



OeHI

Office of eHealth Innovation

eHealth Commission Meeting

HYBRID CONFERENCE

April 16, 2025

April Agenda



OeHI

Office of eHealth Innovation

| Title | Start | Duration |
|--|-------|----------|
| Call to Order <ul style="list-style-type: none">• Roll Call and Introductions• Approval of March Meeting Minutes• April Agenda and Objectives <i>Kaakpema “KP” Yelapaala, Chair</i> | 12:00 | 5 mins |
| Announcements <ul style="list-style-type: none">• Welcoming Remarks• OeHI Updates-eHealth Commission Updates• Decision Items & Action Items <i>Dianne Primavera, Lt. Governor and Director of the Office of Saving People Money on Health Care</i> <i>Stephanie Pugliese, Director, Office of eHealth Innovation (OeHI)</i> <i>All Commissioners and Advisors</i> | 12:05 | 5 mins |
| Current & Emerging Threats in the Health Sector and Staying Safe Online <i>Errol Weis, Chief Security Officer, Health Information Sharing and Analysis Center</i> | 12:10 | 1 hour |
| Public Comment Period | 1:10 | 5 mins |
| Closing Items <ul style="list-style-type: none">• Closing Remarks• Open Discussion• Recap Action Items• Adjourn Public Meeting <i>Kaakpema “KP” Yelapaala, Chair</i> | 1:15 | 5 mins |

OeHI and eHealth Commission Updates



Health-ISAC™

Collaborating for Resilience in Healthcare



Current & Emerging Threats in the Health Sector and Staying Safe Online

Errol Weiss

Chief Security Officer, Health-ISAC

April 2025



Learning Objectives

At the completion of this educational activity, the learner will be able to:

- Describe the **top cyber threats** facing the healthcare sector
- Use the information to **influence cybersecurity budget** and investment decisions
- Leverage practical steps and resources to **improve your own cyber security** posture

4,670



What is an ISAC?

- ISAC is short for “Information Sharing and Analysis Center”
- ISACs empower sharing and collaboration in critical infrastructure communities to prevent, detect and respond to cybersecurity and physical security events
- ISACs collect, analyze, and disseminate actionable threat information to their members and provide them with tools to mitigate risks and enhance resiliency



About Health-ISAC

- Community of over 12,000 Global Security Analysts, built on **trust** and **anonymity**
- Members must be in the health sector and interested in providing value to the overall Health-ISAC eco-system by listening, sharing, and/or contributing
- Benefits



Community

Events



Education



Threat Intelligence

Co









munity Services



Cybersecurity Automation

The Cyber Threat Spectrum

| | HACKTIVISM | CRIME | INSIDER | ESPIONAGE | TERRORISM | WARFARE |
|------------|--|--|--|--|---|--|
| THREATS |  |  |  |  |  |  |
| MOTIVATION | Hacktivists use computer network exploitation to advance their political or social causes. | Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain. | Trusted insiders steal proprietary information for personal, financial, and ideological reasons. | Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies. | Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid. | Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict. |

Source: FBI Cyber Division

Survey Results: Greatest Threats to Health Sector

Top Five Cyber Threats facing organizations in 2024:

1. Ransomware
2. Phishing/Spear Phishing
3. Compromised Credentials
4. Third Party/Partner Breaches
5. Data Breaches

Survey of 200+ healthcare Information Technology and security professionals

- Health-ISAC
- American College of Clinical Engineering (ACCE)
- Association for the Advancement of Medical Instrumentation (AAMI)

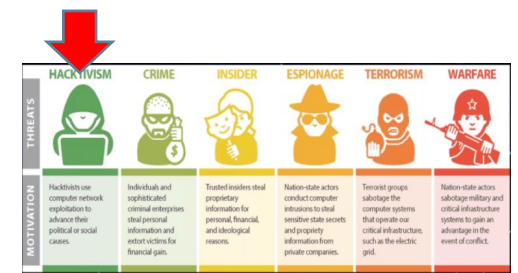
Key Takeaway

- Health sector organizations, regardless of budget, are most concerned about ransomware attacks

Current Threat Landscape



Hacktivism



- Hacktivists use computer network exploitation to advance their political or social causes
- Examples
 - Anonymous support for **Occupy Wall Street** (2011)
 - **Panama Papers** – 11 million financial and legal records exposed corruption and secretive offshore companies (2016)
 - Revealed offshore holdings of 140 politicians and public officials around the world
 - More than 214,000 offshore entities connected to people in more than 200 countries
 - Hacktivist collective **Anonymous** took actions to support Black Lives Matter (BlueLeaks 2020)



