

BUILDING SECURE AND RESILIENT INFRASTRUCTURE – CYBERSECURITY 101

N'gai Oliveras

Cybersecurity Advisor

U.S. Department of Homeland Security (DHS)

Cybersecurity and Infrastructure Security Agency

Region 2 - NY, NJ, PR, USVI



Homeland
Security

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

CISA partners with industry and
government to understand and
manage risk to our Nation's
critical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP
DEVELOPMENT



INFORMATION AND
DATA SHARING



CAPACITY BUILDING



INCIDENT
MANAGEMENT
& RESPONSE



RISK ASSESSMENT
AND ANALYSIS



NETWORK DEFENSE



EMERGENCY
COMMUNICATIONS

Who we are?



The Cybersecurity and Infrastructure Security Agency (CISA) is the newest agency of the federal government, established in 2018 to be the United States Cyber Defense Agency.

We serve as the National Coordinator for Critical Infrastructure Security and Resiliency, leading the effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans depend on every hour of every day.

The Significance of Critical Infrastructure

Critical infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on **national security, the economy, public health or safety, and our way of life.**



Serving Critical Infrastructure

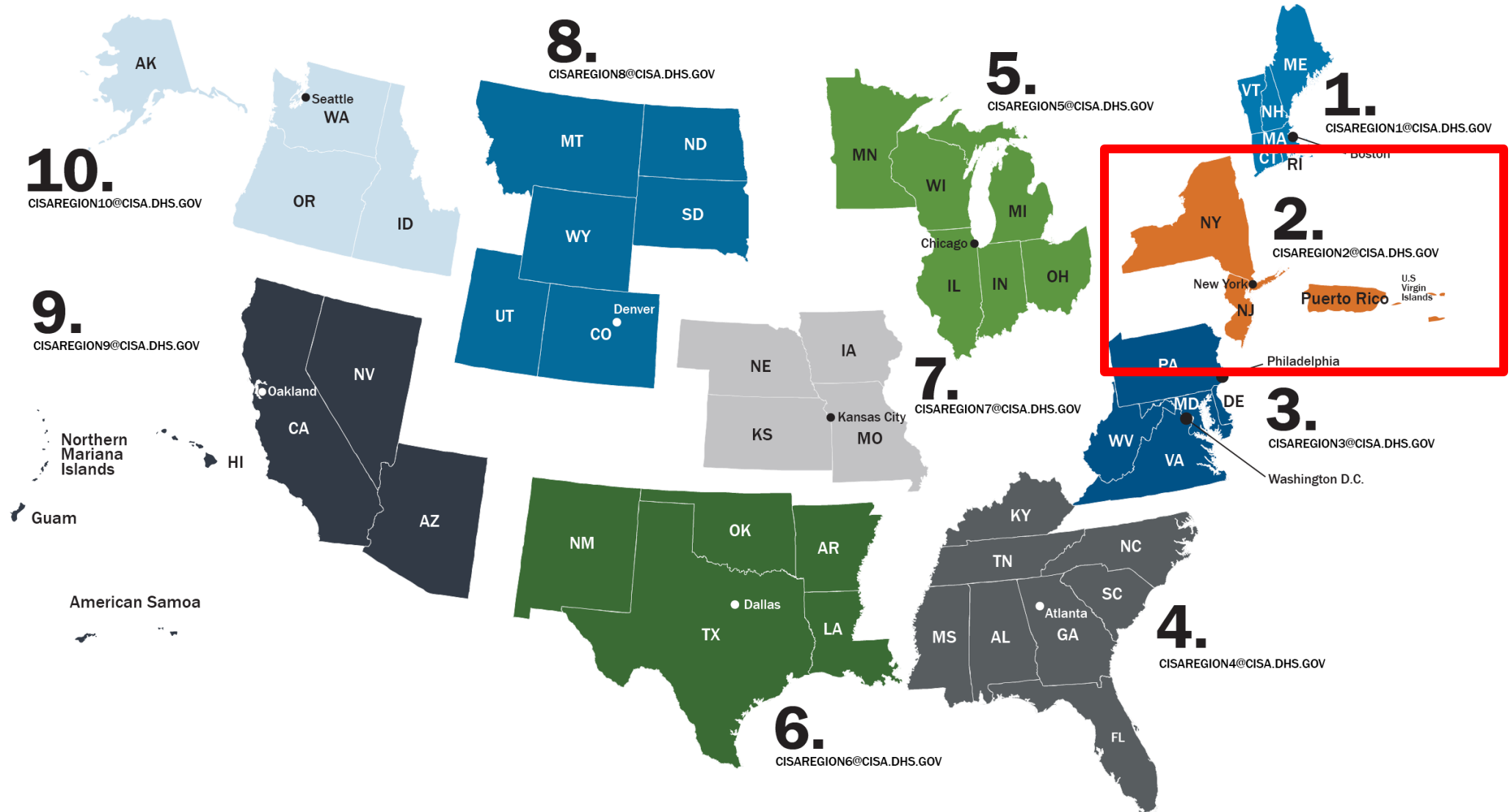
16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA



CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA





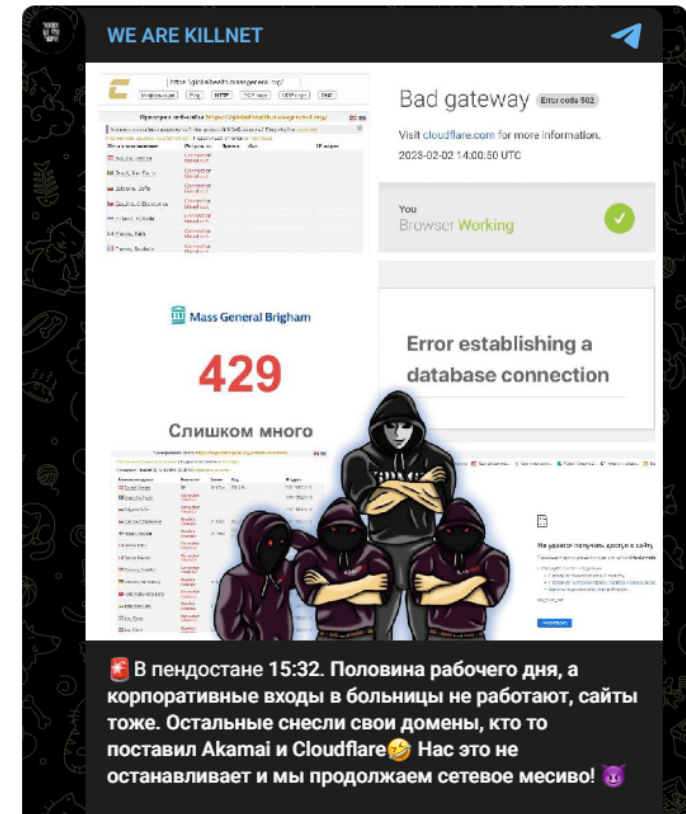
CYBERSECURITY THREATS AND VULNERABILITIES

Healthcare Devices

Current Threat in USA Health Sector

Killnet in 2023

Since the end of January, Killnet has been actively targeting healthcare organizations. In their telegram post, they shared that the corporate entrances and websites of various hospitals were down and that this attack was a joint operation.



