontamination Unit Leader
  - Business Continuity Branch Director
    - IT Systems and Applications Unit Leader
    - Service Continuity Unit Leader
    - Records Management Unit Leader
  - Patient Family Assistance Branch Director
    - Social Services Unit Leader
    - Family Reunification Unit Leader

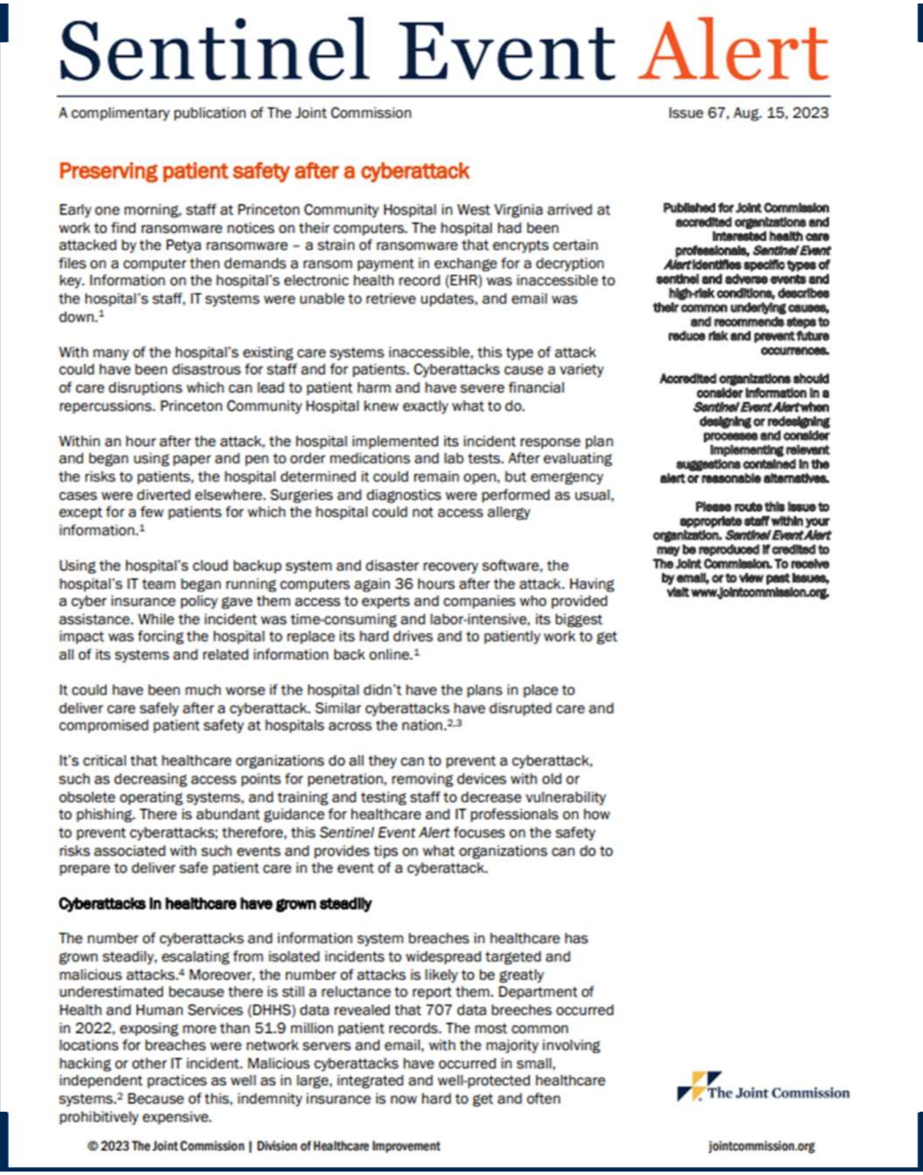
American Hospital Association™

Advancing Health in America


Myla Server
GEM Instrument
UN-3000 w/ floor wagons
VISERA ELITE II / TC-C3
Compact Max
Panther Plus Instrument
Pathology Scanner SG60
Image Management System - (Review Application for SG60)
Aperio LV1
MediaLab
Affinity Lab Automation Line Equipment
Affinity Middleware
Digital pathology) - likely Philips
Unity Data Manager - UDM
Storz Smartview
nCare Image Capture and Management
Storz - Endoscope image capture
Med Vision Server
BSST 128 compatible label printer
TEG 6s System
(not sure of model)
Storz - Endoscope image capture
XNAT/FlyWheel Imaging Informatics/Research PACS
Cios Select with FD
Magnetom Prisma
Magnetom Terra MR 7T
Biograph Vision PET/CT
OEC Elite CFD 31 Mobile 3D C-Arm
Synapse Workflow Conductor
OEC Elite CFD 21 CM C-Arm
Syngo.via (new, not the same as Ambulatory)
ImageX
Magnetom Sigma Onco Suite
Ultimage
Synapse PACS - Picture Archiving and Communication System (PACS)
Synapse VNA - Image Storage Solution or Vendor Neutral Archive - Endoscopy & Bronchoscopy
ViewPoint (for Voluson E 8S)
Vectra Neo
Welleh ZoomScope
DicomObjects
Vein Visualization System
Sonosite LX
Ultrasound Vivid E95
Voluson E 8S Ultrasound
Syngo.via
Imaging Decision Support
Acuson Freestyle #1 (Portable Ultrasound)
Cadent
CLINITEK Status+
ARUP - Reference Lab
Quest
Bladderscan Mobile Cart
5000 Shockwave STL
Epic Care Inpatient
Wearable Communication
(High) RALS
i-STAT 1
OPMI Pico S100
(Dialysis Services)
Madison Capella
Auricol Hit
Auricol Otoscan 300
Madison Astera
MAC VU360 Resting ECG
CIC-550W Communications Software
Implantable Device Cardiac Observation (IDCO)
CIC-550W
DAX
Iguana - Interface Engine
Medication 3500 Syringe Pump
Spectrum IQ
Medfusion Pharmguard
Careeverywhere (Roster)
MAC 5500 HD
Secure SSH Software for Windows
(BiPap Machines)
PageWriter TC70
PeopleSoft - Materials management
Orders
Cupid
Holter and Event Monitors
(High) Dietary/Nutrition Services System
Cadence
Time and Attendance
Workforce Management (Formerly Dimensions)
Hospital Warehouse Management
PeopleSoft Mobile Inventory Management
(High) Workforce Scheduling - On-Call Schedules
PeopleSoft - Supply Chain
Willow Inpatient
Clinical Interface Service
Controlled Substance Manager - CSM
Squashield Pro
(High) Total Parenteral Nutrition (TPN)
Central Pharmacy
VSuite
Bed (ICU Configuration)
Bed (Stem Therapy Configuration)
Digital Twin Campus
CRM
(way finding signage-marketing)
Analytics
Revenue Cycle Ops - Excel Analysis
Prospective Claims Upload (compliance)
DonorSearch AI
Perimeter, Automated, Humphrey Field Analyzer 3
ORA Analyzer (RFB 745-24-802)
Harmony - Ophthalmology
Ocuflight SDK
Numeric Device Integration
Slit Lamp
Telehealth: Clinic to Clinic Video Visits
Telehealth: Inpatient Telerounding
Telehealth
Expression MR400 & IPS w/ Portal 5000
NM 3.0
Address verification
DME
Prelude
PreciseID
Anesthesia
American Joint Replacement Registry
Epic
Bones
Grand Central
Real-Time Location System (RTLS)
Electronic Data Interchange (EDI) NOA
Utilization Review for Case Management
Clinical Case Management
e-Health Exchange
Careeverywhere
CSHIE HASA/SureScripts HISP - Health information exchange (HIE)
MyChart Care Companion
Research
MyChart
OpenScheduling
Identity Verification
Content linking
MyChart Bedside
Healthy Planet
Payer non-confidential agreements with Epic
Value-based Analytics/third-party business intelligence tool
REDCap
Open research publishing
ERMS IRB Software Implementation
Willow Light
Secure Chat
Bone Marrow Transplant
Duo (Citrix/EpicCare Link/MyChart)
Referrals
Voice Over Internet
Splunk
ClinDoc
Beacon
ASAP
Discharge/Check-out Materials
Cheers
Technical
Epic Ambulatory
Beaker
Dragon Medical One
UpToDate
Radiation Oncology Treatment System
Mosaiq - Radiation Oncology Treatment System