Hacktivism: Healthcare Sector Targets



Hacktivism: Healthcare Sector Targets

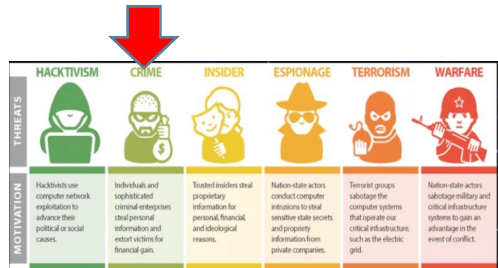
Who is being targeted?

- Healthcare Providers
 - Gender reassignment surgery
 - Family planning and reproductive health / Abortions
 - COVID Vaccines
- Healthcare Insurers
 - Payers of services above

What are the risks?

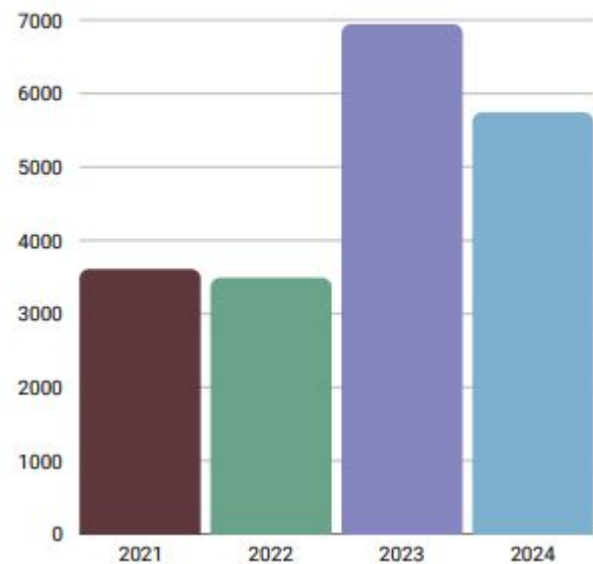
- Exposure of sensitive Patient Health Information (PHI)
- Dis- / Mis-information campaigns
- Doxing targeted individuals
- In extreme cases, transcends to physical attacks

Cybercriminal Activity: Ransomware



- Health-ISAC tracking over 21,000 ransomware cases since 2020
 - In 2024: 5,744 events across all sectors
 - 476 ransomware incidents involving the healthcare sector (**8.3%**)
 - 2020 to 2024: 21,556 events across all sectors
 - 1,367 ransomware incidents involving healthcare sector (**6.3%**)

Total Breaches Tracked: 21,556



Top 5 Ransomware Actors Targeting Health Sector

1. Lockbit
2. INC Ransomware
3. Ransom Hub
4. BianLian
5. QiLin



Source: Health-ISAC Healthcare Heartbeat Q4 2024
<https://health-isac.org/healthcare-heartbeat-2024-q4/>

Ransomware Impacts on Healthcare

- Ambulances forced to divert
- Disrupted delivery of treatments
- Canceled elective procedures
- Delayed laboratory results
- Delays in scheduling appointments
- Downtime for Electronic Health Records management systems
- Patient records unavailable
- Leaked sensitive patient data
- Surrounding area hospitals overwhelmed

CHANGE
HEALTHCARE

 Ascension

Change Healthcare Incident – Feb 2024

Root cause – lack of multifactor authentication on remote access servers

Patient Impacts

- Cancelled procedures
- Unable to fill prescriptions

Health Delivery Impacts

- Revenue losses
- Insurance payments interruptions, negative cash flow impact

Health-ISAC Recommendations

- Identify and analyze health sector systemic risks
- Determine key supplier and sector concentration risks
- Discern lessons learned and update Incident Response Plans
- Hold industry exercises to identify single points of failure and communication gaps

<https://h-isac.org/health-isacs-response-to-the-change-healthcare-incident-and-recommendations-for-action/>

Ascension Incident – May 8, 2024



Patient Impacts

- Patient Diversions
- Delayed tests, imaging, lab results
- Cancelled procedures