July 11, 2023

Cyber attacks in Public Health Sector

Becker's Healthcare: Hospital | ASC

BECKER'S
HEALTH IT

289 healthcare organizations were impacted by ransomware attacks in 2022

Naomi Diaz - Tuesday, January 3rd, 2023



Ransomware attacks impacted more than 289 hospitals in 2022, [BleepingComputer](#) reported Jan. 2.

Ransomware attacks on hospitals and multihospital health systems totalled 24 in 2022 but potentially affected as many as 289 hospitals, according to the report.

The largest ransomware attack on a hospital in 2022 was the Chicago-based [CommonSpirit ransomware attack](#) that compromised the data of 623,000 patients.

In 17 ransomware incidents affecting the healthcare sector, hackers stole files that contained protected health or personal information.



July 11, 2023

Cyber attacks in Public Health Sector



News Media Conferences Resources Subscribe

SPOTLIGHT- Data + Technology | Healthcare Transformation | Leadership | Management | Patient Experience | Product Solutions

Nearly 50 million Americans impacted by health data breaches in 2022

Feb 15, 2023

Ron Southwick



World Business Legal Markets Breakingviews Technology Invest



Data Privacy

Health



4 minute read · February 6, 2023 4:52 PM GMT-4 · Last Updated a month ago



Three U.S. data breaches show varied healthcare exposure risks

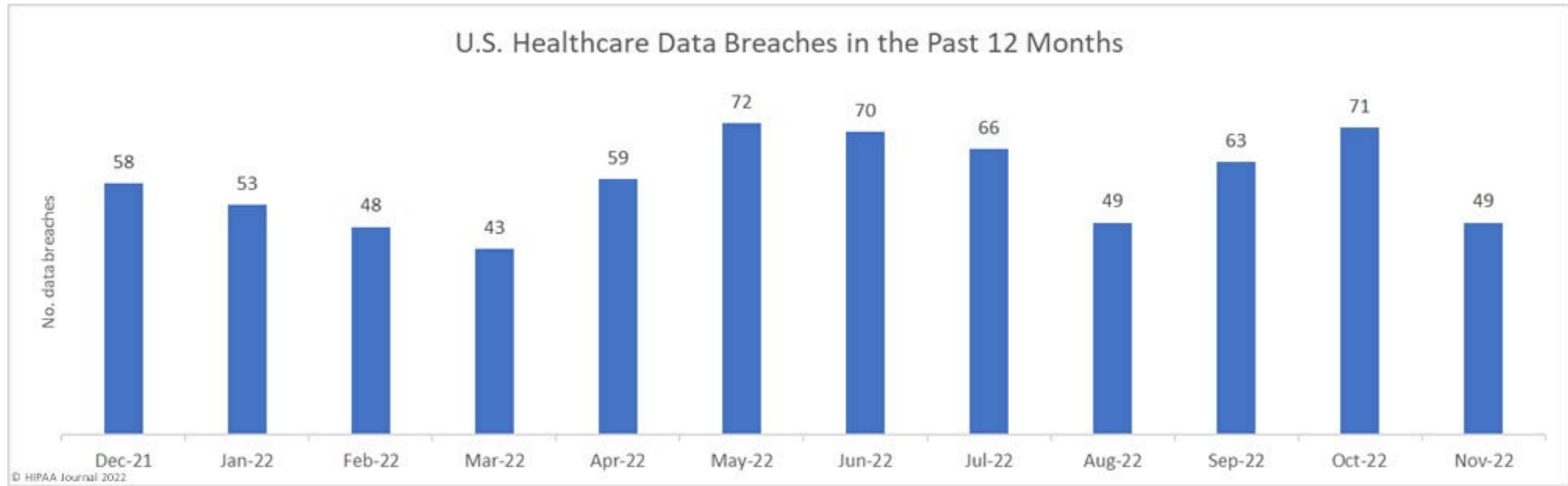
Reuters

NEW YORK(Thomson Reuters Regulatory Intelligence) - Three recent data breaches from across the United States show that the risks of data breaches can come from multiple sources for healthcare providers. Employees, third-party vendor tools and cybercriminals all create data breach risks.