©2023 American Hospital Association

Software
Status)
on (IDCO)
Prism
Medi-Span
Bridges
Administration
Bones
Duo (Citrix/EpicCare link/MyChart)
Willow Light
Bone Marrow Transplant
Fertility
Epic
Referrals
Clinical Case
[Epic] Gallery
Secure Chat
XenApp
Patient facing education in Sc
Student Health
Willow Inventory
Electronic Signature Capture
Voice Over Internet
Welcome
(Registry Reporting
Electronic Case Reporting (Registry Reporting
Splunk Enterprise
MyChart Bed
ASAP
Patient facing educatio
ck-out Materials
Cheers
ClinDoc



Sentinel Event Alert

A complimentary publication of The Joint Commission

Issue 67, Aug. 15, 2023

Preserving patient safety after a cyberattack

Early one morning, staff at Princeton Community Hospital in West Virginia arrived at work to find ransomware notices on their computers. The hospital had been attacked by the Petya ransomware – a strain of ransomware that encrypts certain files on a computer then demands a ransom payment in exchange for a decryption key. Information on the hospital's electronic health record (EHR) was inaccessible to the hospital's staff, IT systems were unable to retrieve updates, and email was down.[1]

With many of the hospital's existing care systems inaccessible, this type of attack could have been disastrous for staff and for patients. Cyberattacks cause a variety of care disruptions which can lead to patient harm and have severe financial repercussions. Princeton Community Hospital knew exactly what to do.

Within an hour after the attack, the hospital implemented its incident response plan and began using paper and pen to order medications and lab tests. After evaluating the risks to patients, the hospital determined it could remain open, but emergency cases were diverted elsewhere. Surgeries and diagnostics were performed as usual, except for a few patients for which the hospital could not access allergy information.[1]

Using the hospital's cloud backup system and disaster recovery software, the hospital's IT team began running computers again 36 hours after the attack. Having a cyber insurance policy gave them access to experts and companies who provided assistance. While the incident was time-consuming and labor-intensive, its biggest impact was forcing the hospital to replace its hard drives and to patiently work to get all of its systems and related information back online.[1]

It could have been much worse if the hospital didn't have the plans in place to deliver care safely after a cyberattack. Similar cyberattacks have disrupted care and compromised patient safety at hospitals across the nation.[2,3]

It's critical that healthcare organizations do all they can to prevent a cyberattack, such as decreasing access points for penetration, removing devices with old or obsolete operating systems, and training and testing staff to decrease vulnerability to phishing. There is abundant guidance for healthcare and IT professionals on how to prevent cyberattacks; therefore, this *Sentinel Event Alert* focuses on the safety risks associated with such events and provides tips on what organizations can do to prepare to deliver safe patient care in the event of a cyberattack.

Cyberattacks in healthcare have grown steadily

The number of cyberattacks and information system breaches in healthcare has grown steadily, escalating from isolated incidents to widespread targeted and malicious attacks.[4] Moreover, the number of attacks is likely to be greatly underestimated because there is still a reluctance to report them. Department of Health and Human Services (DHHS) data revealed that 707 data breeches occurred in 2022, exposing more than 51.9 million patient records. The most common locations for breaches were network servers and email, with the majority involving hacking or other IT incident. Malicious cyberattacks have occurred in small, independent practices as well as in large, integrated and well-protected healthcare systems.[2] Because of this, indemnity insurance is now hard to get and often prohibitively expensive.

Published for Joint Commission accredited organizations and interested health care professionals, *Sentinel Event Alert* identifies specific types of sentinel and adverse events and high-risk conditions, describes their common underlying causes, and recommends steps to reduce risk and prevent future occurrences.

Accredited organizations should consider information in a *Sentinel Event Alert* when designing or redesigning processes and consider implementing relevant suggestions contained in the alert or reasonable alternatives.

Please route this issue to appropriate staff within your organization. *Sentinel Event Alert* may be reproduced if credited to The Joint Commission. To receive by email, or to view past issues, visit www.jointcommission.org.

The Joint Commission

jointcommission.org

"Organizations should be prepared to have life- and safety-critical technology offline **for four weeks or longer**.

These services include pharmacy (particularly medication order entry systems and medication reconciliation services); medical records; and laboratory, radiology and pathology, as well as other services required by a high volume of patients or patients of high acuity
(for example, blood bank, critical care units, intensive care units, infant security, nutrition services, and oncology and transplant)."