Health Delivery Impacts

- Servers encrypted
- Data exfiltrated
- Backups compromised

Health-ISAC Response

- Received IOCs on May 9; shared with members at TLP:AMBER
- May 10 Released Black Basta Threat Advisory TLP:WHITE, updated with TLP:WHITE info from CISA CSA
- May 11 - Ascension's statement updated sharing threat intelligence with Health-ISAC to help protect the community



Cybercriminal Activity: Ransomware Update

1

Encrypt your data and pay ransom to get decryption key



2

Steal your data and threaten to release it publicly unless you pay the ransom



3

Launch a Distributed Denial of Service (DDoS) at your website, rendering it useless, until you pay the ransom



When Cybercriminals Turn to Blackmailing Patients

- Evolution of ransomware extortion
- Alternative means of monetization
- Cases:
 - Vastaamo Psychotherapy Center– Finland
 - Fred Hutchinson Cancer Center – US
 - The Center for Facial Restoration – US
 - Multiple Plastic Surgery Practices in 2023 – US
- Cases targeting individuals may increase
 - Legislation prohibiting companies paying ransoms
 - More groups and individuals linked to cybercrime added to Sanctions Lists

Hacker seeks to extort Finnish mental health patients after data breach

Tens of thousands of patients concerned by massive hack.



NEWS 18 OCT 2023

FBI: Hackers Are Extorting Plastic Surgery Patients

James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Cybercriminals are harvesting sensitive personally identifiable information (PII) and medical records from plastic surgery offices to extort doctors and patients, the FBI has revealed.

The public service announcement issued on October 17, 2023, warned that once harvested, attackers demand a ransom from plastic surgeons and patients to prevent sharing this data, which often includes sensitive photographs.

How the Attackers Operate

The FBI highlighted the three-stage approach cybercriminals are using to launch these scams:

ADVERTISEMENT

ADVERTISING HERE

Hackers Demand Ransom From Patients After Breaching Florida Clinic

Hackers are demanding patients of Florida provider Richard Davis, MD pay a ransom to prevent the release of their personal information following a breach of the clinic's server.



SEATTLE CANCER PATIENTS FACE BLACKMAIL THREATS AFTER RECENT FRED HUTCH DATA BREACH

BY KIRO 1 DECEMBER 08, 2023



As if battling cancer isn't hard enough, now patients at UW's Fred Hutchinson Cancer Center are being extorted. Last month, the Cancer Center experienced a data breach, exposing data for an unknown number of patients. Some of those patients are getting emails threatening to leak their personal information if they don't pay up.

[FULL STORY](#)

RECOMMENDED FOR YOU

[Scripps-Affiliated Docs Pay \\$6.8M to Settle Age Bias Suit](#)

[Power your Revenue Cycle with Automation and AI](#)

[DOJ slaps False Claims Act suit against Steward Healthcare, St. Elizabeth's MC](#)

[For parents of babies in Aurora](#)

When Cybercriminals Turn to Blackmailing Patients

Vastaamo Psychotherapy Center– Finland

- Sept / Oct 2020
- 30,000 patient records leaked
- Aleksanteri Kivimäki, 26 years old
- History of cybercrime, cyber-stalking and cyber-harassment starting as a teen
- Trial ended March 8, 2024
- Found Guilty on April 30, 2024; sentenced to 6 years in prison

•Source:

<https://www.bloomberg.com/news/features/2024-04-22/a-massive-therapy-hack-shows-just-how-unsafe-patients-files-can-be>



Bloomberg

Businessweek | Feature

How a Massive Hack of Psychotherapy Records Revealed a Nation's Secrets

Aleksanteri Kivimäki was a hacker wunderkind with a mean streak. Now he's on trial for the largest crime in Finland's history.



Lehigh Valley Health Network Incident – Jan 2023

Health Delivery Impacts

- BlackCat Ransomware
- LVHN refused to pay ransom

Patient Impacts

- Clinical photos posted online
- Breached sensitive Protected Health Information (PHI)
 - 135,000 patients and employees impacted
 - Personal information, medical record numbers, treatment and diagnosis information and health insurance information

Class Action Settlement

- LVHN agreed to a \$65 million settlement (Nov 2024)
- Some class members will receive up to \$70,000



Russian Ransomware Gangs Disrupt Patient Care

April 2024 - Octapharma

- Blood plasma provider, outage closed over 190 donation centers in 35 states
- BlackSuit Ransomware Gang
- Octapharma supplied 75% of plasma therapies