July 11, 2023

2022 Healthcare Data Breach Report

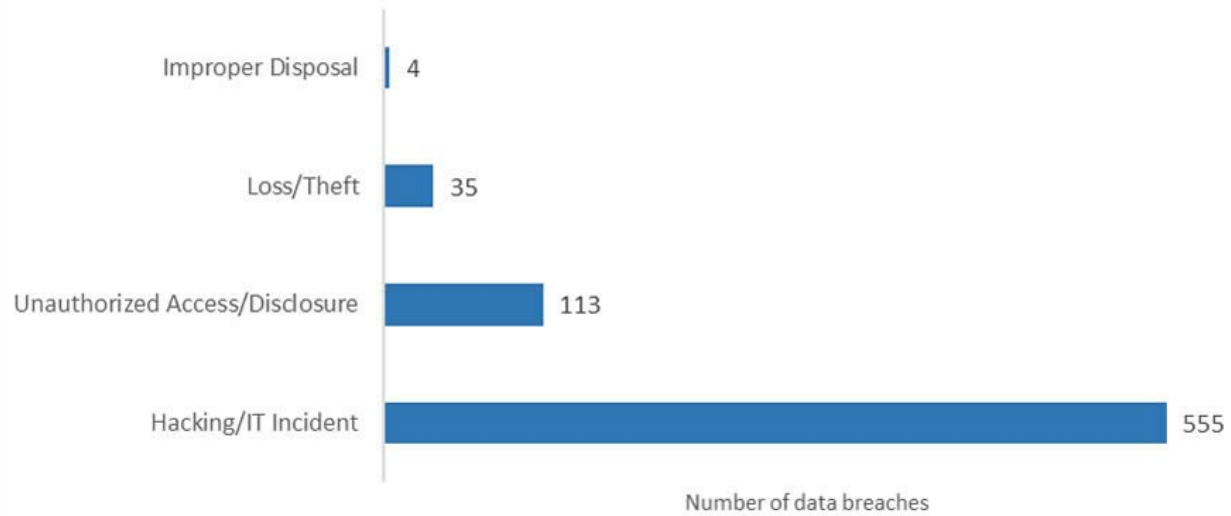


*Information provided by The HIPPA Journal

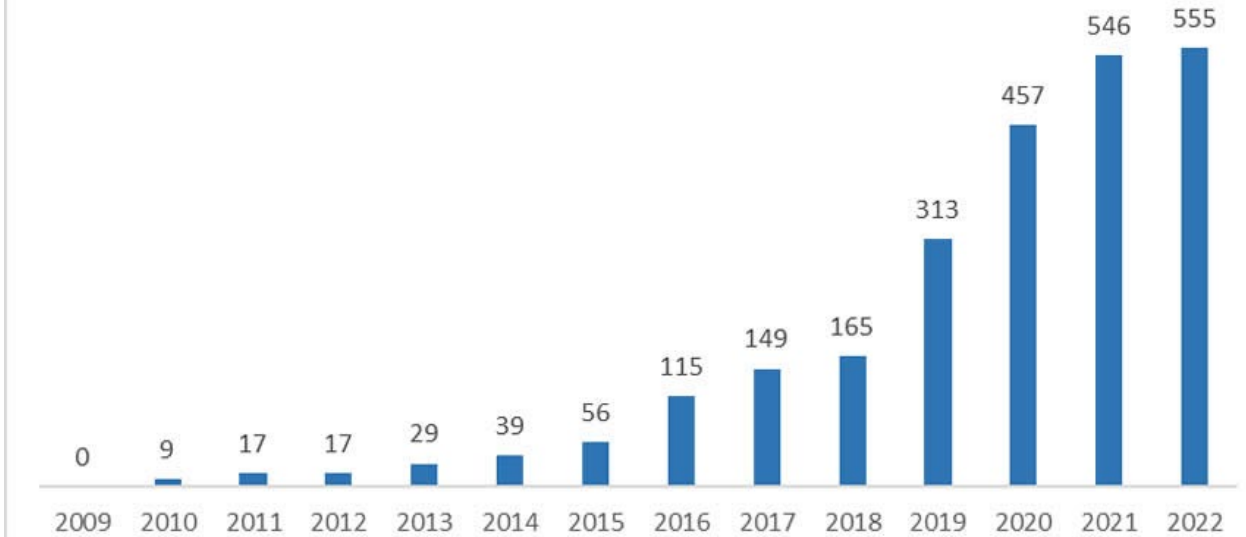
July 11, 2023

2022 Healthcare Data Breach Report

Classification of 2022 Healthcare Data Breaches



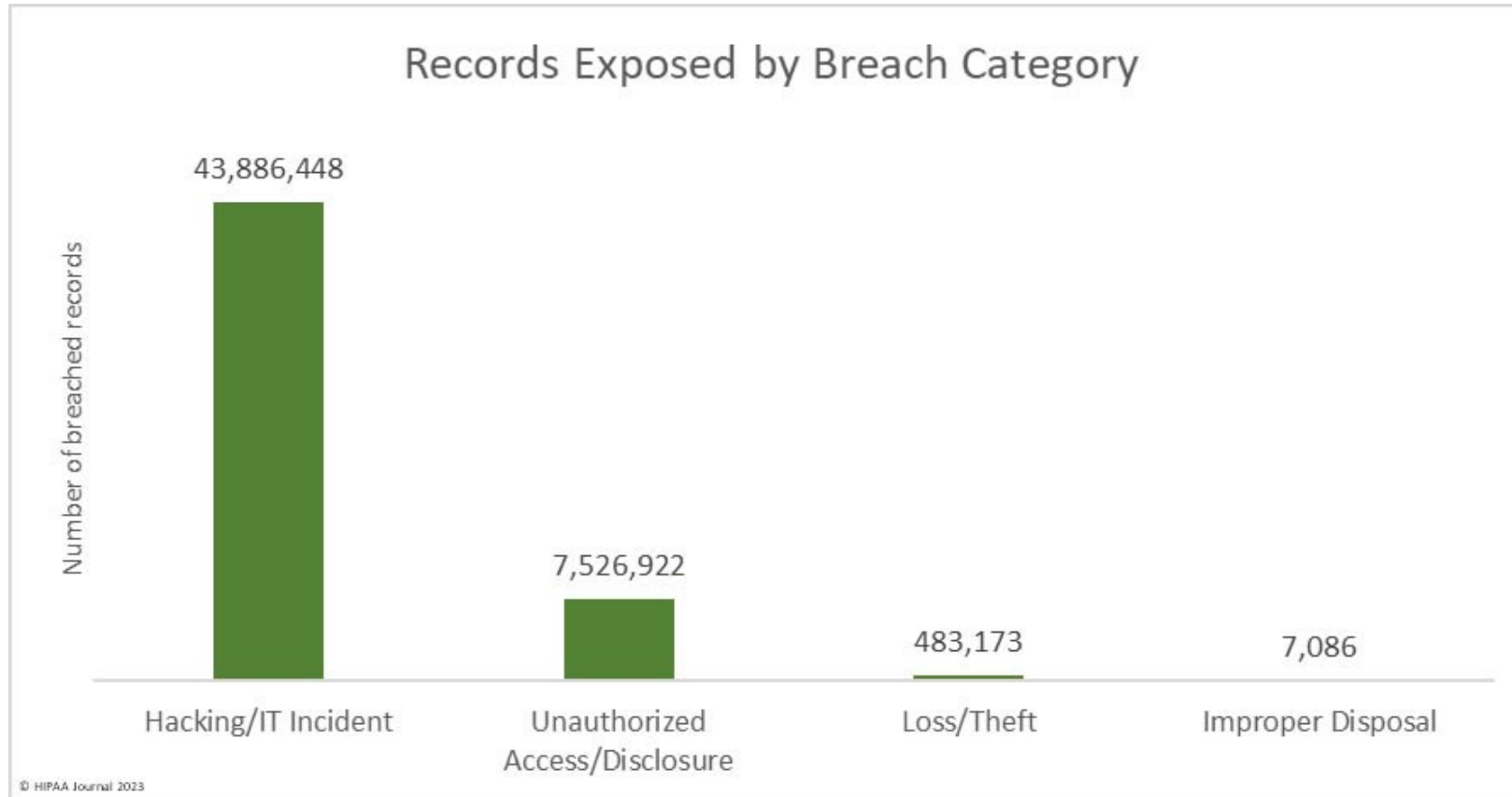
HACKING/IT INCIDENTS



*Information provided by The HIPPA Journal

July 11, 2023

2022 Healthcare Data Breach Report

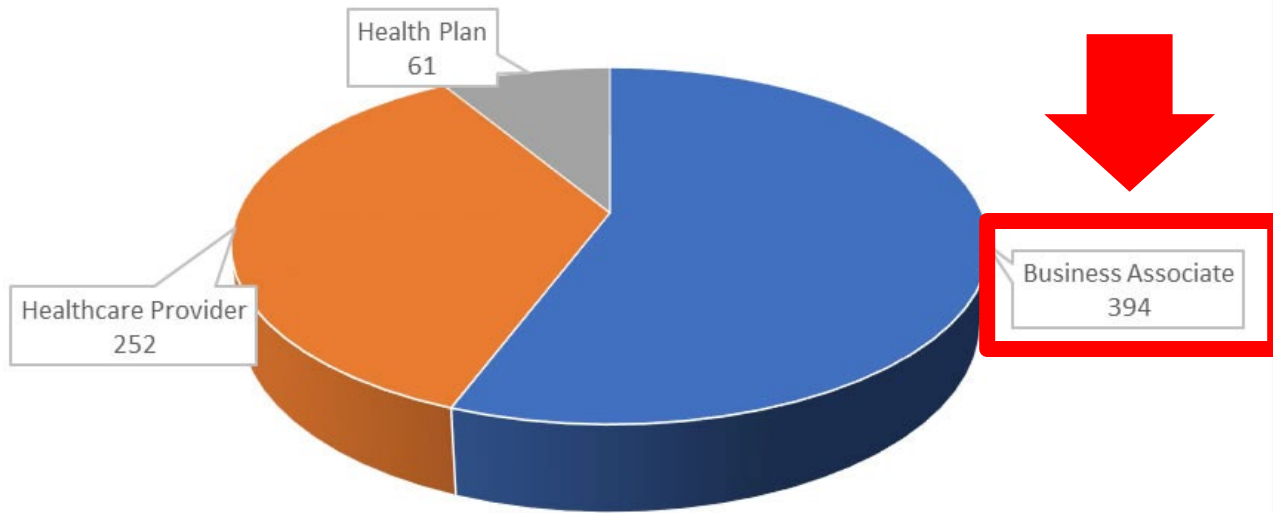


*Information provided by The HIPPA Journal

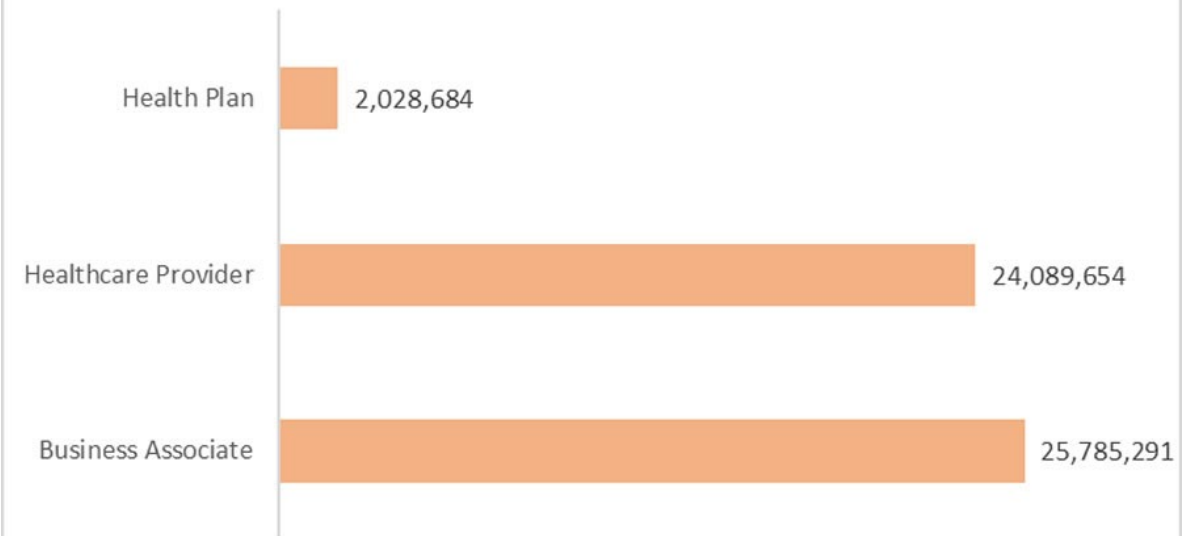
July 11, 2023

2022 Healthcare Data Breach Report

Where Did The Data Breaches Occur?



Records Exposed in 2022 Healthcare Data Breaches