"The loss of clinical decision support during an EHR downtime clearly had an adverse impact on the patient"

Business Continuity is **not** the same as ***Clinical Continuity*** – Sample Areas to Develop Clinical Continuity Procedures

Administrative Support Team

Area	Operations Leader	Informatics Resource
Clinical Excellence		
Human Resources		
Legal		
Marketing & Communications		
Payroll		
Risk Management		
Information Technology		
Telecom		

Clinical Support Team

Area	Operations Leader	Informatics Resource	Physician
Biomedical			
Facilities, Safety & Security			
Health Information Management			
Supply Chain			

Physician Oversight Team

Area	Operations Leader	Informatics Resource
Inpatient Medical		
Medicine		
Medical Group & Ambulatory		

Clinical Care Team

Area	Operations Leader	Informatics Resource	Physician
Cardiology			
Care Management			
Clinical Education			
Food & Nutrition/Kitchen			
Home & Community			
Imaging			
Lab			
Nursing (see sub team)			
Patient Access			
Patient Scheduling			
Pharmacy			
Medical Group & Ambulatory			
Radiation Oncology			
Rehab Therapies			
Respiratory			

Ransomware Preparedness Considerations

- Some other real world urgent decisions and cascading "events" you will be faced with:

  - Downtime computers are encrypted – Now what?
  - Radiology, imaging downtime procedures? Stroke center impact?
  - Cath lab technology down – contingency plan/downtime procedures?
  - ED wait times soar at all your locations. Plan?
  - Outside physicians trying to contact your organization, requesting prescriptions, labs, records.
  - Elective surgeries and appointments – Cancel? How do you notify patients?
  - Radiation oncology down – contingency plan? Linear accelerators need internet connection to function.
  - Family members of patients can't get through on phones, showing up at hospital. Complaining to press.
  - What mission critical medical technology is on prem vs hosted in the cloud?
  - Alternate communications path to cloud hosted services? EMR?
  - How do you contact and reallocate personnel? Relief schedule? Runners?
  - Do you hold on outpatient radiology?
  - Where will you have your hospital based incident command center? How frequently will you communicate with senior leadership at all locations?
  - How do you print labels for patient wrist bands, charts, medications, IV bags etc?
  - Do you use new downtime MRNs and MARs?
  - How will you identify the ancillary/temp staff you need?
    - Runners to help with lab and pharmacy delivery
  - Home health care and home health care telemetry?
  - Pharmacy, dietary and drug cabinets?

Cyber Attack and TTX Findings, Recommendations and Observations

- **INTEGRATE PLANS:** Integrate and coordinate cyber incident response, emergency management, incident command, business continuity and disaster recovery plans. Business continuity plans should specify plans for ***clinical continuity and operational continuity*** *during a partial or full loss mission critical technology.*

- ***READINESS, RESPONSE, RESILIENCY AND RECOVERY (4R CONCEPT)*****:** The cyber incident response plan should be developed on an organization wide basis. All system level, hospital level and department level actions and responses, including all IT, operational, business and clinical functions, should be defined in the plan for the duration of the incident and for post incident recovery.

- ***REGIONAL, READINESS, RESPONSE, RESILIENCY AND RECOVERY (5R CONCEPT):*** It is recommended that **REGIONAL** cyber incident response and communication plans be developed for a high impact cyber attack having regional impact on healthcare delivery.. Leverage emergency preparedness plans and mutual aid agreements. Plans should consider contingencies to possibly accommodate **diversion of patients** and functions between facilities as needed and to **provide assistance to impacted facilities** with surge of personnel, communications, medical devices and technology. Regional facilities will also face increased strain or collateral impact.

- ***ENHANCE DOWNTIME PROCEDURES TO SUSTAIN OPERATIONS, WITHOUT TECHNOLOGY, FOR UP TO 4 WEEKS -*** for *every* **life critical, mission critical and business critical system and technology** – to sustain clinical and business operations for up to 4 weeks, without the benefit of technology. Enhance *clinical, operational, financial and administrative downtime processes and proficiency of staff* ***on all shifts*** *Ensure downtime supplies are in place or external printing arrangements have been made to continue operations and care delivery through manual procedures in the event of a simultaneous loss of all medical, information and operational technology.*

- **IDENTIFY CLINICAL AND MISSION CRITICAL THIRD PARTY SERVICES AND ESTABLISH DOWNTIME PROCEDURES IF THEIR SERVICES ARE UNAVAILABLE:** This includes cloud and technology service providers. Determine clinical, operational and information technology impact if they are struck with ransomware and their services become unavailable – establish compensating on-premises downtime procedures, including manual procedures and backup strategy.

- **DESIGNATE DOWNTIME COACHES AND DOWNTIME SAFETY OFFICERS FOR EACH SHIFT:** The loss of access to the EMR/EHR may cause disruption and delay to healthcare delivery as a significant proportion of staff may not be proficient in manual downtime procedures. Loss of embedded safety and treatment protocols in the EMR/EHR may increase risk to patient safety.

Cyber Attack and TTX Findings, Recommendations and Observations

- **NETWORK BACKUP STATUS, SEGMENTATION AND SECURITY**. Recommend regular cadence of vulnerability and penetration testing of backups. Review, document and communicate estimates of network restoration time objective and restoration point objective. Implement immutable backup solution as part of standard 3-2-1 backup strategy. 3-2-1**+1 immutable backup copy**

- ***DOCUMENT ROLES WHICH HAVE DESIGNATED AND DELEGATED AUTHORITIES*** to make independent, high impact decisions during a cyber incident/crisis such as disconnection of the organization from internet or shutting down of large parts of the network, under *defined* urgent circumstances. (**3D** concept –**D**ocument **D**esignate and **D**elegate authorities) Board notifications, authority and involvement?