June 2024 - Synnovis

- Lab services provider in UK, 800 operations delayed, 700 outpatient appointments rescheduled
- QiLin Ransomware Gang
- 900,000 Patient Records Exposed

July 2024 - OneBlood

- Blood supplier for hospitals in Florida and neighboring states
- Ransom Hub Ransomware-as-a-Service



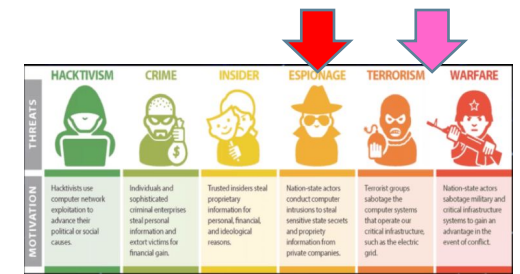
Observations

- Three critical third-party supply chain attacks in three months
- Russian ransomware cybercriminal gangs
- Operational impacts over a large geographic area

Recommendations

- Supply chain risk management
 - Health Industry Cybersecurity Supply Chain Risk Management Guide ([HIC SCRiM](#))
- Alternative suppliers
- See [American Hospital Association and Health-ISAC Joint Threat Bulletin](#)

Notable Nation-State Activity



- **Russia**

- APT 29 WINELOADER Campaign
 - Cross sector attacks including healthcare and pharmaceuticals, in the United States and Europe using WINELOADER malware; also targeted European diplomats, German political parties

- **China**

- UTA 0178 Exploitation of Ivanti Vulnerabilities
 - Remote VPN exploitation for espionage and theft of intellectual property

- **North Korea**

- Remote IT Worker Fraud
 - North Korean campaign to obtain remote jobs in NATO countries and extort them for money following employment

Why??

Provide strategic advantages in healthcare, biotechnology, and national security.

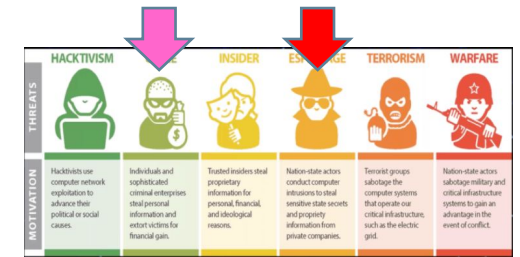
- Pharmaceutical and Biotechnology R&D
- Medical Device Technology
- Genomic Research
- Artificial Intelligence in Healthcare
- Infectious Disease Research

Notable Nation – North Korea

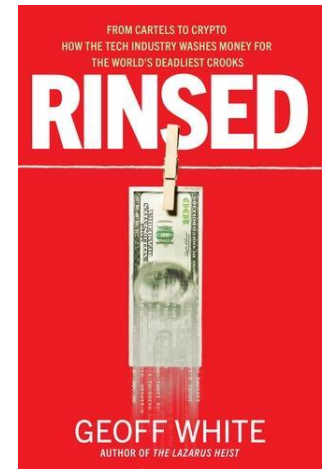
- Financially motivated and used to generate revenue for state and military objectives
- Espionage
- Ransomware
- Cryptocurrency Theft
 - Bybit Hack - \$1.46 billion (Feb 2025)
 - Axie Infinity and Tornado Cash -- \$625 million heist (March 2022)



<https://www.bbc.co.uk/programmes/w13xtvg9/episodes/downloads>



<https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-a-digital-military-machine>



<https://geoffwhite.tech/>

Geopolitical Activity

- Russia/Ukraine War Escalation
- Threats to EU Infrastructure
- Middle East Escalation



Potential Terror Threat Targeted at Health Sector – AHA & Health-ISAC Joint Threat Bulletin

March 20, 2025

#AHA #American Hospital Association #Terrorism #Threat Intelligence

The American Hospital Association (AHA) and Health-ISAC observed a social media post related to the active planning of a coordinated, multi-city terrorist attack on hospitals in the coming weeks.

THREAT BULLETIN

Potential Terror Threat Targeted at Health Sector – AHA & Health-ISAC Joint Threat Bulletin

On March 18, 2025, the American Hospital Association (AHA) and Health-ISAC observed a social media post related to the active planning of a coordinated, multi-city terrorist attack on hospitals in the coming weeks.