*Information provided by The HIPPA Journal

July 11, 2023



Example of third-party providers Incidents

FAA NOTAM Statement

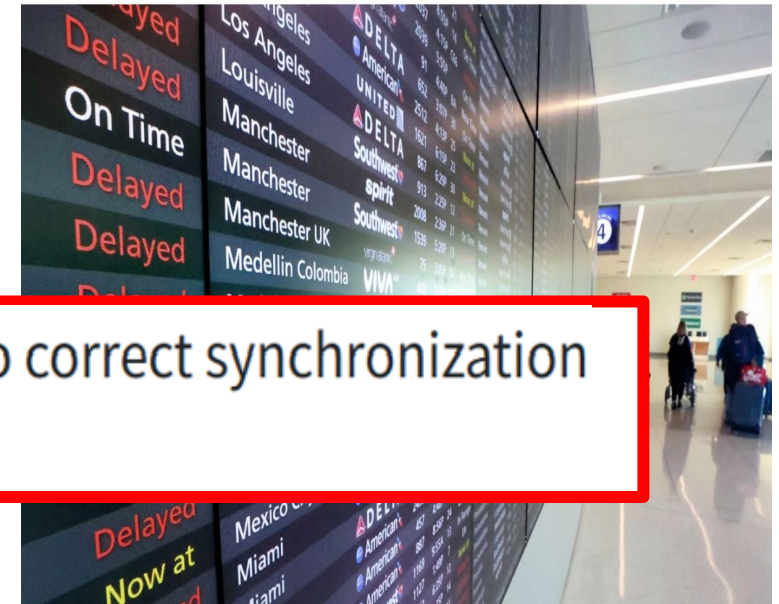
Thursday, January 19, 2023

FAA STATEMENT 7:15 p.m. EST

A preliminary FAA review of last week's outage of the Notice to Air Missions (NOTAM) system determined that contract

contract personnel unintentionally deleted files while working to correct synchronization the live primary database and a backup database.

The FAA made the necessary repairs to the system and has taken steps to make the NOTAM system more resilient. The agency is acting quickly to adopt any other lessons learned in our efforts to ensure the continuing robustness of the nation's air traffic control system.