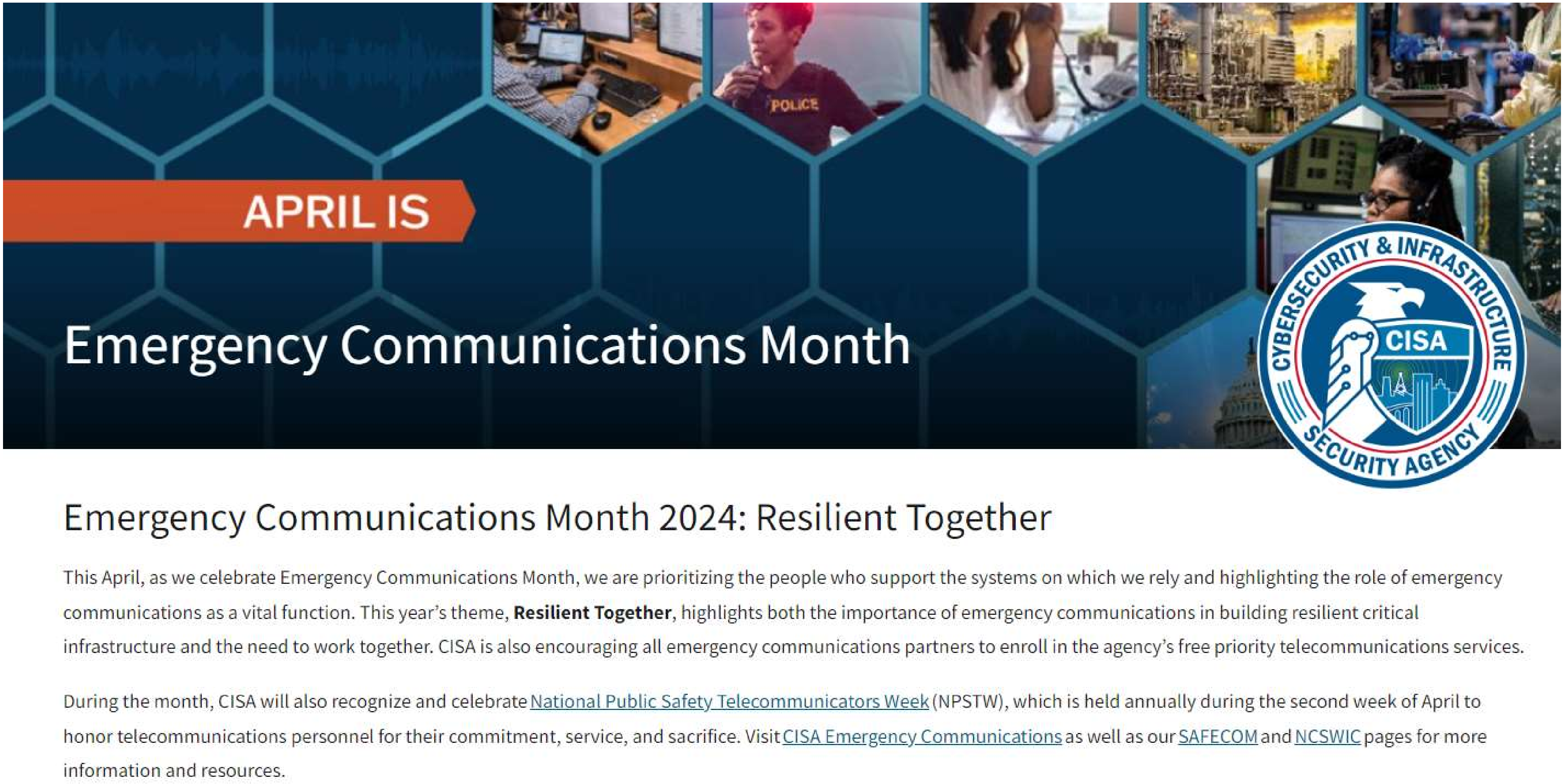
- **DEFFINE AND DOCUMENT "TRIGGERS"** or facts and circumstances authorizing high impact decisions, such as organizational disconnection from the internet. Specify leadership escalation, incident command activation and staff notification protocols. "Trigger" examples include indication that ransomware is spreading or beaconing to external "command and control" or indication of ongoing data exfiltration.

- ***DEFINE INTERNAL IMPACT TO LIFE CRITICAL, MISSION CRITICAL AND BUSINESS CRITICAL DEVICES AND SERVICES:*** Map clinical, operational and administrative impact of decisions related to complete or partial shut down of internal network or internet disconnection. Document impact and incorporate into overall incident response plan and communicated to leaders.

- **DEFINE EXTERNAL DEPENDENCIES IMPACT**, especially external clinical dependencies, which may be impacted or disrupted by a ransomware attack against your organization and unavailability of your network. Such as impact to other hospitals, clinics and homecare telemetry.

- **REVIEW CYBER INSURANCE COVERAGE:** Determine sufficiency of coverage based upon risk profile and current cybersecurity posture. Determine proficiency of incident response assets and your confidence in them prior to an incident. Review "act of war" exclusion given current geopolitical events. It is recommended that plan information be kept highly secured, encrypted with limited access to prevent adversary discovery.

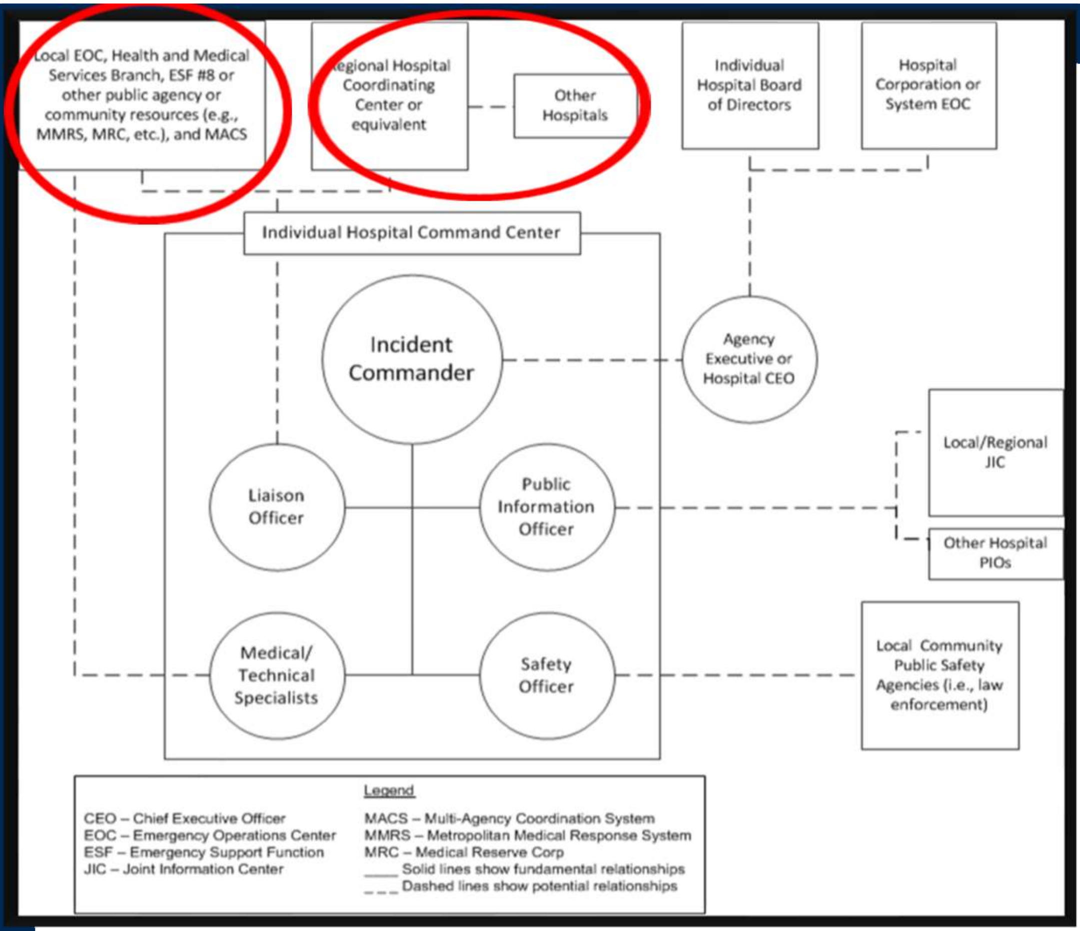
- **REVIEW BUSINESS ASSOCIATE AGREEMENT FOR BREACH NOTIFICATION AND INSURANCE REQUIREMENTS**: Determine to whom breach is to be reported 24/7 and timeline (24 – 72 hours for data theft, immediate for ransomware) including weekends and off hours. **Test!** Do cyber insurance requirements in BAAs scale with level of cyber risk presented by the individual business associate?