The AHA and Health-ISAC have reviewed and are sharing this bulletin and all associated information to support the response of the health sector. The AHA and Health-ISAC will continue to monitor the situation and will provide additional information as it becomes available.







All information is provided to other stakeholders in accordance with the Health-ISAC Policy. Security, Privacy, and Compliance.

Update:

On March 26, 2025, the FBI advised that, after extensive investigation and intelligence review, they have not identified any specific credible threat targeted against hospitals in any U.S. city. The FBI advised if they receive credible threat information, they will immediately advise any identified potential targets and, if appropriate, alert the broader health sector through the AHA, Health-ISAC and other appropriate channels.

KillNet DDoS / (Jan 2023)

Distributed Denial-of-Service Attacks

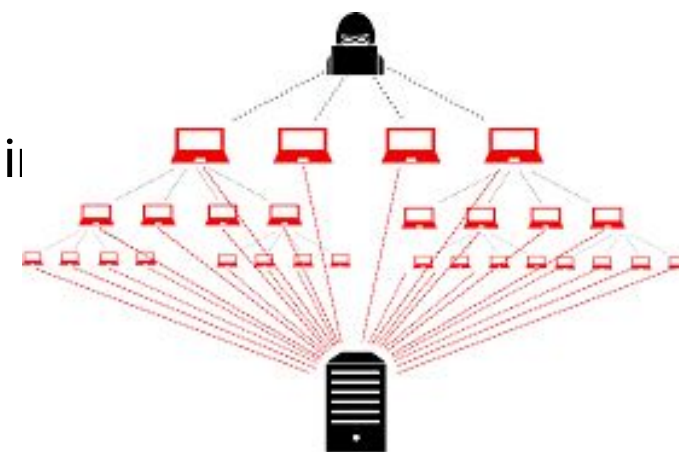
| | HACKTIVISM | CRIME | INSIDER | ESPIONAGE | TERRORISM | WARFARE |
|------------|--|--|--|--|---|--|
| THREATS |  |  |  |  |  |  |
| MOTIVATION | Hacktivists use computer network exploitation to advance their political or social causes. | Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain. | Trusted insiders steal proprietary information for personal, financial, and ideological reasons. | Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies. | Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid. | Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict. |

Who are they?

- Hacktivist Group targeting critical infrastructure globally including hospitals
- Ties to Russian Intelligence (GRU)
- Ties to Anonymous
- Ties to Anonymous Sudan
- Ties to Anonymous Russia

How to protect against their attacks?

- DDoS mitigation services
- Targeted Alerts
- Health-ISAC Information on DDoS, including mitigation strategies




Recent Cyber Threats to Healthcare



Notable Tactics Targeting the Health Sector

- Help Desk Targeting
 - Threat actors targeting help desk staff
- Telephone-Oriented Attack Delivery (TOAD) Campaigns
 - Malicious emails targeting health sector organizations
- Email Spam Bomb Campaigns
 - Victims added spam lists, then malicious actors pose as tech support to fix the problem, leading to malware delivery

Call Back Scam or “Telephone-Oriented Attack Delivery (TOAD)”



815 West Market Street
Louisville KY 407087

INVOICE/2024/41580/PEVO4

Balance

Helpline:- +1 (848) 229

Dear Subscriber,

Your Account has been charged with **\$349.99** and will be going to deduct from your account within 24 hours. If you did not recognize this transaction or want to cancel please reach our Customer Help Center: **+1 (801) 938-7004**

Billed To :

Customer Id Number : 43578456
Invoice Number : 3245673
Renewal Date : 7th March,2024


| Product Name | Product Amount | Product Code | Order ID |
|-------------------|----------------|--------------|----------|
| Norton Anti-virus | \$349.99 | 23456734 | 23456734 |


you didn't authorize this charge, You have 24 Hrs. To cancel & get an instant refund of your annual membership, Please contact our customer care: **+1 (801) 938-7004**

Please do not reply to this email. This mailbox is not monitored, And you will not receive response.

Digitally Yours ,

Customer Support : **+1 (801) 938-7004**





McAfee

2024-03-01
EIFFJDQ97YTWDOY2Y5U1

Customer Care Support
+1 (803) 336-4822

Dear errolw65@gmail.com,

choice of McAfee for your security needs. This email is your detailed invoice for your recent purchase. Your McAfee account has been automatically ensuring uninterrupted online protection with a seamless annual subscription

EIFFJDQ97YTWDOY2Y5U1

McAfee Total Security Protection
H9NRSTTK20J4TTOM/ymqj04bm6c1vav
2024-03-01


\$349.95

| Description | Amount |
|----------------------------------|----------|
| McAfee Total Security Protection | \$349.95 |
| TOTAL | \$349.95 |

Thank You
Regards
Team McAfee

received in your spam box, ask the service desk to verify the Invoice Number.