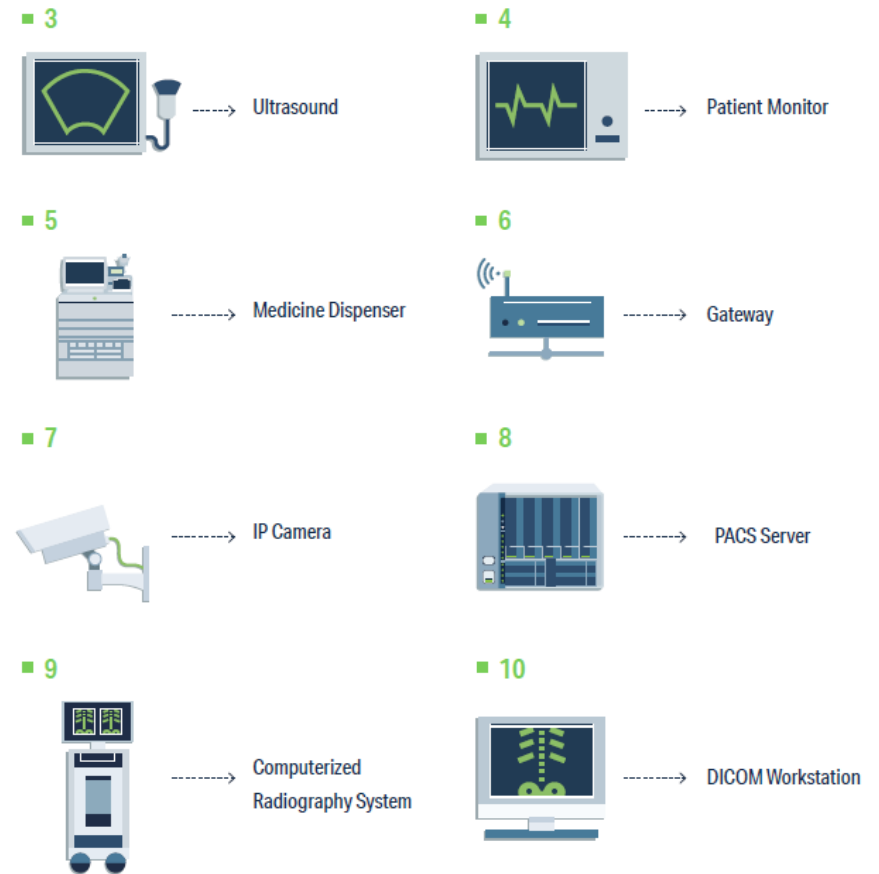
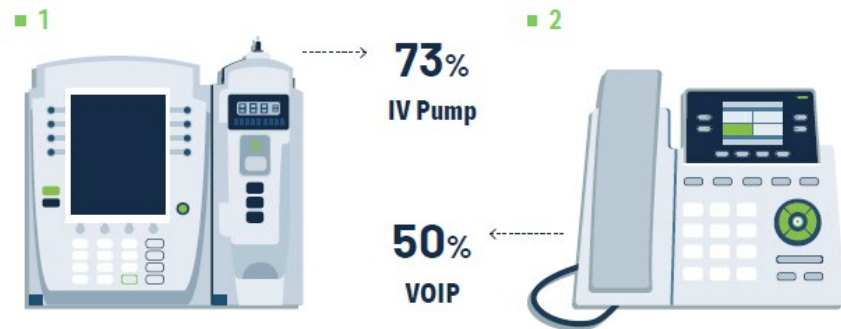
July 11, 2023

Health IoT Devices Vulnerabilities

What Are the Bedside Healthcare IoT Devices with the Most Identified Vulnerabilities?

A glimpse into the devices closest to patients

The closer a healthcare IoT device gets to the patient's bedside, the higher the risk score of a vulnerability detected on it will increase, since it has a much greater chance of adversely affecting a patient's care. When Cynerio technology first enters a hospital environment where there has never been any healthcare IoT cybersecurity before, these are the devices that most commonly have a critical risk while connected to a patient.



* Reference taken from the Cynerio – The State of Healthcare IoT Device Security 2022 Whitepaper

Cyber attacks can cause loss of life...

TECH / SCIENCE / HEALTH

Woman dies during a ransomware attack on a German hospital

By [NICOLE WETSMAN](#)

Sep 17, 2020, 3:11 PM GMT-4 | [0 Comments](#) / [0 New](#)



/ It could be the first death directly linked to a cybersecurity attack

THE CYBERSECURITY 202

Ransomware attack might have caused another death



Analysis by [Joseph Marks](#)

October 1, 2021 at 7:07 a.m. EDT

Nurses did not notice the fetal heart rate change, which was recorded on a strip of paper printed by the bedside monitor. It would normally have appeared on a large digital display at the nurses' station where monitoring was far easier.

The case is a stark reminder of the devastating human costs that can derive from cyberattacks, where the damage is more typically measured in lost money and productivity.



July 11, 2023



CYBERSECURITY AWARENESS

**EVERYONE's
Responsibility**

Cybersecurity is EVERYONE's responsibility

77% of the reported attacks in 2021 were caused by **phishing, software vulnerabilities and poor password security** (brute-force attack).

Phishing

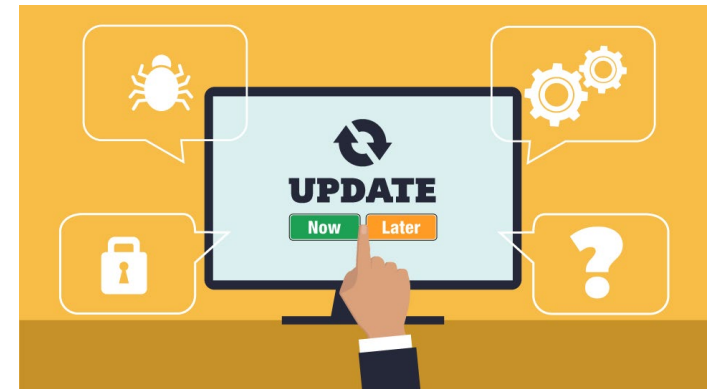


New Password

Weak

New Password

Strong



Phishing Examples

Mac OS window header with window control buttons (red, yellow, green), a search icon, and a list icon. Below the header are standard email headers: To: ACCOUNTING DEPARTMENT, Cc: TomHeald@strategictax.com, Subject: W2's for All Employees, From: Tom Smith, and Signature: None.

Please send our W2 Tax Documents for all employees to Tom Heald at Strategic Tax Consultants. I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith
CEO
BetterSystems Inc



Light grey email header area. It shows 'From Accountant <laura@...> ☆', 'Subject Customer Invoice', and a redacted 'To' field.

Dear Customer,

Here's invoice INV-0052 for \$AUD 3,226.00.
We will be appreciated if you will react promptly.
To download the invoice, please follow the next link:

<http://...com/view>

If you are unable to download your Invoice, please contact us immediately . Thank you.

