LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Electronic Medical Records in Healthcare

02/17/2022

TLP: WHITE, ID# ***202202171300***

Agenda

- What Is an EMR, and How Is It Used in Healthcare?
- Top EHR Software Used in Hospitals
- Benefits & Risks of Using EMR/HER
- Why EMRs/EHRs Are Valuable to Cyber Attackers
- How Are EMR/EHRs Stored and Handled?
- EMR Compromised, Healthcare & Critical Industries Hacked
- Healthcare Industry Under Attack
- Healthcare Industry Under Attack, Part II
- Top Data Breaches of 2021
- Top Threats Against Electronic Medical & Health Records
- Costs of Data Breach
- Protecting EMR & EHR Data
- References

Slides Key:

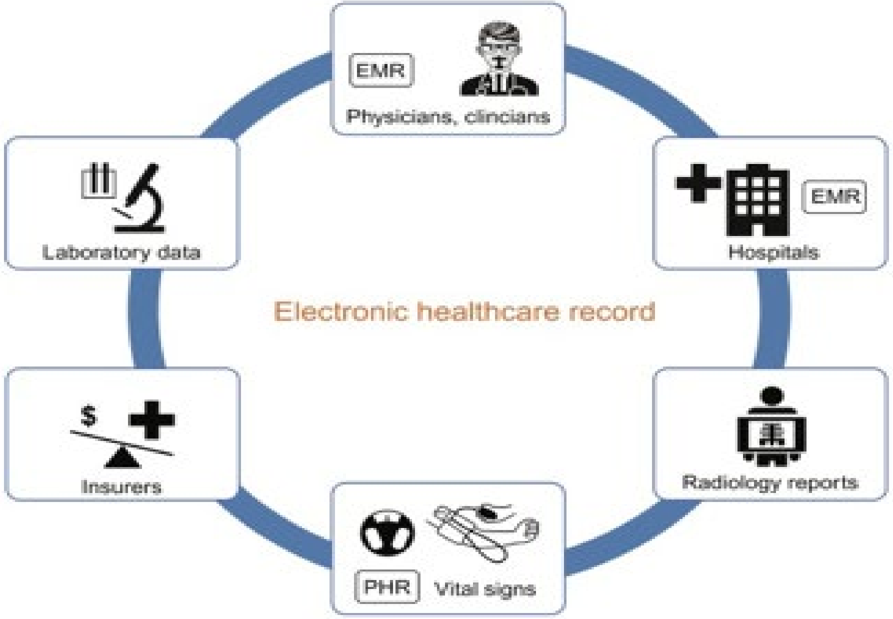
Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What Is an EMR and How Is It Used in Healthcare? EMR vs EHR

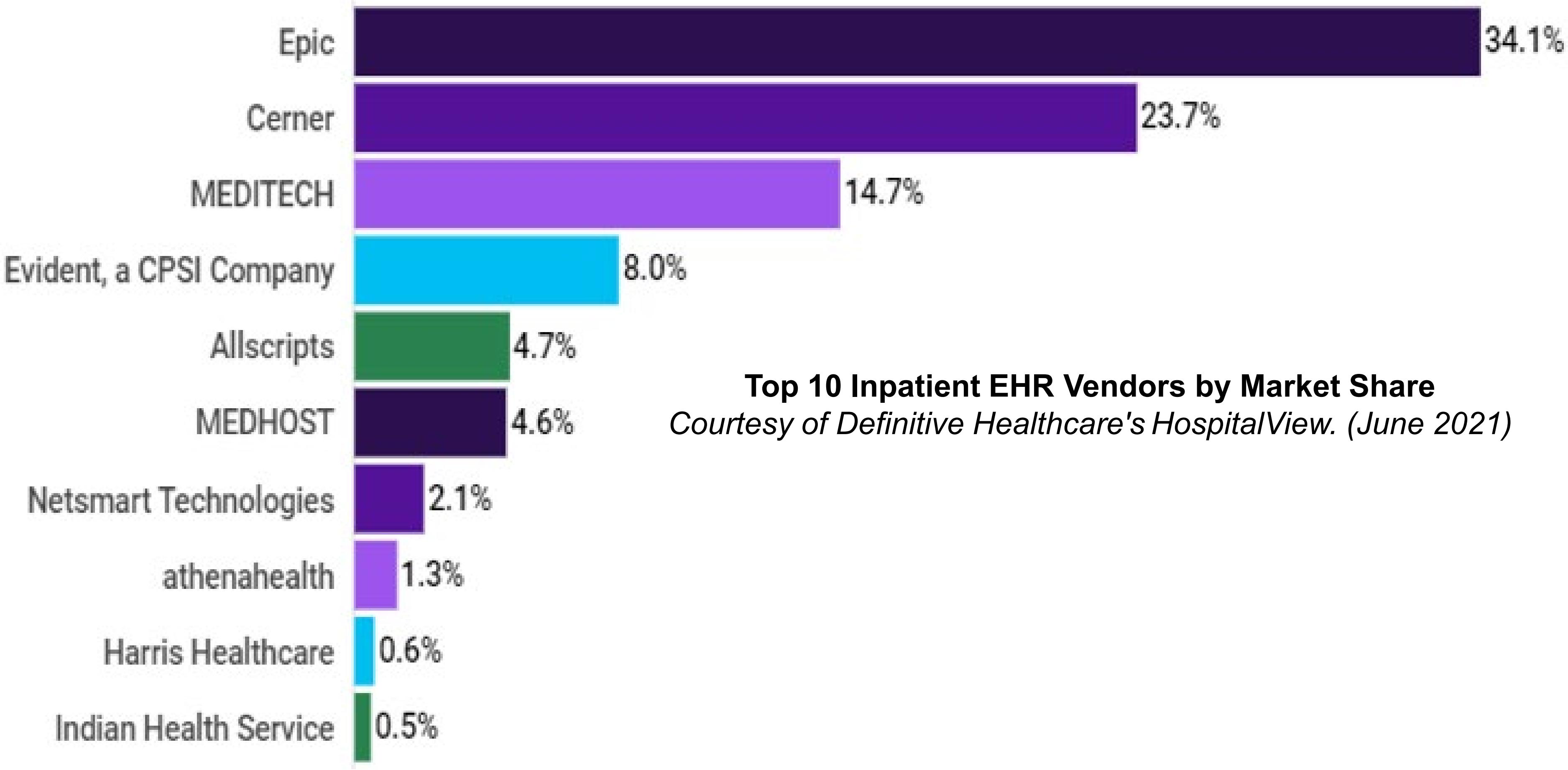
Electronic medical records (EMRs) and electronic health records (EHRs) are often used interchangeably. An EMR allows the electronic entry, storage, and maintenance of digital medical data. EHR contains the patient's records from doctors and includes demographics, test results, medical history, history of present illness (HPI), and medications. EMRs are part of EHRs and contain the following:

- Patient registration, billing, preventive screenings, or checkups
- Patient appointment and scheduling
- Tracking patient data over time
- Monitoring and improving overall quality of care



Electronic healthcare record process diagram

Top EMR/EHR Software Systems Used in Hospitals



Top 10 Inpatient EHR Vendors by Market Share
Courtesy of Definitive Healthcare's HospitalView. (June 2021)

Benefits and Risks of Using EMR/EHR

Some benefits of using electronic medical records and electronic health records are:

- Comprehensive patient-history records
- Makes patient data shareable
- Improved quality of care
- Convenience and efficiency

Some risks of using electronic medical records / electronic health records are:

The risks to EHRs relate primarily to a range of factors that include user-related issues, financial issues and design flaws that create barriers to using them as an effective tool to deliver healthcare services. EMR is also a top target in healthcare breaches. Additional risks are as follows:

- Security or privacy issues
- Potentially vulnerable to hacking
- Data can be lost or destroyed
- Inaccurate paper-to-computer transmission
- Cause of treatment error