APRIL IS
Emergency Communications Month
POLICE
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Emergency Communications Month 2024: Resilient Together

This April, as we celebrate Emergency Communications Month, we are prioritizing the people who support the systems on which we rely and highlighting the role of emergency communications as a vital function. This year's theme, **Resilient Together**, highlights both the importance of emergency communications in building resilient critical infrastructure and the need to work together. CISA is also encouraging all emergency communications partners to enroll in the agency's free priority telecommunications services.

During the month, CISA will also recognize and celebrate National Public Safety Telecommunicators Week (NPSTW), which is held annually during the second week of April to honor telecommunications personnel for their commitment, service, and sacrifice. Visit CISA Emergency Communications as well as our SAFECOM and NCSWIC pages for more information and resources.



Local EOC, Health and Medical Services Branch, ESF #8 or other public agency or community resources (e.g., MMRS, MRC, etc.), and MACS

Regional Hospital Coordinating Center or equivalent

Other Hospitals

Individual Hospital Board of Directors

Hospital Corporation or System EOC

Individual Hospital Command Center

Incident Commander

Agency Executive or Hospital CEO

Local/Regional JIC

Other Hospital PIOs

Liaison Officer

Public Information Officer

Medical/ Technical Specialists

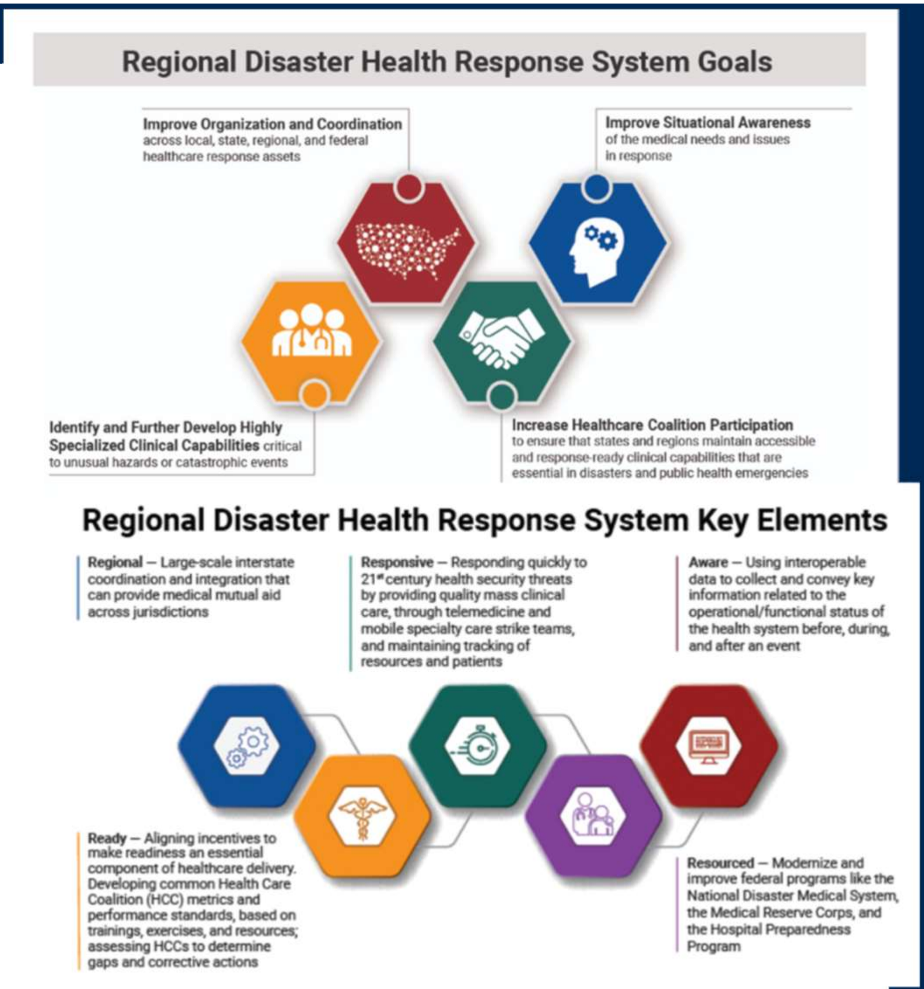
Safety Officer

Local Community Public Safety Agencies (i.e., law enforcement)

Legend

CEO – Chief Executive Officer
EOC – Emergency Operations Center
ESF – Emergency Support Function
JIC – Joint Information Center

MACS – Multi-Agency Coordination System
MMRS – Metropolitan Medical Response System
MRC – Medical Reserve Corp
____ Solid lines show fundamental relationships
_ _ _ Dashed lines show potential relationships



Regional Disaster Health Response System Goals

Improve Organization and Coordination across local, state, regional, and federal healthcare response assets

Improve Situational Awareness of the medical needs and issues in response

Identify and Further Develop Highly Specialized Clinical Capabilities critical to unusual hazards or catastrophic events

Increase Healthcare Coalition Participation to ensure that states and regions maintain accessible and response-ready clinical capabilities that are essential in disasters and public health emergencies

Regional Disaster Health Response System Key Elements

Regional – Large-scale interstate coordination and integration that can provide medical mutual aid across jurisdictions

Responsive – Responding quickly to 21st century health security threats by providing quality mass clinical care, through telemedicine and mobile specialty care strike teams, and maintaining tracking of resources and patients