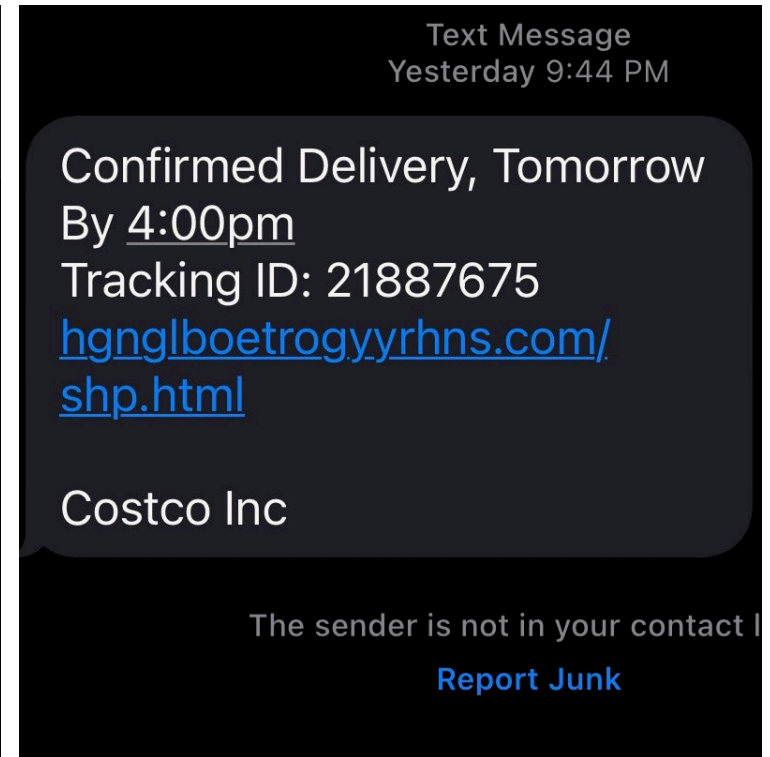
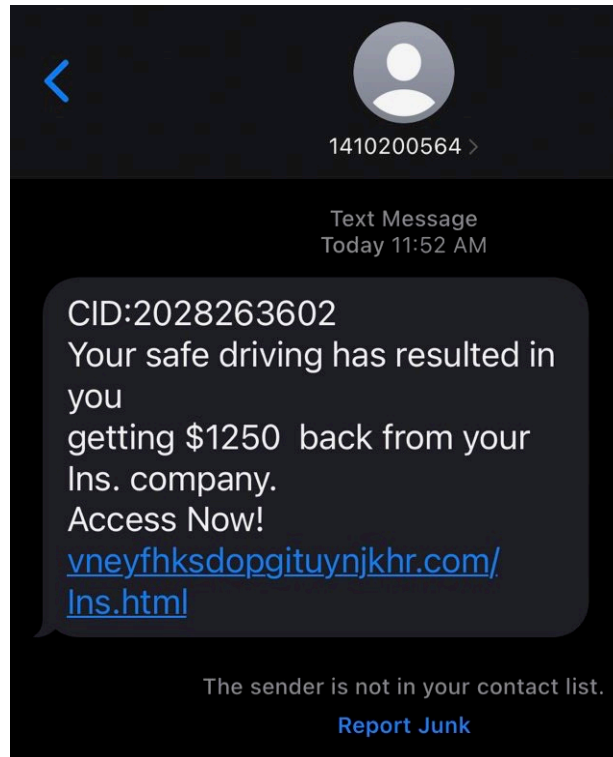
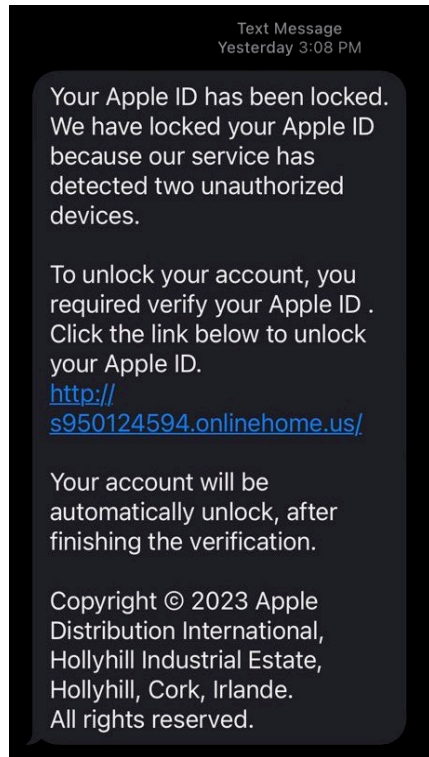
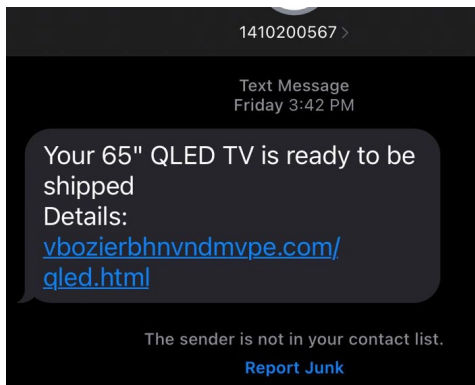
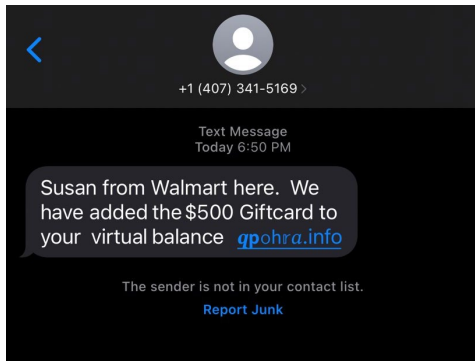
Kind regards,

Rachael Gatt | CPA

Accountant

July 11, 2023

Smishing Examples – Text Messages



Vishing Example – Phone Calls

“This call is from the Department of Social Security administration the reason you have _____ call from our department is to inform you that we just suspend your Social Security number because we found some suspicious activity so if you want to know about this case just press one thank you...”

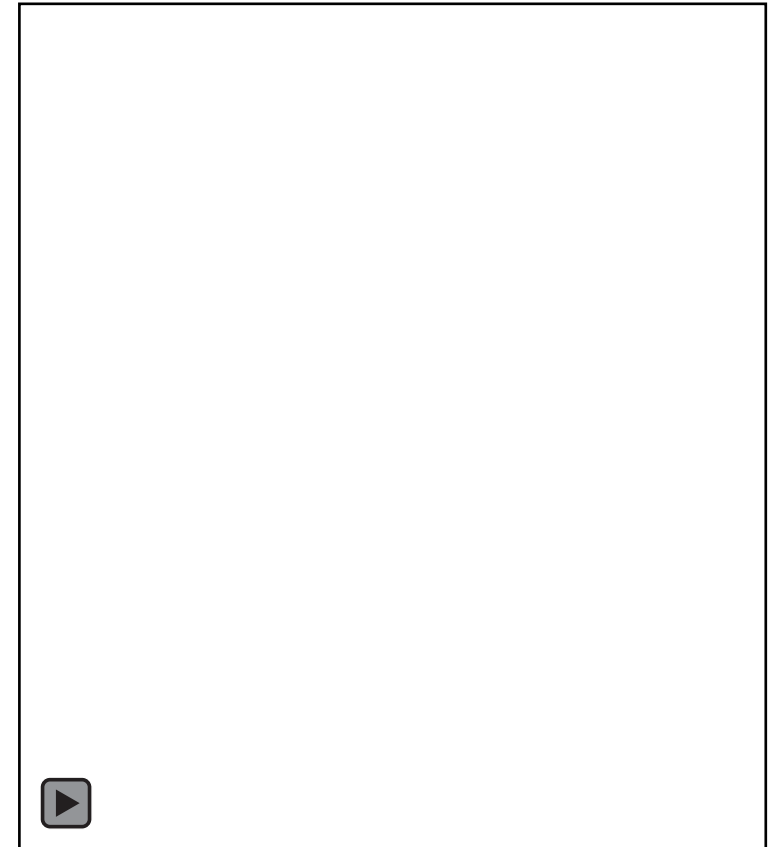


Phishing Example – Social Media



Phishing Attack Example

Phishing



Action Steps - Phishing

Phishing



- **Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Provide Cybersecurity Awareness training to **ALL** the users in your organization.**