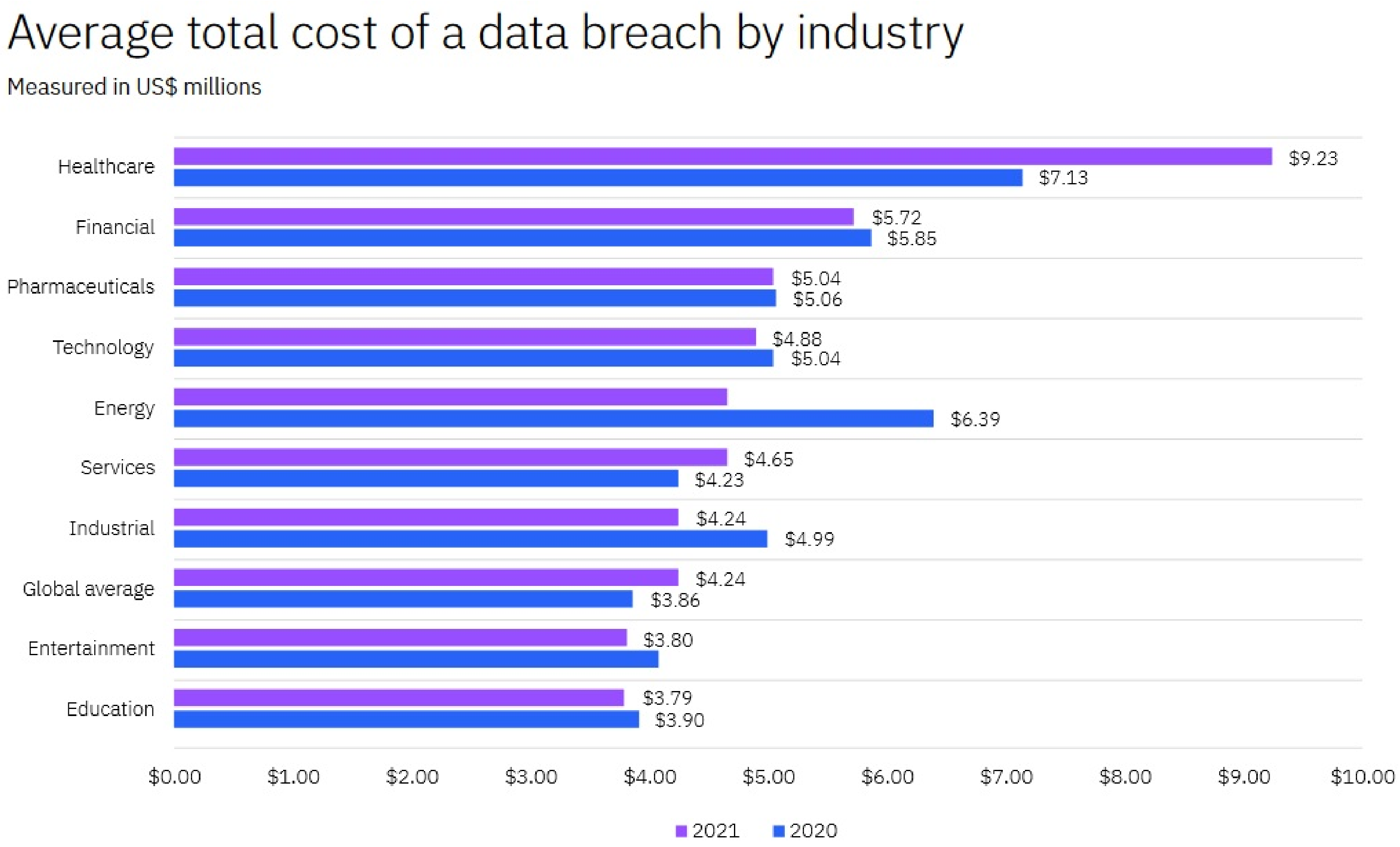
Why EMRs/EHRs Are Valuable to Cyber Attackers

EMR/EHRs are valuable to cyber attackers because of the Protected Health Information (PHI) it contains and the profit they can make on the dark web or black market. These 18 identifiers provide criminals with more information than any other breached record. Extortion, fraud, identity theft, data laundering, Hacktivist / Promoting Political Agenda and Sabotage are some ways cyber attackers use this data for profit.

HIPAA Protected Health Identifiers (PHI)		
Names	Dates, except year	Telephone numbers
Geographic data	FAX numbers	Social Security numbers
Email addresses	Medical record numbers	Account numbers
Health plan beneficiary numbers	Certificate/license numbers	Vehicle identifiers and serial numbers including license plates
Web URLs	Device identifiers and serial numbers	Internet protocol (IP) addresses
Full face photos and comparable images	Biometric identifiers (i.e. retinal scan, fingerprints)	Any unique identifying number or code

Why EMRs/EHRs Are Valuable to Cyber Attackers, Part II

According to IBM, stolen healthcare data is the most valuable, as the graph below shows:



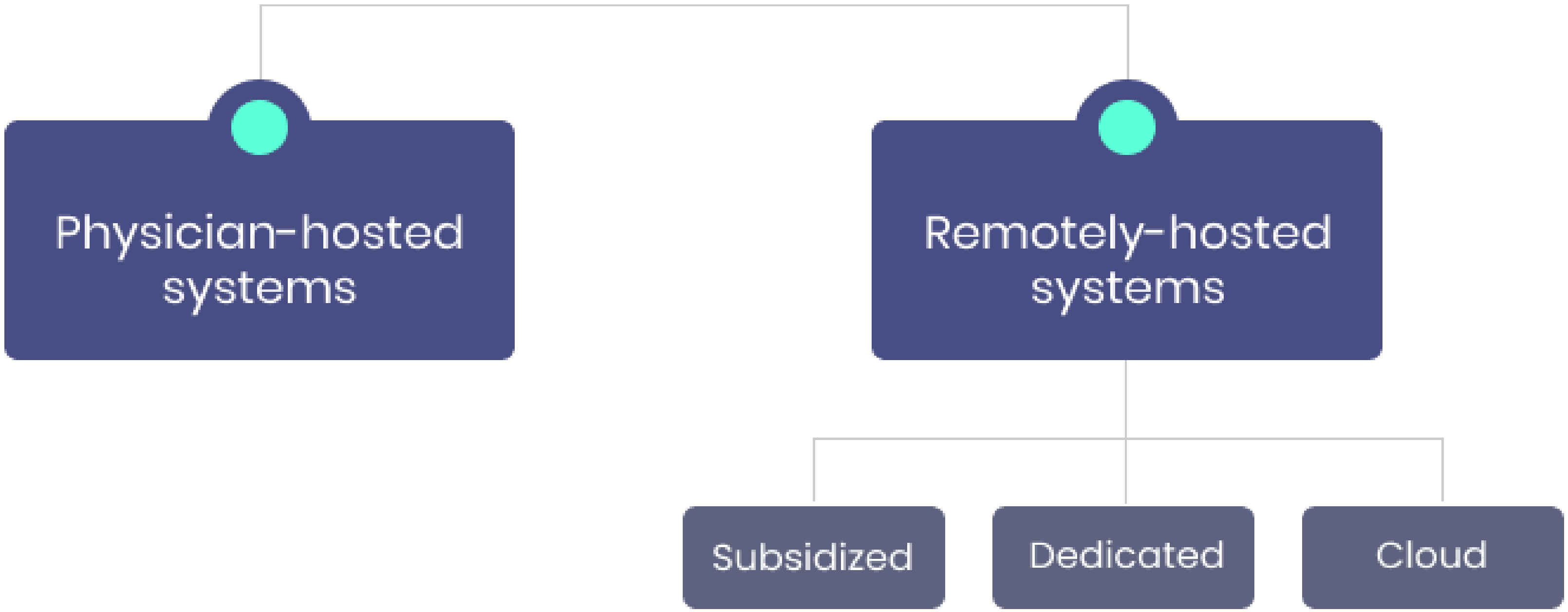
Average total cost of a data breach by industry

Measured in US$ millions

How EMRs/EHRs Are Stored and Handled

EMR / EHR data is stored on dedicated servers in specific, known physical locations.

Types of EHR & EMR systems by deployment



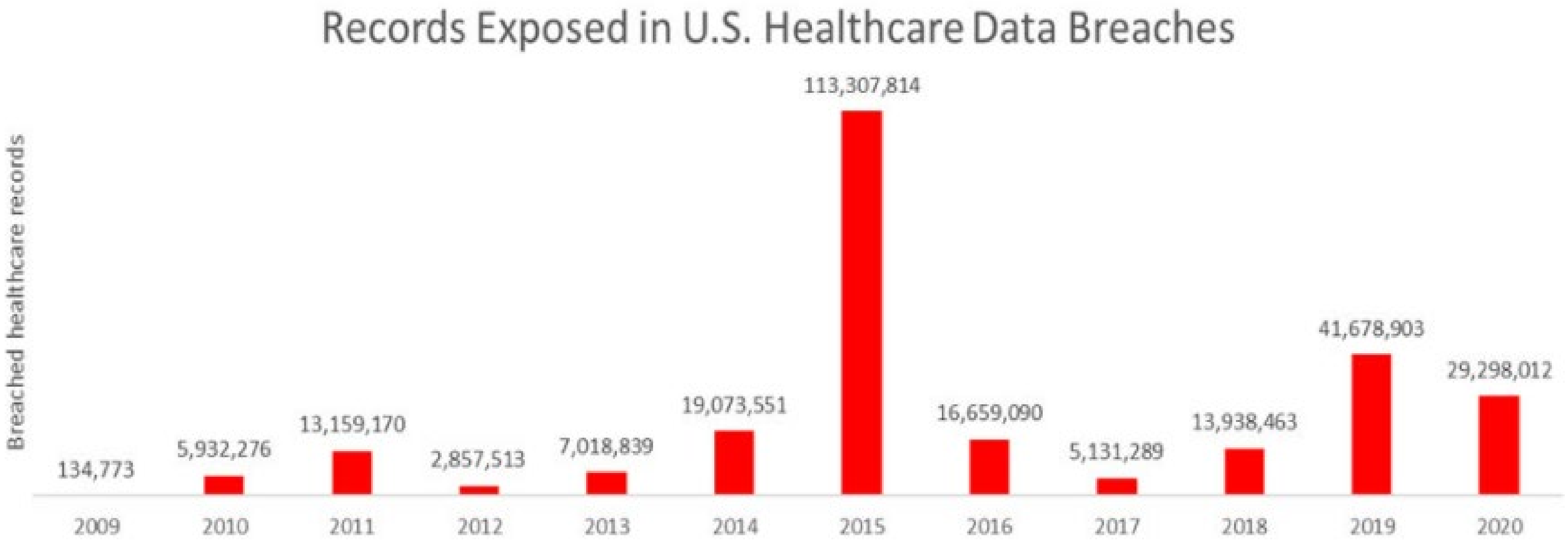
EMR Compromised, Healthcare & Critical Industries Hacked