Aware – Using interoperable data to collect and convey key information related to the operational/functional status of the health system before, during, and after an event

Ready – Aligning incentives to make readiness an essential component of healthcare delivery. Developing common Health Care Coalition (HCC) metrics and performance standards, based on trainings, exercises, and resources; assessing HCCs to determine gaps and corrective actions

Resourced – Modernize and improve federal programs like the National Disaster Medical System, the Medical Reserve Corps, and the Hospital Preparedness Program

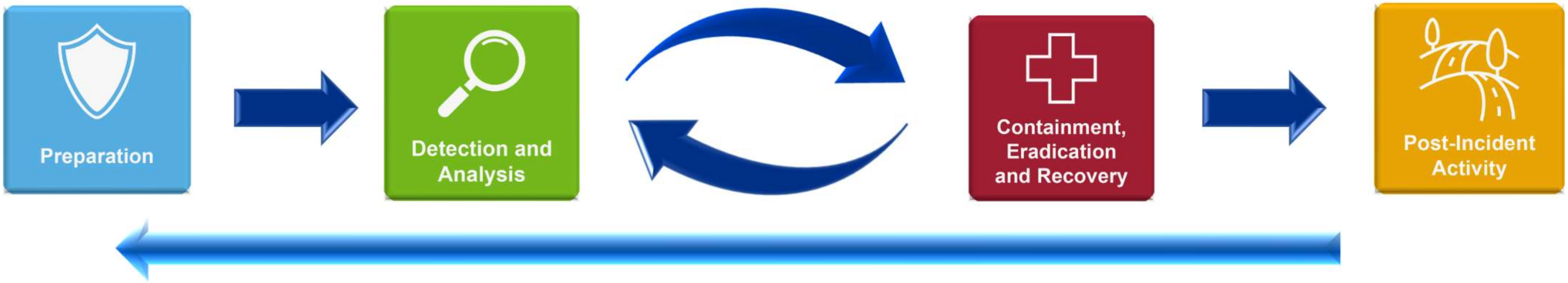
https://emsa.ca.gov/wp-content/uploads

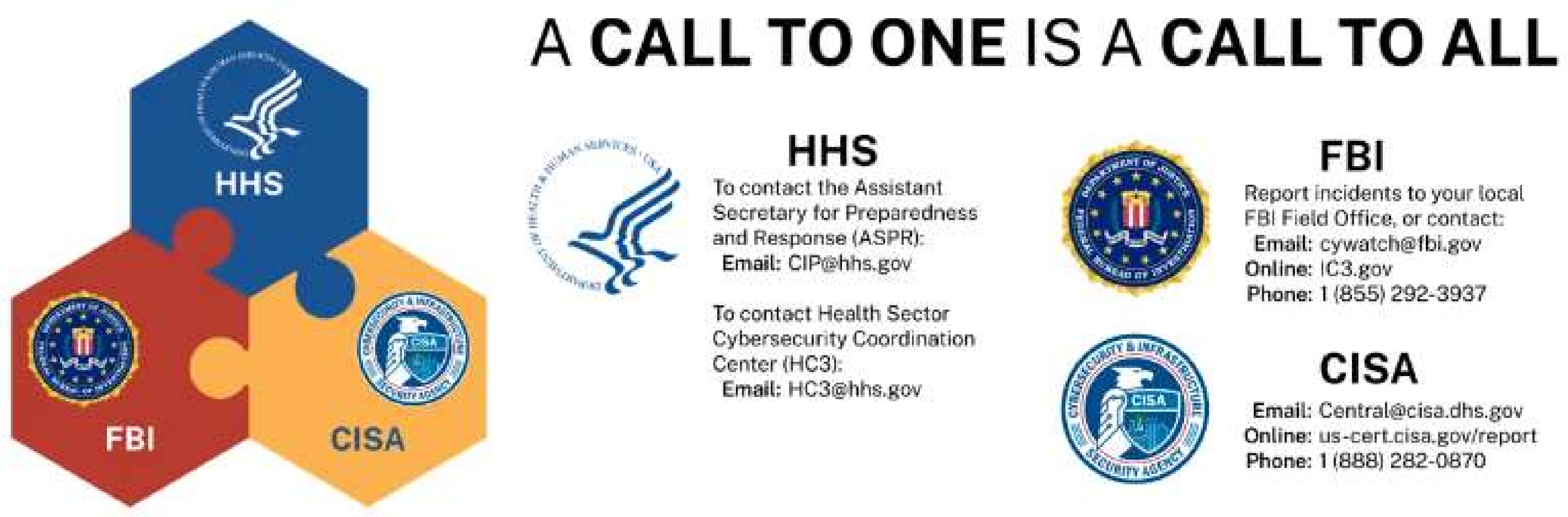
https://aspr.hhs.gov/RDHRS/Pages/rdhrs-overview.aspx

Overview and Objectives of the Exercise

- The goal of this strategic cyber and risk exercise is to engage organizational leadership in a critical thinking exercise and test preparedness, incident response plans and decision making processes in dealing with a major incident. ***The intent is to provoke discussion and thought on how clinical, technical, business and administrative functions of the organization react to the various facts of the incident, in a coordinated and effective response – to mitigate risk to the organization and to the patients.***

- The exercise will contain multiple, complex elements, derived from analysis of real world events. **Just as in a real world scenario, *participants will need to identify and make key decisions with limited information, under time constraints and adversarial conditions.*** There **are no absolute correct or incorrect responses.** We hope to learn as a group based upon our collective knowledge and experience.




HHS
FBI
CISA

A CALL TO ONE IS A CALL TO ALL

HHS

To contact the Assistant Secretary for Preparedness and Response (ASPR):
Email: CIP@hhs.gov

To contact Health Sector Cybersecurity Coordination Center (HC3):
Email: HC3@hhs.gov