Action Steps - Passwords

New Password

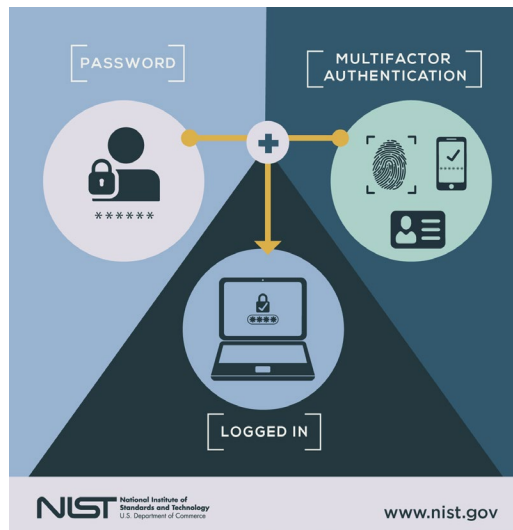
123456

Weak

New Password

a81@BnM_78

Strong



- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated.



Action Steps – Software Updates



- **Update Your Software:** Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.





CISA SERVICES AND RESOURCES

Sampling of Physical Security Offerings

- **Protective Security Advisors**
- **Active Shooter Training**
- **Tabletop Exercises Program**
- **Assist Visits**
- **Infrastructure Survey Tool**
- **Infrastructure Visualization Platform**
- **Regional Resiliency Assessment Program**



Sampling of Cybersecurity Offerings

- **CISA Central**

- National US-CERT
 - Remote Assistance
 - Malware Analysis

- **Cybersecurity Advisors**

- **Cyber Tabletop Exercises Program**

- **User Awareness Training**

- Cybersecurity National Awareness Month Campaign

- **CISA Cybersecurity Services**

- **Cyber Hygiene**

- Vulnerability Scanning
- Web Application Scanning

- ***Risk & Vulnerability Assessment (RVA)**

- ***Remote Penetration Testing (RPT)**

- ***Phishing Campaign Assessment (PCA)**

- **Cyber Security Evaluation Tool (CSET)**

- Ransomware Readiness Assessment (RRA)
- Cybersecurity Maturity Level Assessment (CMM)
- Cyber Resilience Review (CRR)

* Services offered by invitation only.



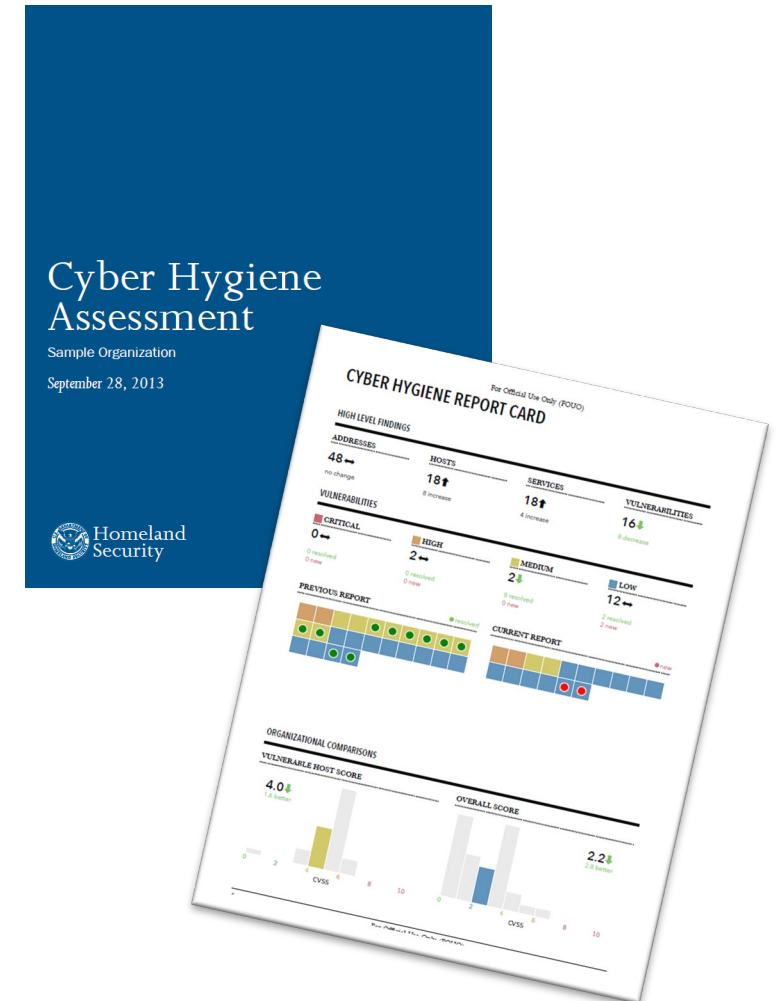
Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness



Cyber Security Evaluation Tool (CSET)

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
 - Immediately available for download upon request
 - <https://www.cisa.gov/uscert/ics/Downloading-and-Installing-CSET>
 - Understanding of operational technology and information technology network security practices
 - Ability to drill down on specific areas and issues
 - Helps to integrate cybersecurity into current corporate risk management strategy