Copyright © McAfee, All Right Reserved, McAfee LLC.




Transaction Confirmation - Mozilla Thunderbird

Subscription <imocor@consulnetti.com> ☆

Transaction Confirmation

☆



Dear Customer,

Thank You for choosing Geek Total Protection.
We have renewed your Subscription as per your electronic consent.
Hope you are with us.
This email is to inform you that an amount of \$499.99 has been charged for the services.
For any assistance, please call: **+1-808-666-6112**.

Order details:
Invoice Number: **GS-93404-0841036**
Registered Email: **imocor@consulnetti.com**
Service: Geek Total Protection
Renewal Date: May 20, 2022
Next Renewal: May 20, 2023

Multi-Factor Authentication Fatigue



Mitigation Strategies

- Time-based one-time passwords
- Biometric authentication
- Context-aware authentication
- Adaptive authentication

Source: [Proofpoint](#)

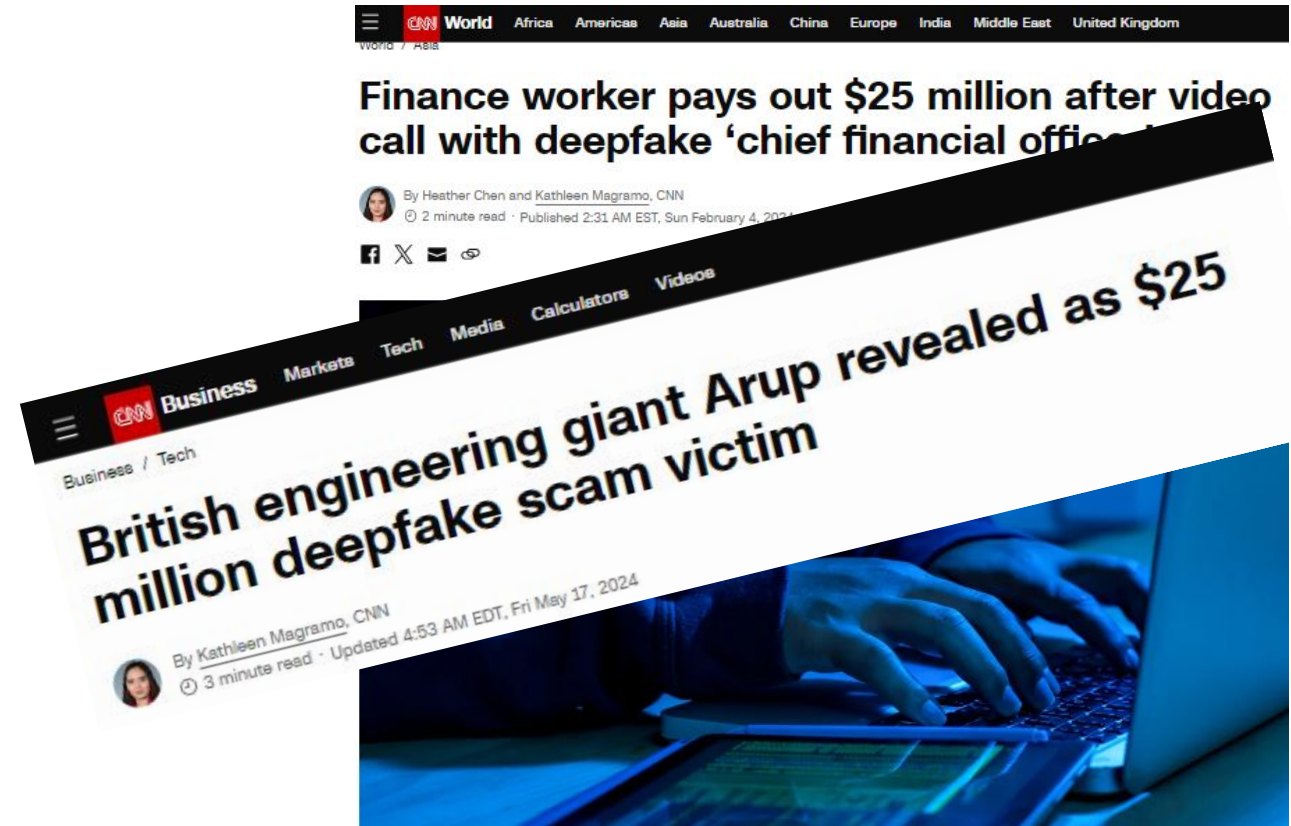
Threats on the Horizon: Artificial Intelligence

Artificial What?