In 2020, at least 2,354 U.S. government, healthcare facilities and schools were impacted by a significant increase in ransomware. The cyber attacks caused significant disruption across the healthcare industry. Organizations impacted by these attacks are as follows:

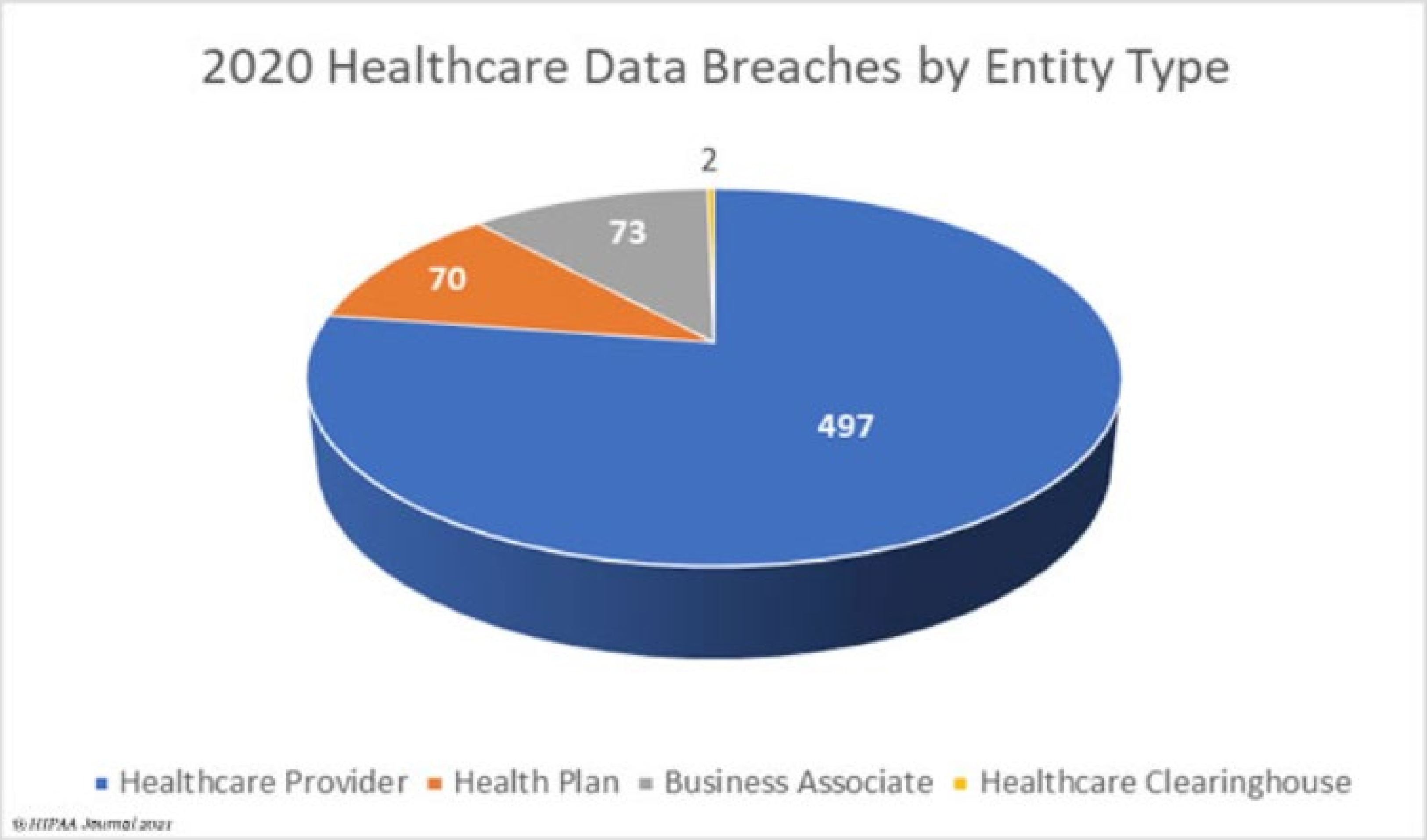
- 113 federal, state and municipal governments and agencies
- 1,681 schools, colleges and universities
- 560 healthcare facilities
- Pennsylvania Health Services Company (operates 400 hospitals & healthcare facilities)

Healthcare Industry Under Attack

Healthcare data breaches have increased significantly. According to the HIPAA Journal's 2020 Healthcare Data Breach Report, the healthcare industry in 2020 had the third largest number of data breaches on record since 2009.



Entities With the Most Data Breaches (per HIPAA Journal):



Top Data Breaches of 2021

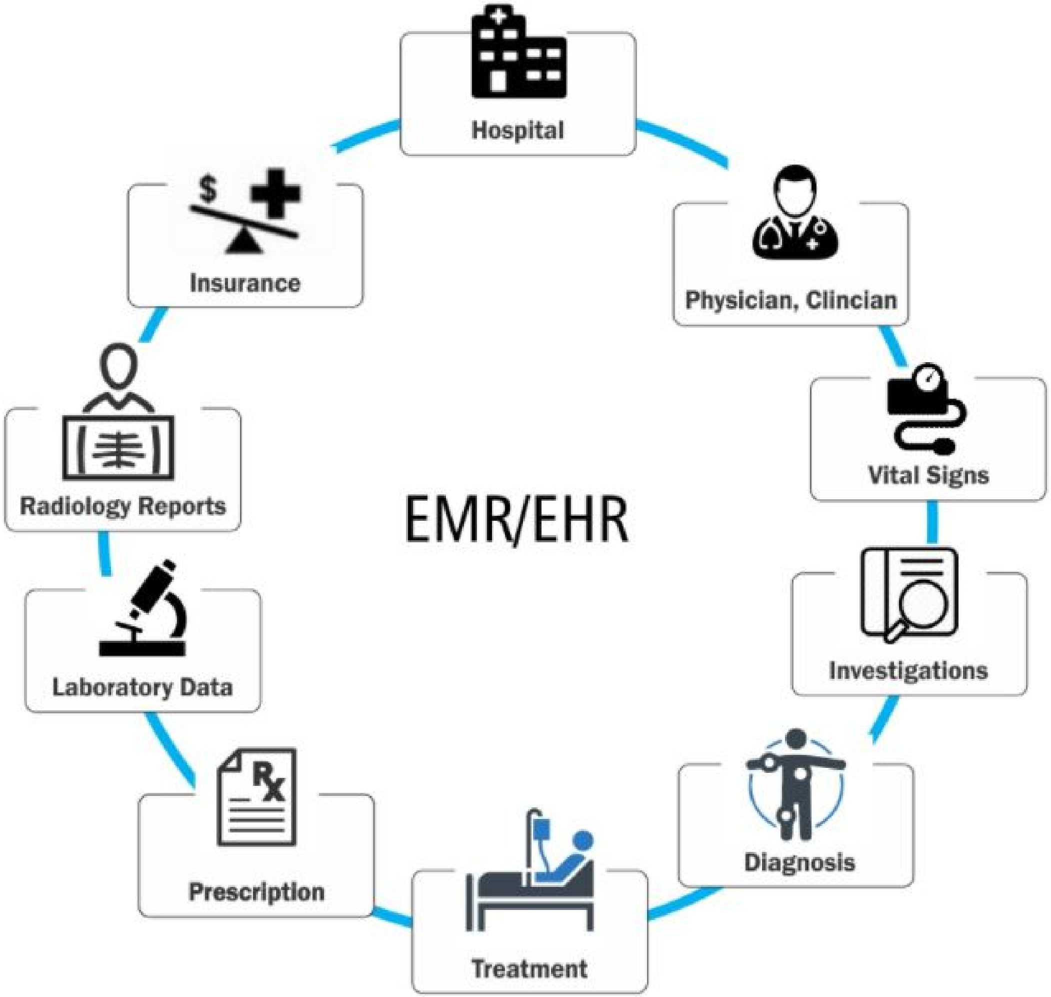
In 2021, HHS received reports of data breaches from 578 healthcare organizations, impacting more than 41.45 million individuals. The following list is of organizations with the most individuals affected in 2021:

- Florida Pediatric Health Pediatric Organization: 3.5 million
- Florida Vision Care Provider: 3.25 million
- Wisconsin Dermatologist: 2.41 million
- Texas Health Network: 1.66 million
- Indiana General Health Provider: 1.52 million
- Ohio Pharmacy Network: 1.47 million
- Georgia Health Network: 1.4 million
- Nevada University Health Center: 1.3 million
- New York Anesthesiologist: 1.27 million
- New York Medical Management Solutions Provider: 1.21 million

In January 2022, 38 organizations reported nearly 2 million individuals were impacted by data breaches.