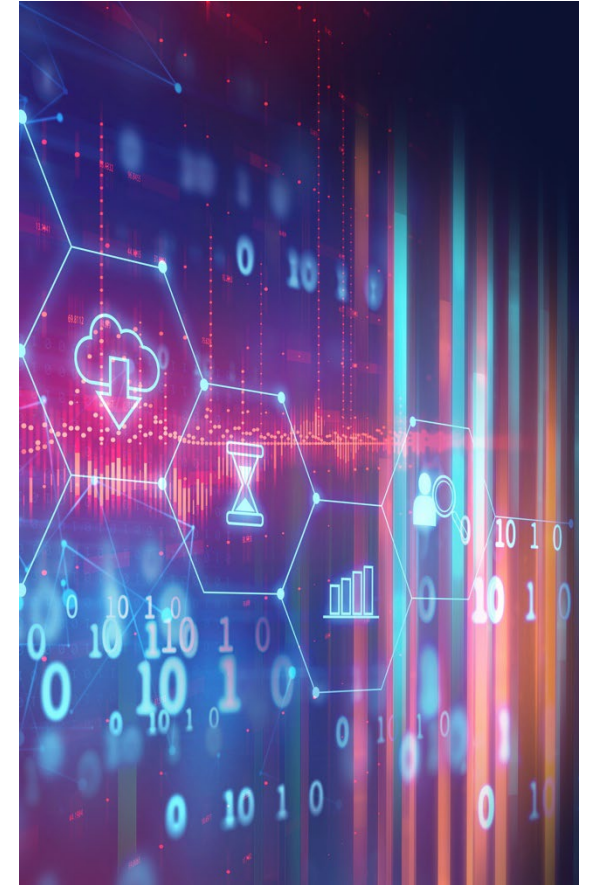
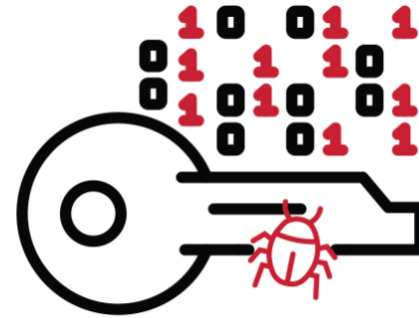


Cyber Security Evaluation Tool (CSET)


CISA Ransomware Readiness Assessment (RRA)

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware disrupts or halts an organization's operations and poses a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and restore operations themselves. The methods used to access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid. Ransomware attacks target the organization's data.

To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA).



Cybersecurity Awareness Program

 An official website of the United States government [Here's how you know](#) ▾

[REPORT](#) [SUBSCRIBE](#) [CONTACT](#) [SITE MAP](#)



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



cisa.gov/uscert

[Report Cyber Issue](#)

[Subscribe to Alerts](#)



CYBERSECURITY



INFRASTRUCTURE
SECURITY



EMERGENCY
COMMUNICATIONS



NATIONAL RISK
MANAGEMENT



ABOUT
CISA



MEDIA

[Cybersecurity](#) > [CISA Cybersecurity Awareness Program](#)

Cybersecurity

[Cybersecurity Training & Exercises](#)

[Cybersecurity Summit 2020](#)

[Cyber QSMO Marketplace](#)

[Combating Cyber Crime](#)

[Securing Federal Networks](#)

[Protecting Critical Infrastructure](#)

[Cyber Incident Response](#)

[Cyber Safety](#)

CISA CYBERSECURITY AWARENESS PROGRAM

The CISA Cybersecurity Awareness Program is a national public awareness effort aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

Cyber Tips and Resources

About the CISA Cybersecurity Awareness Program

The CISA Cybersecurity Awareness Program is a national public awareness effort that increases the understanding of cyber threats and empowers the American public to be safer and more secure online.



Join the CISA Cybersecurity Awareness Program

Non-profit organizations, government agencies, colleges and universities, and individuals can join the CISA Cybersecurity Awareness Program. Join today.



<https://www.cisa.gov/cisa-cybersecurity-awareness-program>

July 11, 2023

Additional Resources

Cross-Sector Cybersecurity Performance Goals | CISA



https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf

July 11, 2023

Additional Resources



CISA has a new webpage with the latest guidance on how organizations can regardless of size – adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets.

This guidance is available at www.cisa.gov/shields-up.



Free Tools



CISA published a new catalog of **free cybersecurity services and tools** available to critical infrastructure owners and operators who would benefit from tools to help their security and resilience. The webpage is a one-stop resource where organizations of all sizes can find free public and private sector resources to reduce their cybersecurity risk.

You can find this here www.cisa.gov/free-cybersecurity-services-and-tools



Additional Resources

The screenshot shows the homepage of stopransomware.gov. At the top left is the "STOP RANSOMWARE" logo. To its right is a search bar with a magnifying glass icon. Below these is a red navigation bar with the following links: "RESOURCES", "NEWSROOM", "ALERTS", "REPORT RANSOMWARE", and "CISA.GOV". The main content area is divided into three sections:

- Left Section:** Features the "STOP RANSOMWARE" logo, an image of three padlocks (two blue, one red) on a background of binary code, the hashtag "#STOPRANSOMWARE", and the text "RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE FUND" above the large "DPRK" logo and "ESPIONAGE ACTIVITIES".
- Middle Section:** Shows a laptop screen with the word "RANSOMWARE" and binary code. It includes the text "HAVE YOU BEEN HIT BY RANSOMWARE?" and a "LEARN MORE" button.
- Right Section:** A dark blue area with a red border containing the text "Known Exploited Vulnerabilities Catalog" and "cisa.gov". It also features a red "UPdated" badge and the CISA logo.

stopransomware.gov



July 11, 2023

Training Resources



The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans. [Click here](#) to view the FedVTE course catalog.

Log In with an Existing Account

Email:

Password: [I forgot my Password](#)

[Log In](#)

Public Content

[Click Here for Publicly Available Free Courses](#)

New Users

If you are a federal, state, local, tribal, or territorial government employee, a federal contractor, or a US military veteran, you can create a new account by clicking the button below.

[Register Here](#)

<https://fedvte.usalearning.gov/>



July 11, 2023

Training Resources

Publicly Available Free Courses		
101 Coding for the Public		Launch Course
101 Critical Infrastructure Protection for the Public		Launch Course
101 Reverse Engineering for the Public		Launch Course
Cloud Computing Security	2.5 Hours	Launch Course
Cloud Security - What Leaders Need to Know	1 Hour	Launch Course
Cryptocurrency for Law Enforcement for the Public		Launch Course
Cyber Supply Chain Risk Management for the Public		Launch Course

Cyberessentials	1 Hour	Launch Course
Don't Wake Up to a Ransomware Attack	1 Hour	Launch Course
Foundations of Cybersecurity for Managers	2 Hours	Launch Course
Fundamentals of Cyber Risk Management		Launch Course
Introduction to Cyber Intelligence	2 Hours	Launch Course
Securing Internet-Accessible Systems	1 Hour	Launch Course
Understanding DNS Attack	1 Hour	Launch Course
Understanding Web and Email Server Security	1 Hour	Launch Course

<https://fedvte.usalearning.gov/>



Report

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

www.cisa.gov/report

report@cisa.gov

[1\(888\) 282-0870](tel:18882820870)



Questions?

Puerto Rico & USVI Contacts:

Department of Homeland Security (DHS)

Cybersecurity and Infrastructure Security Agency (CISA)

Julio González

Protective Security Advisor

Region 2 - NY, NJ, **PR, USVI**

787.244.8195

julio.gonzalez@hq.dhs.gov

N'gai Oliveras

Cybersecurity Advisor

Region 2 - NY, NJ, **PR, USVI**

202.826.8916

ngai.oliveras@cisa.dhs.gov