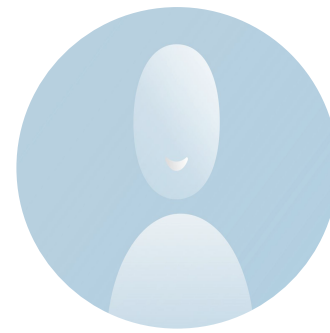
- Large Language Models
- Generative AI
- ChatGPT / Google Bard Gemini

Threats

- Adversarial Use
 - Perfect Phishing & Scams
 - Deep Fakes
- Data Loss
- Lack of Trust / Integrity
 - AI Poisoning
 - AI Hallucination



Current Cyber Threat Trends (March 2025)



Blended Threats Cyber-Physical Risks - chatter online discussing harm to health sector organizations and executives. While the likelihood of these attacks coming to fruition is low, it is recommended to take them seriously.

Remote IT Fraud Workers - ongoing campaign of fraudulent job applicants extort health sector organizations once employment is gained.

Credential Compromise - compromised healthcare sites serving commodity malware to unsuspecting patients and harvest information about their visitors, then distribute different payloads accordingly. The malware deployed often steals credentials from victim systems.

RMM Weaponization - ongoing use of remote monitoring and management (RMM) software like ScreenConnect to gain access to devices to steal sensitive information or deploy malware.

Procurement Fraud - threat actors targeting procurement teams via impersonation emails. These campaigns are fueled by business email compromise, wherein seemingly legitimate communications, sent from compromised third-party vendor contacts, are used to alter banking information to accounts controlled by threat actors.



Staying Safe On-Line

Quick Tips

Use Strong Passwords

- Do not reuse the same username / password combination across different sites
- Consider using a password manager



1Password



DASHLANE



LastPass



Google Password Manager



NordPass



KEEPER
Cybersecurity Starts Here

Use Multi-Factor Authentication (MFA)



Source: <https://news.vanderbilt.edu/2020/04/08/enroll-in-multi-factor-authentication-to-protect-vanderbilt-systems-and-data/>

Use Multi-Factor (or Two-Factor) Authentication!

Don't be a victim of cybercrime!

Amazon

<https://www.amazon.com/gp/help/customer/display.html?nodeId=201596330>



Apple

<https://support.apple.com/en-us/HT204152>

Dropbox

<https://help.dropbox.com/account-access/enable-two-step-verification>

eBay

<https://accounts.ebay.com/acctsec/security-center>

Facebook:

<https://www.facebook.com/help/148233965247823>



Gmail

<http://www.google.com/intl/en-US/landing/2step/features.html>

LinkedIn

<https://www.linkedin.com/help/linkedin/answer/531?lang=en>



Microsoft / Outlook.com

<http://windows.microsoft.com/en-us/windows/two-step-verification-faq>

Paypal

<https://www.paypal.com/us/webapps/mpp/security/security-protection>

SnapChat

<https://support.snapchat.com/en-US/ca/login-verification>

Twitter

<https://support.twitter.com/articles/20170431#>

US Internal Revenue Service (IRS) (**ID.me**)

<https://www.irs.gov/payments/your-online-account>

US Postal Service (USPS)

Go to "My Preferences" then "Security" to enable 2FA

US Social Security Administration (**Login.gov or ID.me**)

<https://www.ssa.gov/myaccount/MoreInformationAboutMFA.html>



Yahoo!

<https://help.yahoo.com/kb/SLN5013.html>

- Financial Institutions
- Online Retailers
- ... and more...