Top Threats Against Electronic Medical & Health Records

- Phishing Attacks
- Malware & Ransomware Attacks
- Encryption Blind Spots
- Cloud Threats
- Employees

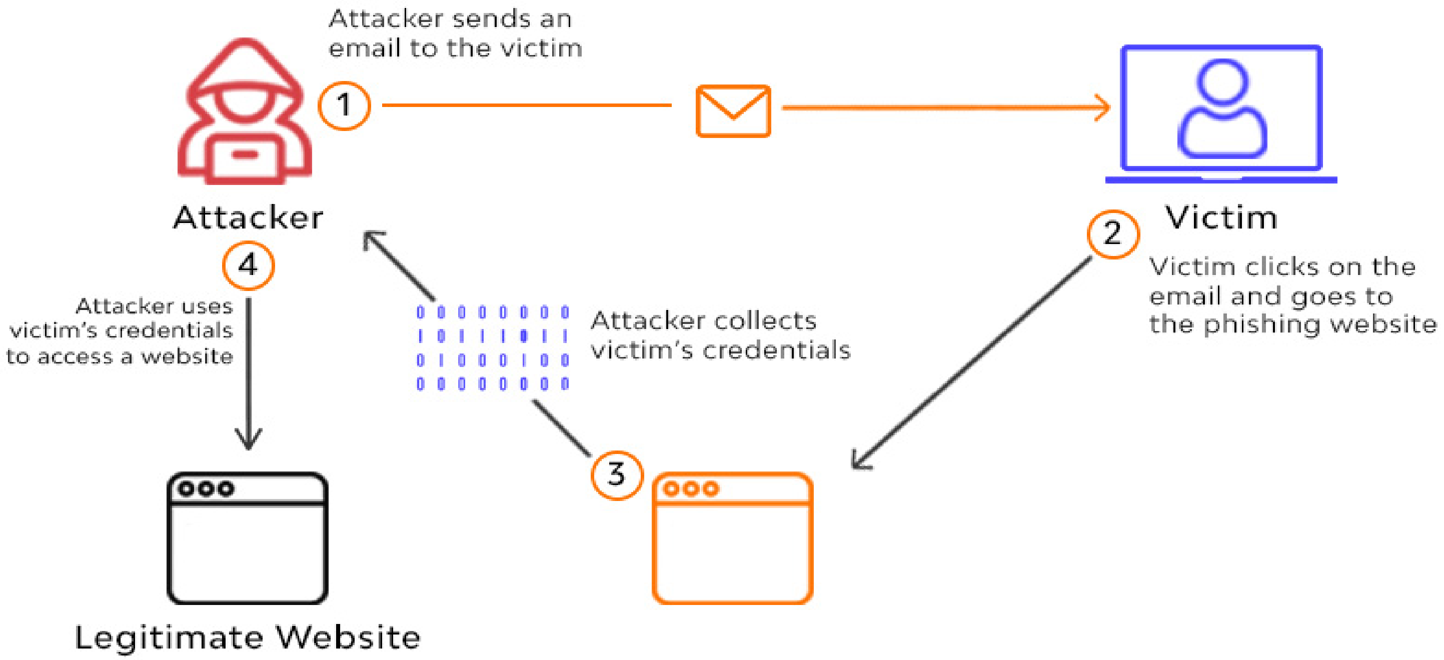


Phishing Attacks

A phishing attack is a type of social engineering attack where the threat actor pretends to be a trusted source and tricks their target into opening an email or clicking a link, revealing their login credentials and depositing malware.

You can protect EMRs/EHRs by doing the following:

- Educate healthcare professionals
- Do not click links within an email that do not match, or has a TLD associated with suspicious sites
- Physicians should verify all EHR file-share requests before sending any data



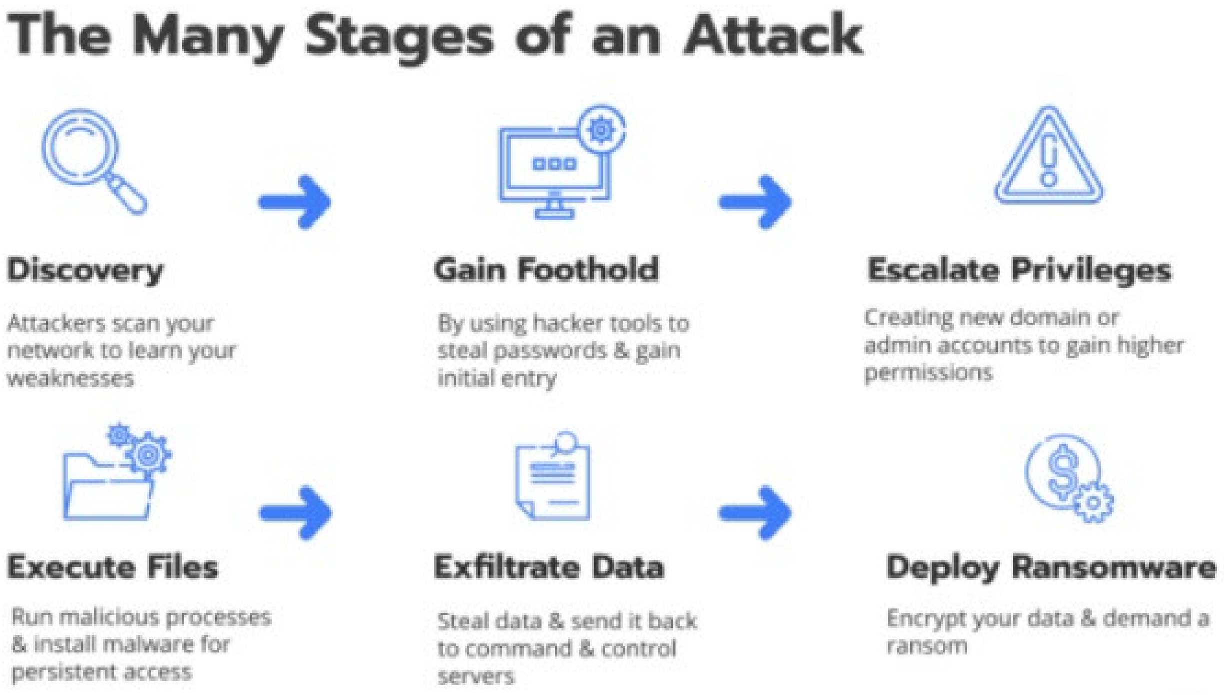
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

Malware and Ransomware Attacks

Malware enters a healthcare system's computer network through software vulnerabilities, encrypted traffic, downloads, and phishing attacks. The effect of each type of malware attack ranges from data theft to harming host computers and networks.

Ransomware is a type of malware that locks users out of their network system or computer until the threat actor or hacker who launched the attack is paid for regained access to data, information, and files.

This could be dangerous for hospitals, healthcare facilities, and others who rely on EHRs or EMRs for up-to-date information to provide patient care.



The Many Stages of an Attack

Discovery

Attackers scan your network to learn your weaknesses

Gain Foothold

By using hacker tools to steal passwords & gain initial entry

Escalate Privileges

Creating new domain or admin accounts to gain higher permissions

Execute Files

Run malicious processes & install malware for persistent access

Exfiltrate Data

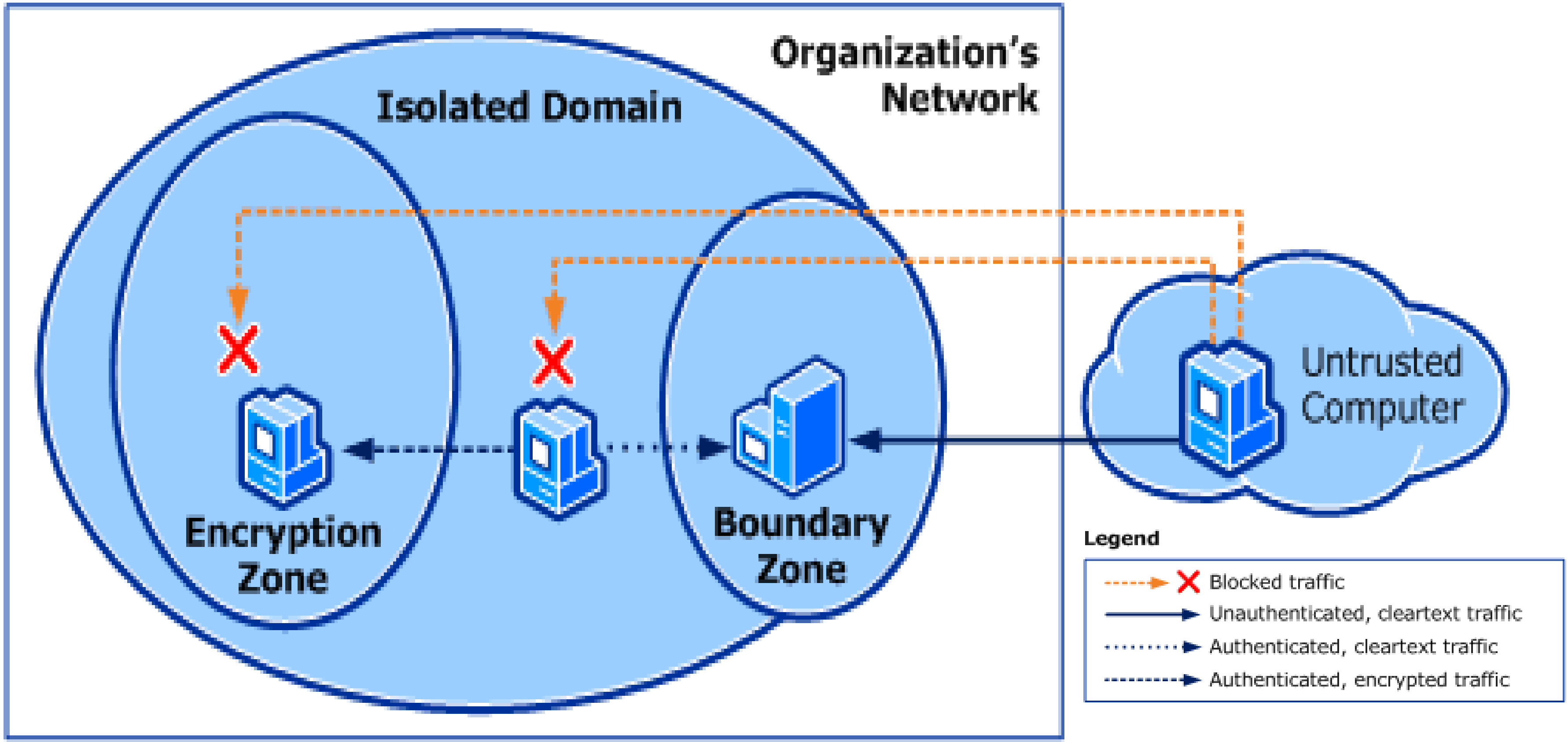
Steal data & send it back to command & control servers