FBI

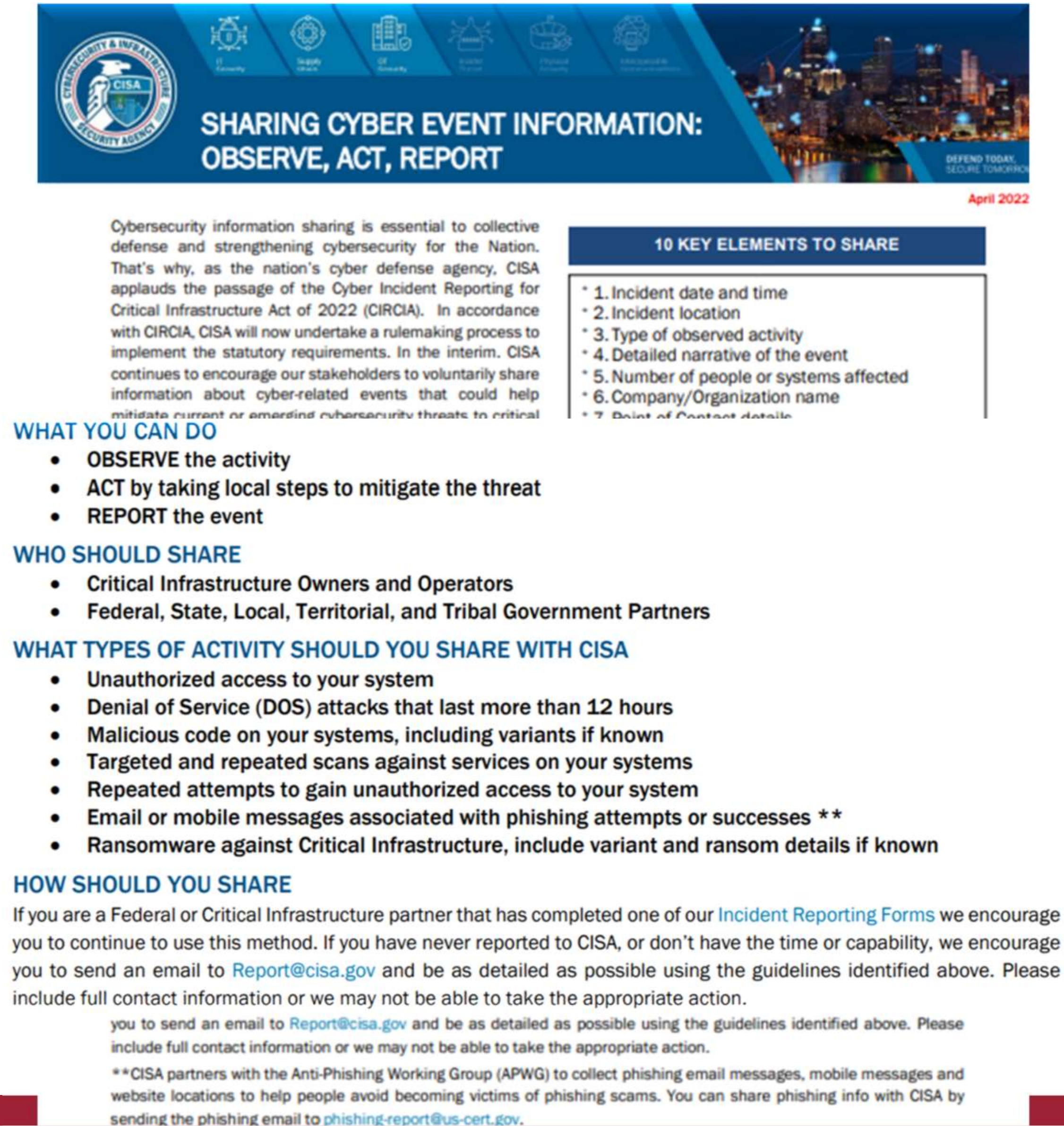
Report incidents to your local FBI Field Office, or contact:
Email: cywatch@fbi.gov
Online: IC3.gov
Phone: 1 (855) 292-3937

CISA

Email: Central@cisa.dhs.gov
Online: us-cert.cisa.gov/report
Phone: 1 (888) 282-0870

John Riggi, AHA National Advisor for Cybersecurity and Risk, jriggi@aha.org
(O) 202-626-2272

American Hospital Association™
Advancing Health in America



SHARING CYBER EVENT INFORMATION: OBSERVE, ACT, REPORT

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

April 2022

Cybersecurity information sharing is essential to collective defense and strengthening cybersecurity for the Nation. That's why, as the nation's cyber defense agency, CISA applauds the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). In accordance with CIRCIA, CISA will now undertake a rulemaking process to implement the statutory requirements. In the interim, CISA continues to encourage our stakeholders to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical

10 KEY ELEMENTS TO SHARE

* 1. Incident date and time
* 2. Incident location
* 3. Type of observed activity
* 4. Detailed narrative of the event
* 5. Number of people or systems affected
* 6. Company/Organization name
* 7. Point of Contact details

WHAT YOU CAN DO

- OBSERVE the activity
- ACT by taking local steps to mitigate the threat
- REPORT the event

WHO SHOULD SHARE

- Critical Infrastructure Owners and Operators
- Federal, State, Local, Territorial, and Tribal Government Partners

WHAT TYPES OF ACTIVITY SHOULD YOU SHARE WITH CISA

- Unauthorized access to your system
- Denial of Service (DOS) attacks that last more than 12 hours
- Malicious code on your systems, including variants if known
- Targeted and repeated scans against services on your systems
- Repeated attempts to gain unauthorized access to your system
- Email or mobile messages associated with phishing attempts or successes **
- Ransomware against Critical Infrastructure, include variant and ransom details if known

HOW SHOULD YOU SHARE

If you are a Federal or Critical Infrastructure partner that has completed one of our Incident Reporting Forms we encourage you to continue to use this method. If you have never reported to CISA, or don't have the time or capability, we encourage you to send an email to Report@cisa.gov and be as detailed as possible using the guidelines identified above. Please include full contact information or we may not be able to take the appropriate action.

you to send an email to Report@cisa.gov and be as detailed as possible using the guidelines identified above. Please include full contact information or we may not be able to take the appropriate action.

**CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages, mobile messages and website locations to help people avoid becoming victims of phishing scams. You can share phishing info with CISA by sending the phishing email to phishing-report@us-cert.gov.