Recommendations & Free Resources (Technical)

Health Industry Cybersecurity Practices (HICP) 2023 from the Health Sector Coordinating Council

<https://405d.hhs.gov/information#hicp>

★ **HICP Main Document** - <https://405d.hhs.gov/Documents/HICP-Main-508.pdf> □ **Top 5 Threats**

★ Technical Volume 1 (Small Healthcare Orgs) - <https://405d.hhs.gov/Documents/tech-vol1-508.pdf>

★ Technical Volume 2 (Medium & Large Healthcare Orgs) - <https://405d.hhs.gov/Documents/tech-vol2-508.pdf>

Top 10
Cybersecurity
Practices

More resources:

- Health Sector Coordinating Council - <https://healthsectorcouncil.org/>
 - Cybersecurity for the Clinician Video Training Series - <https://healthsectorcouncil.org/cyberclinicianvideos/>
 - HPH Sector Cybersecurity Framework Implementation Guide - <https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide>
 - Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT) - <https://healthsectorcouncil.org/securingtelehealth/>
 - Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2) - <https://healthsectorcouncil.org/HIC-SCRiM-v2/>
 - Coordinated Healthcare Incident Response Plan - https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf

Recommendations & Free Resources

Health-ISAC – www.h-isac.org

- Annual Threat Report - <https://health-isac.org/health-isac-2025-health-sector-cyber-threat-landscape/>
- Information on DDoS, including mitigation strategies - <https://health-isac.org/white-paper-distributed-denial-of-services-ddos-attacks/>
- AHA & Health-ISAC / Preparing for the Next “SolarWinds” Event - <https://h-isac.org/preparing-for-the-next-solarwinds-event-2/>

Health Sector Cybersecurity Coordination Center (HC3) - <https://www.hhs.gov/about/agencies/asa/ocio/hc3>

HHS 405(d) Aligning Health Care Industry Security Approaches - <https://405d.hhs.gov/>

HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) - aspr.hhs.gov

Personal Tips for Staying Safe Online - <https://www.youtube.com/watch?v=0QRC0QrVcZk>

- Multi-Factor Authentication and the best defense is a good offense

The Lazarus Heist Podcast and YouTube Series

- <https://www.bbc.co.uk/programmes/w13xtvg9/episodes/downloads>

More About Health-ISAC

- Annual membership fees start at \$2,400
- Benefits



Community

Events



Education



Threat Intelligence

Co



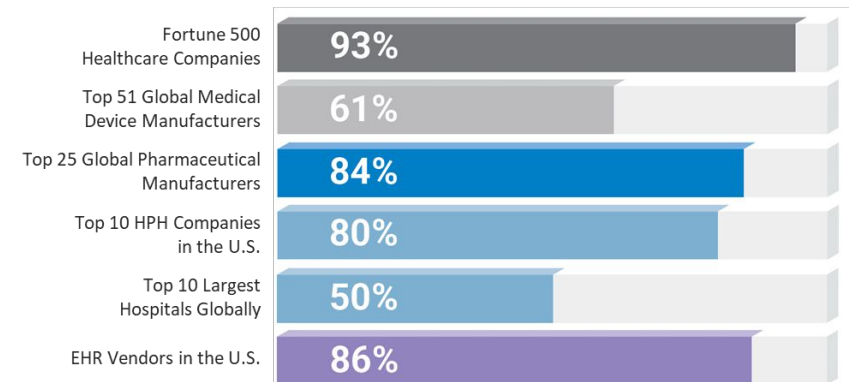
munity Services



Cybersecurity Automation

- Visit Health-ISAC to learn more
www.health-isac.org

Health-ISAC Members include:



Questions?

Errol Weiss

Chief Security Officer, Health-ISAC

+1 321-209-9898

eweiss@h-isac.org

Health-ISAC 2025 Health Sector Cyber Threat Landscape Report

<https://health-isac.org/health-isac-2025-health-sector-cyber-threat-landscape/>

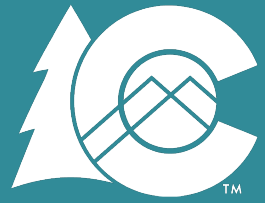


Health-ISAC™

Collaborating for Resilience in Healthcare



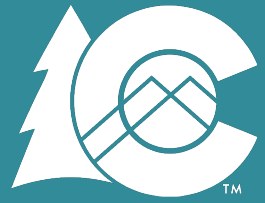
Visit Health-ISAC to learn more
www.health-isac.org



OeHI

Office of eHealth Innovation

Public Comment Period



OeHI

Office of eHealth Innovation

Closing Remarks