Deploy Ransomware

Encrypt your data & demand a ransom

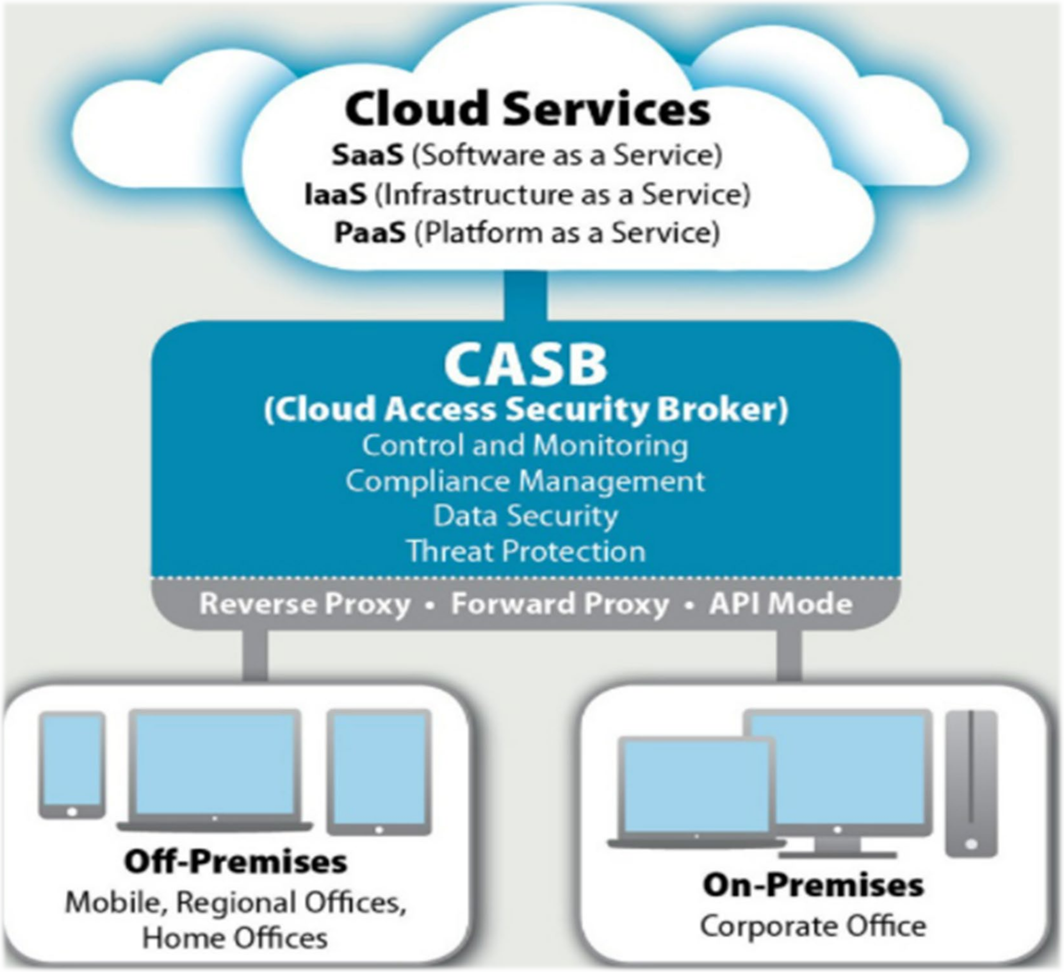
Encryption Blind Spots

Data encryption protects and secures EMR/EHR data while it is being transferred between on-site users and external cloud applications. Blind spots in encrypted traffic could pose a threat to IT healthcare because threat actors or hackers are able to use encrypted blind spots to avoid detection, hide, and execute their targeted attack. Also helps with HIPAA, FISMA, and Sarbanes-Oxley Act of 2002 compliance.



Cloud Threats

More healthcare organizations are using Cloud services to improve patient care, so there is an increasing need to keep private data secure while complying with HIPAA.


Cloud Services
SaaS (Software as a Service)
IaaS (Infrastructure as a Service)
PaaS (Platform as a Service)
CASB
(Cloud Access Security Broker)
Control and Monitoring
Compliance Management
Data Security
Threat Protection
Reverse Proxy • Forward Proxy • API Mode
Off-Premises
Mobile, Regional Offices, Home Offices
On-Premises
Corporate Office

Employees: Insider Threats

Insider threats apply across industries, including the heath sector. It is recommended that your healthcare organization has a cybersecurity strategy and policy that’s not only understood but followed and enforced. An effective strategy involves:

- Educating all healthcare partners and staff
- Enhancing administrative controls
- Monitoring physical and system access
- Creating workstation usage policies
    - Auditing and monitoring system users
    - Employing device and media controls
    - Applying data encryption

Costs of Data Breach

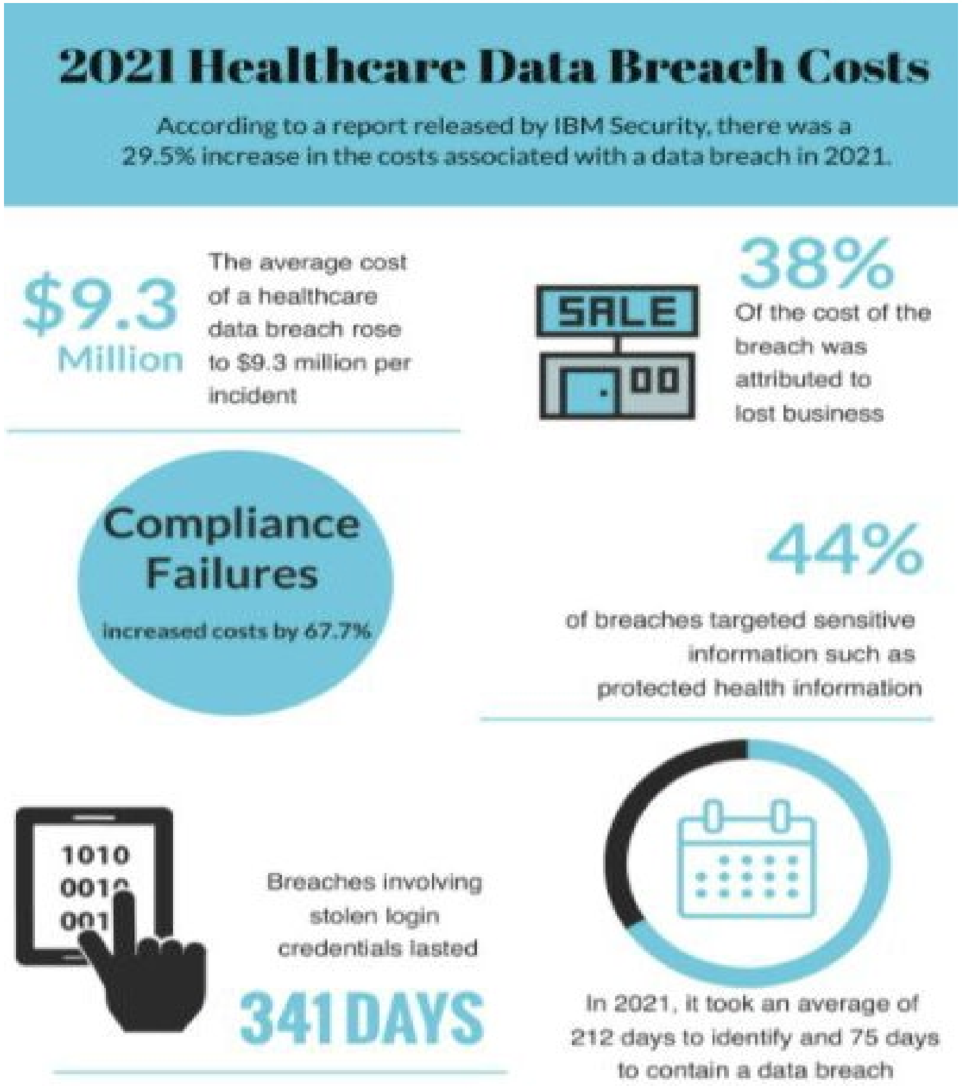
Data breaches targeting EMRs/EHRs have been costly for the healthcare industry. According to IBM, the average cost per incident in 2021 was $9.3 million, and there were 40 million patient records compromised. HIPAA developed four tiers of penalties for failure to protect PHI:

First Tier: $100-$50K per incident (up to $1.5M)

Second Tier: $1,000-$50K (up to $1.5M)

Third Tier: $10,000-$50,000 (up to $1.5M) per incident

Fourth Tier: at least $50,000 (up to $1.5M) per incident



2021 Healthcare Data Breach Costs

According to a report released by IBM Security, there was a 29.5% increase in the costs associated with a data breach in 2021.