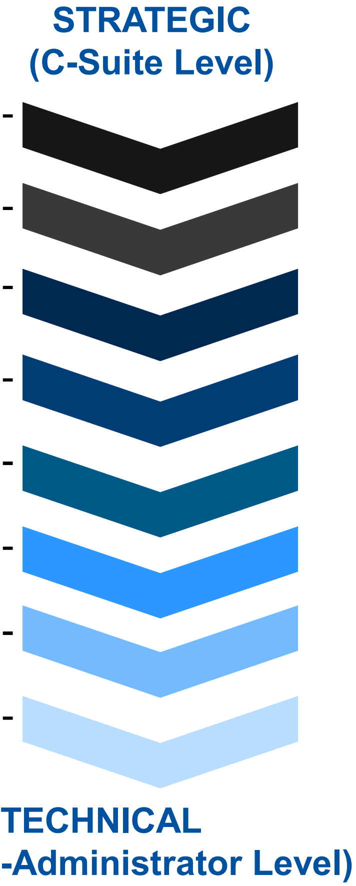
10 KEY ELEMENTS TO SHARE

* 1. Incident date and time
* 2. Incident location
* 3. Type of observed activity
* 4. Detailed narrative of the event
* 5. Number of people or systems affected
* 6. Company/Organization name
* 7. Point of Contact details
* 8. Severity of event
* 9. Critical Infrastructure Sector if known
10. Anyone else you informed

*Priority

CISA Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool (Strategic/Technical)
- Phishing Campaign Assessment (Technical)
- Vulnerability Scanning / Hygiene (Technical)
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)

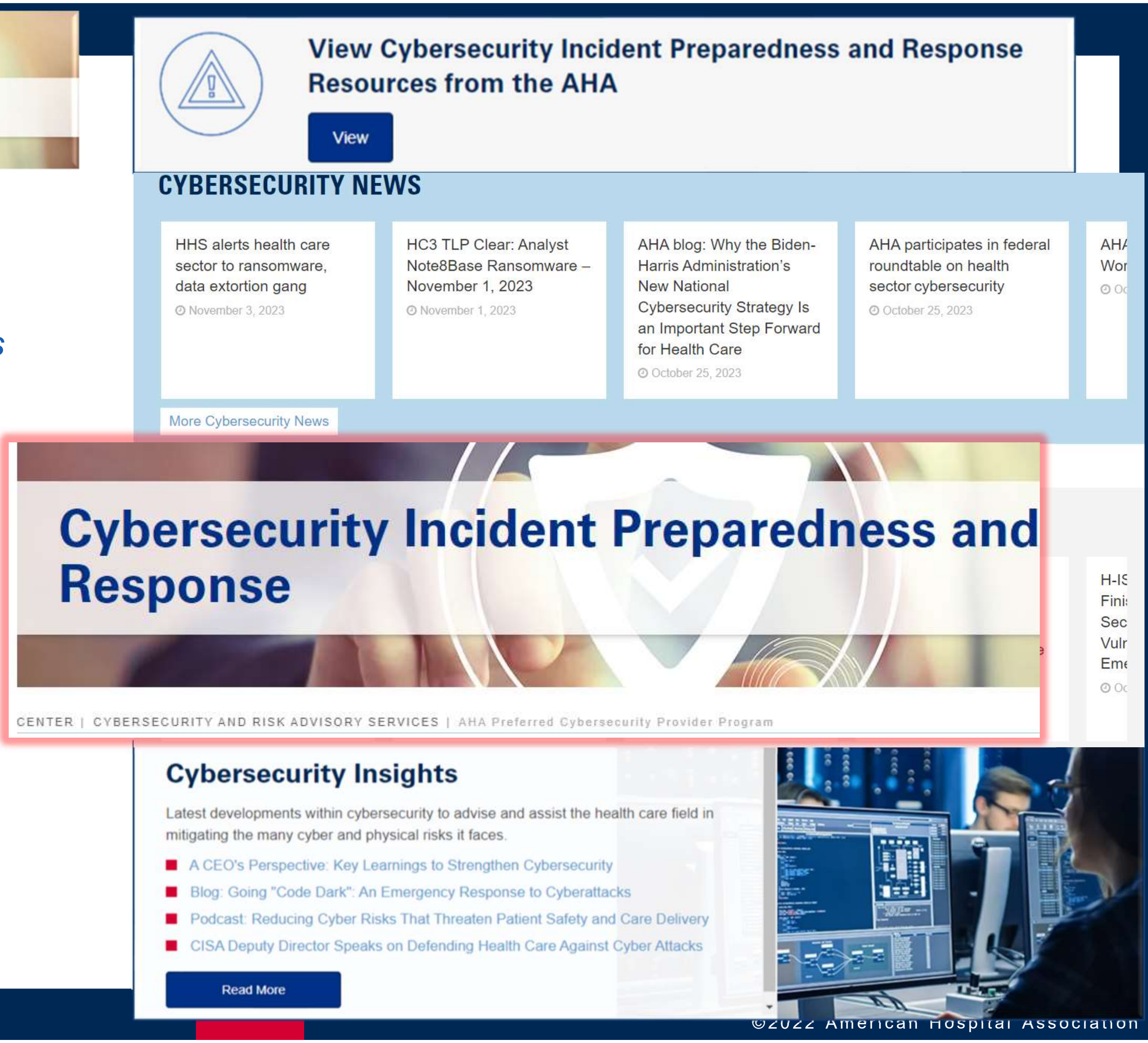


Cybersecurity & Risk Advisory

www.aha.org/cybersecurity

- *Cyber incident response resources*
- *Alerts from the FBI, NSA, CISA, HHS and FDA*
- *H-ISAC technical intelligence*
- *Podcasts with members and government officials*
- *Guidance and commentary from John Riggi, AHA National Advisor for Cybersecurity and Risk*

H-ISAC
HEALTH - ISAC



View Cybersecurity Incident Preparedness and Response Resources from the AHA

CYBERSECURITY NEWS

HHS alerts health care sector to ransomware, data extortion gang
November 3, 2023

HC3 TLP Clear: Analyst Note8Base Ransomware – November 1, 2023
November 1, 2023

AHA blog: Why the Biden-Harris Administration's New National Cybersecurity Strategy Is an Important Step Forward for Health Care
October 25, 2023

AHA participates in federal roundtable on health sector cybersecurity
October 25, 2023

AHA
Wor
Oc

Cybersecurity Incident Preparedness and Response

CENTER | CYBERSECURITY AND RISK ADVISORY SERVICES | AHA Preferred Cybersecurity Provider Program

H-IS
Fini
Sec
Vulr
Eme
Oc

Cybersecurity Insights

Latest developments within cybersecurity to advise and assist the health care field in mitigating the many cyber and physical risks it faces.

- A CEO's Perspective: Key Learnings to Strengthen Cybersecurity
- Blog: Going "Code Dark": An Emergency Response to Cyberattacks
- Podcast: Reducing Cyber Risks That Threaten Patient Safety and Care Delivery
- CISA Deputy Director Speaks on Defending Health Care Against Cyber Attacks

MIAMI-DADE COUNTY
HEALTHCARE PREPAREDNESS
COALITION
EMERGENCY
PREPAREDNESS

AMERICAN HOSPITAL ASSOCIATION
NISI DOMINUS FRUSTRA
FOUNDED 1898

Questions and Discussion

What will you change??

John Riggi
jriggi@aha.org
202-626-2272