$9.3 Million

The average cost of a healthcare data breach rose to $9.3 million per incident

38%

Of the cost of the breach was attributed to lost business

Compliance Failures

increased costs by 67.7%

44%

of breaches targeted sensitive information such as protected health information

Breaches involving stolen login credentials lasted

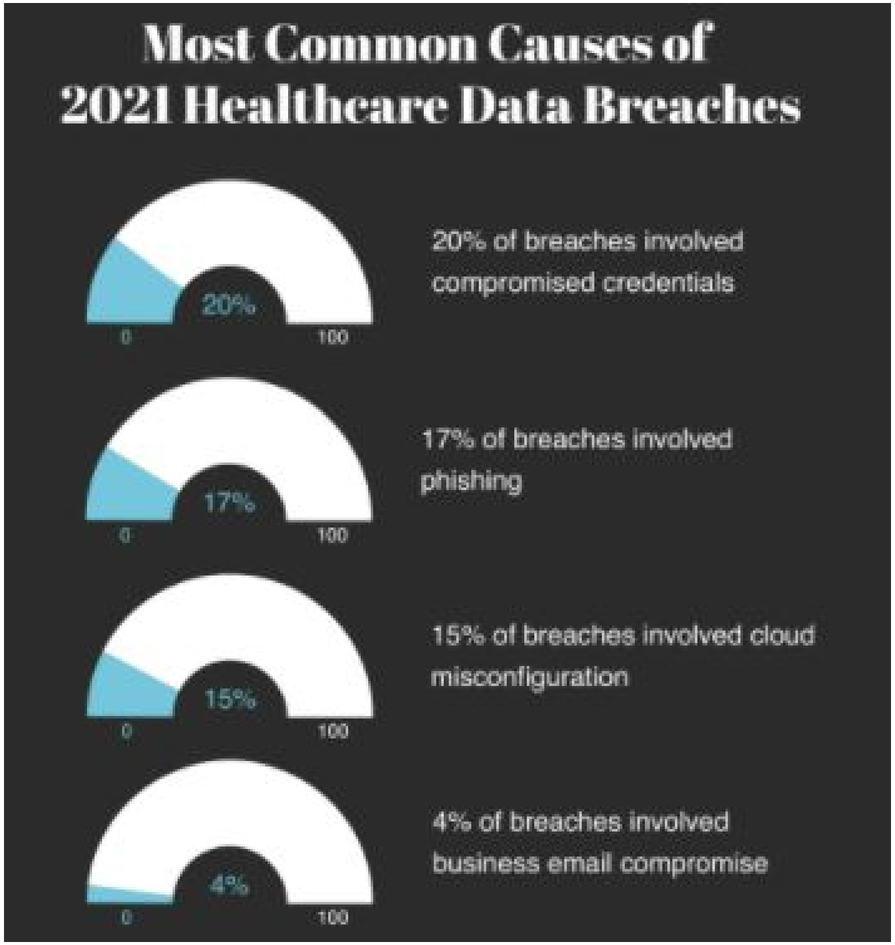
341 DAYS

In 2021, it took an average of 212 days to identify and 75 days to contain a data breach

Protecting EMR & EHR Data

Here are a few strategies that healthcare leaders should consider to strengthen their organization’s cyber posture:

- Evaluate risk before an attack
- Use VPN with multifactor authentication (MFA)
- Develop an endpoint hardening strategy
- Endpoint Detection and Response (EDR)
- Protect emails and patient health records
- Engage Cyber Threat Hunters
- Conduct red team / blue team exercises
- Moving beyond prevention



Most Common Causes of 2021 Healthcare Data Breaches

20% of breaches involved compromised credentials

17% of breaches involved phishing

15% of breaches involved cloud misconfiguration

4% of breaches involved business email compromise

Protecting EMR & EHR Data – Evaluate Risk Before an Attack

Healthcare leaders should understand where operational vulnerabilities exist in their organization, from marketing all the way down to critical health records. By understanding the scope of the task at hand, management and other healthcare leaders can create a preparedness plan to address any weaknesses in digital infrastructure.

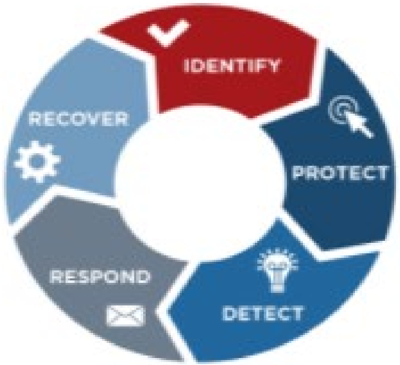
1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity



2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

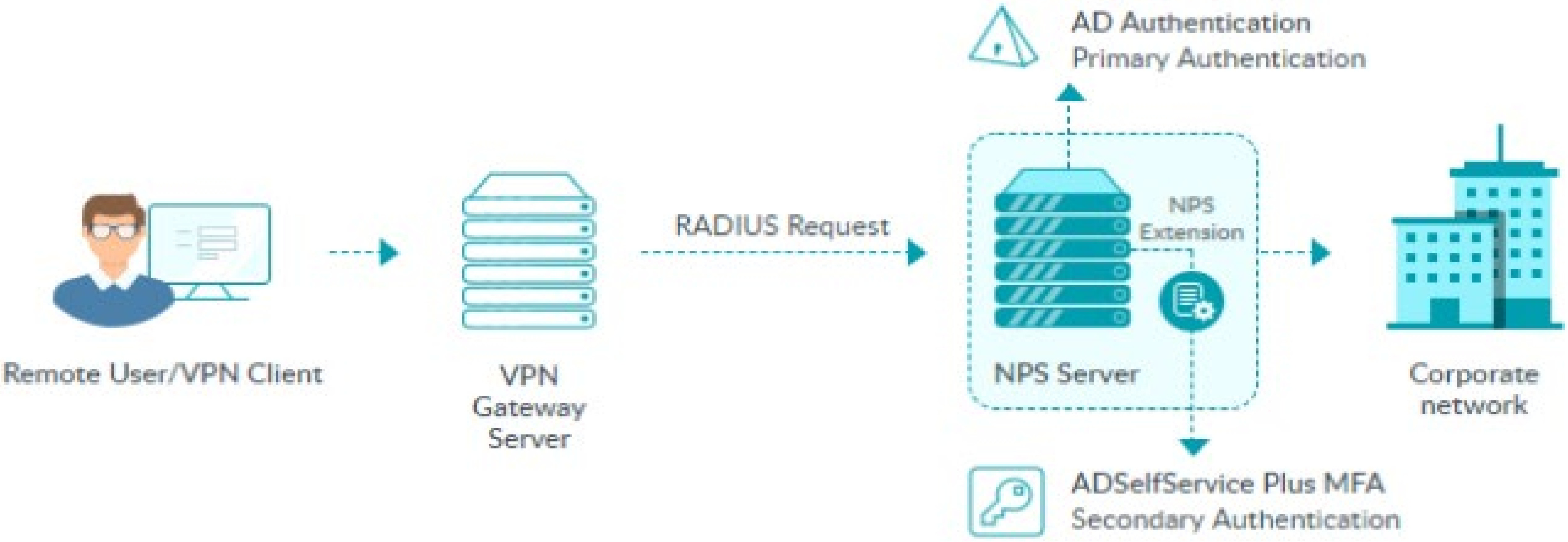
Consider cyber insurance

Make improvements to processes/ procedures/ technologies

Protecting EMR & EHR Data – Use VPN with MFA

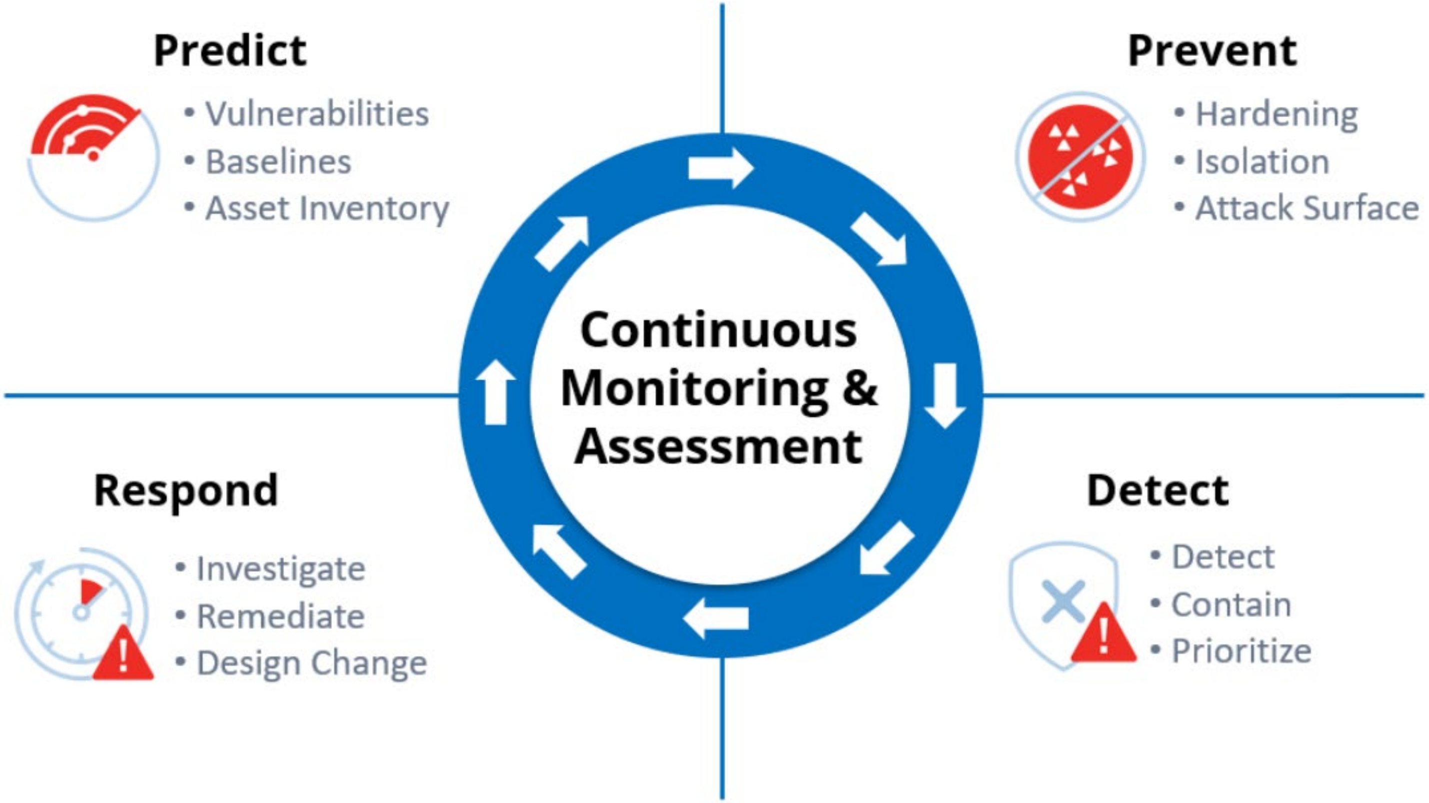
Leaders in the healthcare industry should consider developing a strategy to combat ransomware that targets Remote Desktop Protocol (RDP) and other applications that face the Internet.

Healthcare leaders should also consider adding a VPN with multifactor authentication to avoid exposing their RDP and prioritize patching for vulnerabilities in VPN platform and other applications.



Protecting EMR & EHR Data – Develop Endpoint Hardening Strategy with EDR

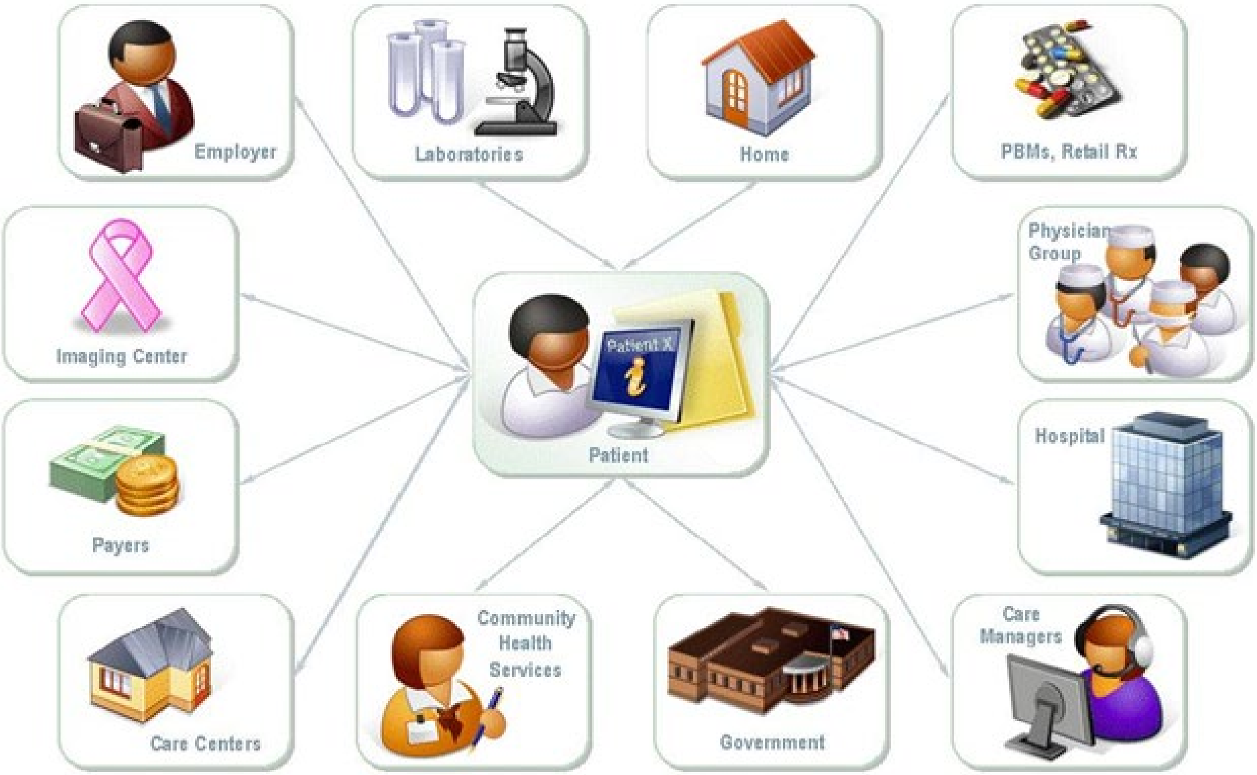
Developing an endpoint hardening strategy allows healthcare leaders the ability to harden their digital infrastructure with multiple defense layers at various endpoints. This strategy also detects and contains an attack before it can reach patient medical records or other sensitive information. Endpoint Detection and Response (EDR) should also be added to detect and mitigate cyber threats.



Protecting EMR & EHR Data – Emails & Patient Health Records

It is imperative that patient health records and emails are protected. In addition to threat actors using Remote Desktop Protocol (RDP) to gain access, HIVE ransomware attacks malicious files attached to phishing emails to gain access to health records and company systems.

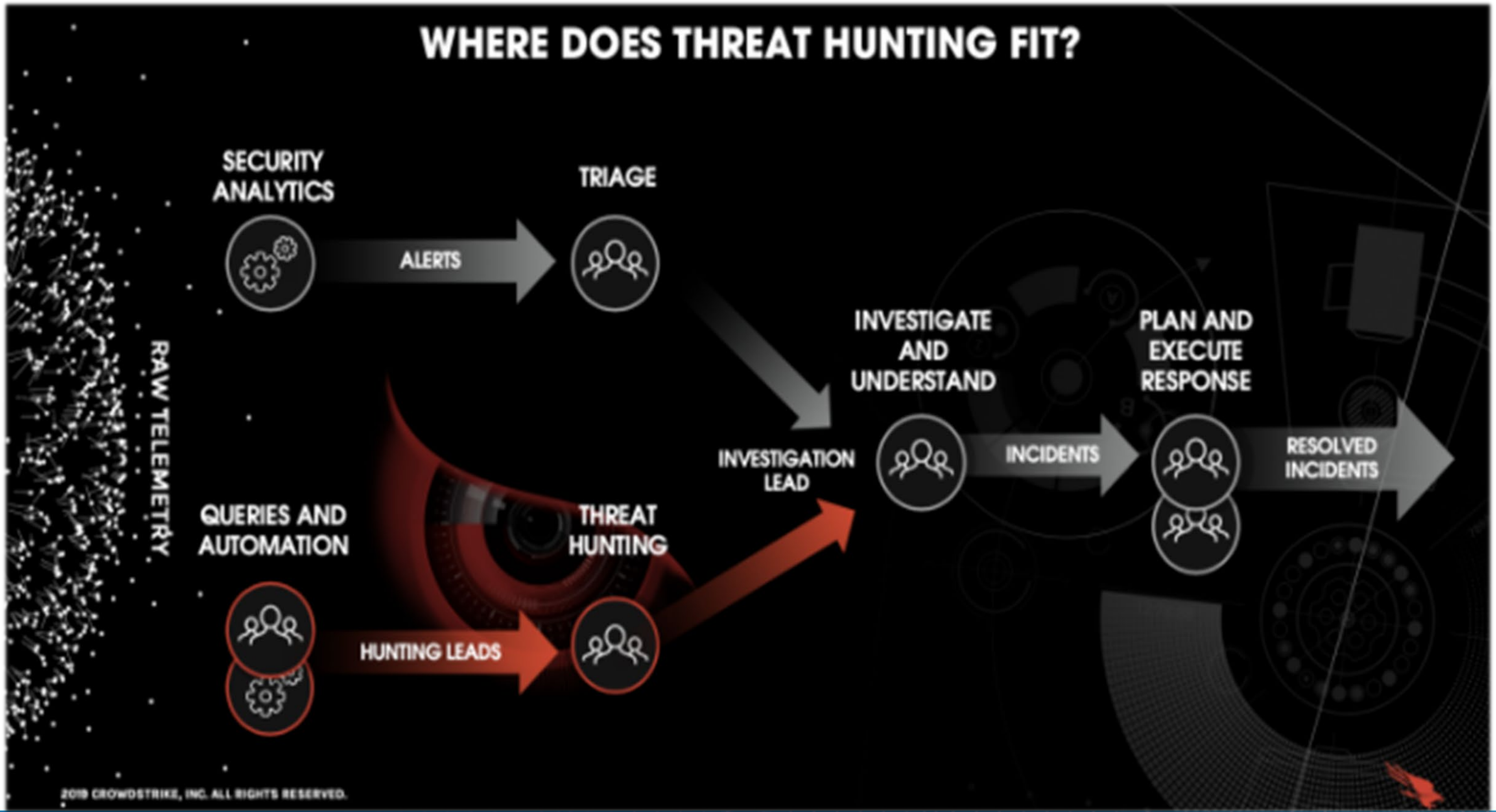
Email security software with URL filtering and attachment sandboxing is recommended as a mitigation strategy.



Protecting EMR & EHR Data – Engage Cyber Threat Hunters

Threat hunting is a proactive practice that finds threat actors or hackers who have infiltrated a network's initial endpoint security defenses.

This type of human threat detection capability operates as an extension of the organization's cyber team that will track, prevent, or even stop potential cyber attacks on an organization.



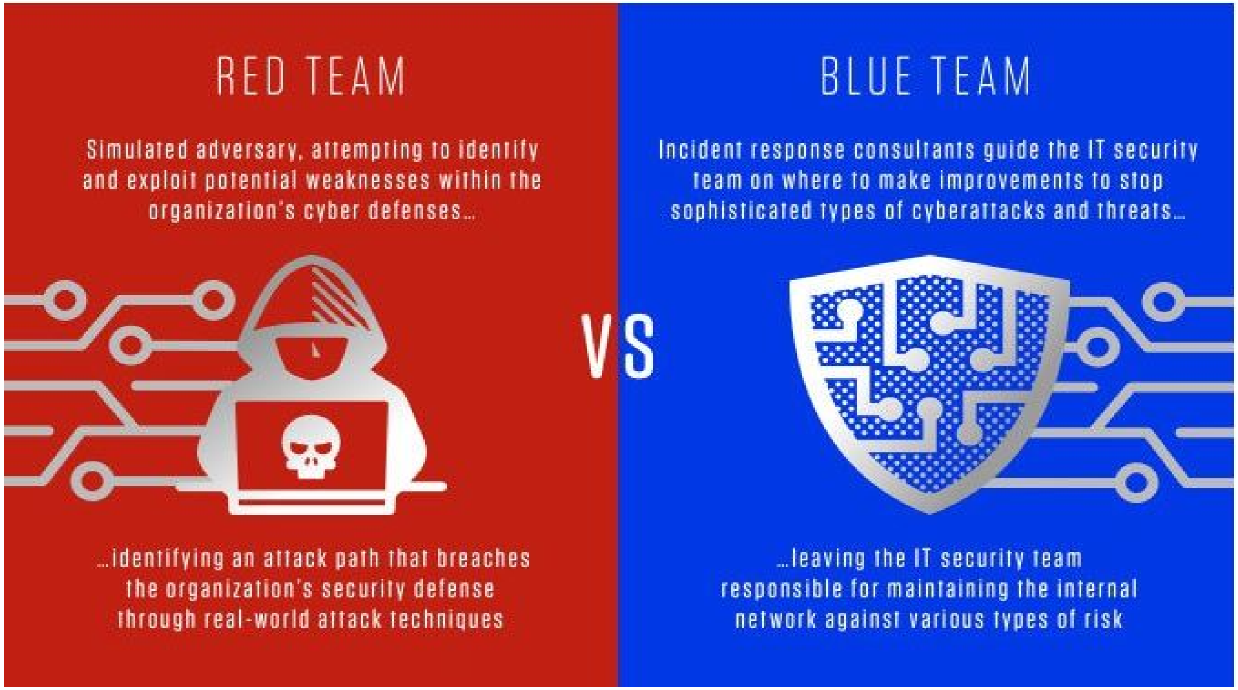
2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

Protecting EMR & EHR Data – Conduct Red Team / Blue Team Exercises

Red and blue team exercises are essentially a face-off between two teams of highly trained cybersecurity professionals:

- ***Red Team*** *uses real-world adversary tradecraft to compromise the environment.*
- ***Blue Team*** *consists of incident responders who work within the security unit to identify, assess and respond to the intrusion.*

These exercises are imperative to understanding issues with an organization's network, vulnerabilities and other possible security gaps.


RED TEAM
Simulated adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses…
…identifying an attack path that breaches the organization's security defense through real-world attack techniques
VS
BLUE TEAM
Incident response consultants guide the IT security team on where to make improvements to stop sophisticated types of cyberattacks and threats…
…leaving the IT security team responsible for maintaining the internal network against various types of risk

Protecting EMR & EHR Data – Moving Beyond Prevention

It is recommended that healthcare leaders shift their focus by moving beyond a prevention strategy and creating a proactive preparedness plan.

This helps understand vulnerabilities in the current network landscape and provides guidance needed for framework that will be effective in identifying and preventing attacks, which is key to protecting EMRs/EHRs, along with access to vital patient data.

Reference Materials

References

- Duffin, Sonya. “Top 10 Cybersecurity Best Practices to Combat Ransomware,” Threat Post. November 12, 2021. https://threatpost.com/cybersecurity-best-practices-ransomware/176316/.
- Green, Jeff. “Disadvantages of EHR systems - dispelling your fears,” EHR Knowledge Zone. August 15, 2019. https://www.ehrinpractice.com/ehr-system-disadvantages.html.
- “What are the Consequences of a Medical Record Breach,” American Retrieval. September 22,2020. https://www.americanretrieval.com/medical-records-breach.
- O’Connor, Stephen. “Top 5 Risks You May Encounter After an EHR Software Implementation,” Advanced Data Systems Corruption. January 31, 2017. https://www.adsc.com/blog/top-5-risks-you-may-encounter-after-an-ehr-software-implementation.
- Marchesini,Kathryn;Massihi, Ali. “4 Ways Using the HHS Security Risk Assessment Tool Can Help Your Organization,” Health IT Buzz. October 30, 2019. https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/4-ways-using-the-hhs-security-risk-assessment-tool-can-help-your-organization.
- “2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020,” HIPAA Journal. January 19, 2021. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.
- “Programs/Electronic Medical Records(EMR),” MedixOnline. May 21, 2021. https://medixonline.ca/programs/electronic-medical-records-emr/.
- Luyer, Eric M. “Cybersecurity Risks in Medical Devices Are Real,” MedTech Intelligence. February 23, 2017. https://www.medtechintelligence.com/feature_article/cybersecurity-risks-medical-devices-real/.
- Cepero, Robert. “How Hospitals Can Protect Their EMR Data,” Bleuwire. December 16, 2020. https://bleuwire.com/how-hospitals-can-protect-their-emr-data/.

References

- Cepero, Robert. “How Hospitals Can Protect Their EMR Data,” Bleuwire. December 16, 2020. https://bleuwire.com/how-hospitals-can-protect-their-emr-data/.
- Vaidya, Anuja.“5 ways U.S. hospitals can protect against ‘imminent’ ransomware threat,” MedCityNews. October 29, 2020. https://medcitynews.com/2020/10/5-ways-u-s-hospitals-can-protect-against-imminent-ransomware-threat/.
- “Understanding EMR vs. EHR,” NextGen Healthcare. July 19, 2019. https://nextgen.com/insights/emr-vs-ehr/emr-vs-ehr.
- “Why is PHI Valuable to Criminals?,” Compliancy Group. November 16, 2020. https://compliancy-group.com/why-is-phi-valuable-to-criminals/.
- Taylor, Tori. “Hackers, Breaches, and the Value of Healthcare Data.” December 8, 2021. https://www.securelink.com/blog/healthcare-data-new-prize-hackers/.
- Adams, Katie. “10 Biggest Patient Data Breaches in 2021,”Becker Hospital Review. December 7,2021. https://www.beckershospitalreview.com/cybersecurity/10-biggest-patient-data-breaches-in-2021.html.
- “Costs of a Data Breach Report 2021,” IBM Security. July 28, 2021.

https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=Healthcare%20organizations%20experienced%20the%20highest,industries%2C%20and%20year%20over%20year.

- Deford, Drex. “Under Siege: How Healthcare Organizations Can Fight Back,” CPO Magazine. November 25,2021. https://www.cpomagazine.com/cyber-security/under-siege-how-healthcare-organizations-can-fight-back/.
- Kumar, S.Rakesh, Gayathri,N. Muthuramalingam,S., Balamurugan, B, Ramesh,C., Nallakaruppan, M.K. “Medical Big Data Mining and Processing in e-Healthcare,” Internet of Things in BioMedical Engineering. November 1,2019. https://www.sciencedirect.com/topics/engineering/electronic-health-record .

References

- “What Is An EMR? About EMR Systems - Electronic Medical Records,” Healthcare IT Skills. January 5, 2020. https://healthcareitskills.com/what-is-an-emr-ehr/.
- “The 10 Most Common Inpatient EHR Systems by 2021 Market Share,” Definitive Healthcare

  https://www.mdhinsight.com/services/emr-data-extraction.
- Zelinska, Solomija. “Which Types of EMR/EHR Systems are the Best for Your Business,”Empeek. March 5, 2021. https://empeek.com/which-types-of-emr-ehr-systems-are-the-best-for-your-business/ .

Questions

Questions

Upcoming Briefs

- 3/3 – Healthcare Cybersecurity: 2021 Year-in-Review / A Look Forward to 2022

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV