Healthcare Technology Security

September 19, 2024

TLP:CLEAR, ID:202409191300

Agenda

The health sector must protect universal technologies, as well as industry-specific technologies, from exploitation to remain properly secure.

- Concepts and Definitions
- Technologies
  - PACS
  - DICOM
  - Medical devices
    - Insulin pumps
    - Pneumatic tubes
  - Electronic health records
  - Artificial intelligence
- Defense and mitigation
- Conclusion

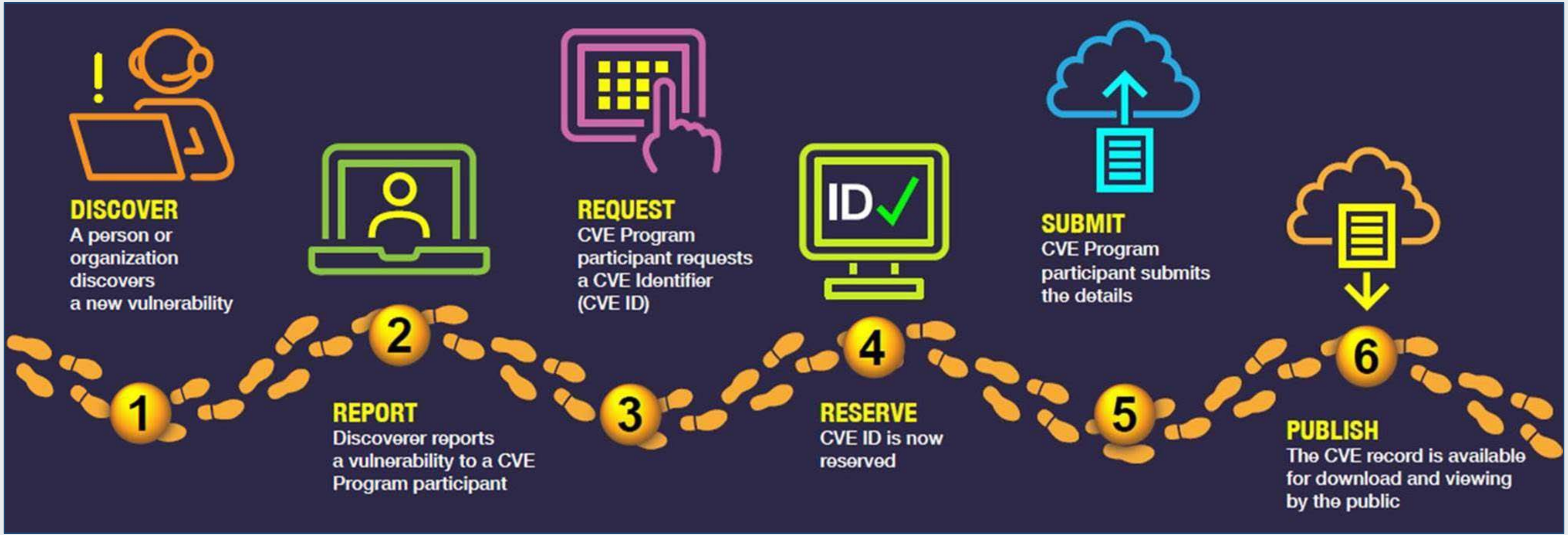
Slides Key:

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

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

CVE Programs

The Common Vulnerabilities and Exposures (CVE) program serves to identify and catalog cybersecurity vulnerabilities across industries. The process is as follows:



1 **DISCOVER** A person or organization discovers a new vulnerability

2 **REPORT** Discoverer reports a vulnerability to a CVE Program participant

3 **REQUEST** CVE Program participant requests a CVE Identifier (CVE ID)

4 **RESERVE** CVE ID is now reserved

5 **SUBMIT** CVE Program participant submits the details

6 **PUBLISH** The CVE record is available for download and viewing by the public

Image source: CVE.org

For more information: https://www.cve.org/About/Process

Concepts and Definitions

More on vulnerabilities…

Vulnerability: A weakness or flaw in a system, network or application that can be exploited by malicious actors in a way that was not intended by those that designed it, exploited to take actions that cause undesirable consequences.

Zero-day vulnerability: A vulnerability that is unknown to the vendor, which implies that no mitigation actions or patches are in the process of being developed.

One-day vulnerability: A known vulnerability for which a patch or mitigation is available but has not yet been applied. The “one day” term refers to the period between when the vulnerability is disclosed and when affected systems are patched.

N-day vulnerability: Similar to a one-day vulnerability (see above), however more than a single day may have passed since the vulnerability disclosure without a patch being released.

This presentation is vulnerability-centric, but all healthcare organizations are strongly urged to pay close attention to other cyberattack vectors, including tactics such as phishing and compromise of legitimate remote-access tools.

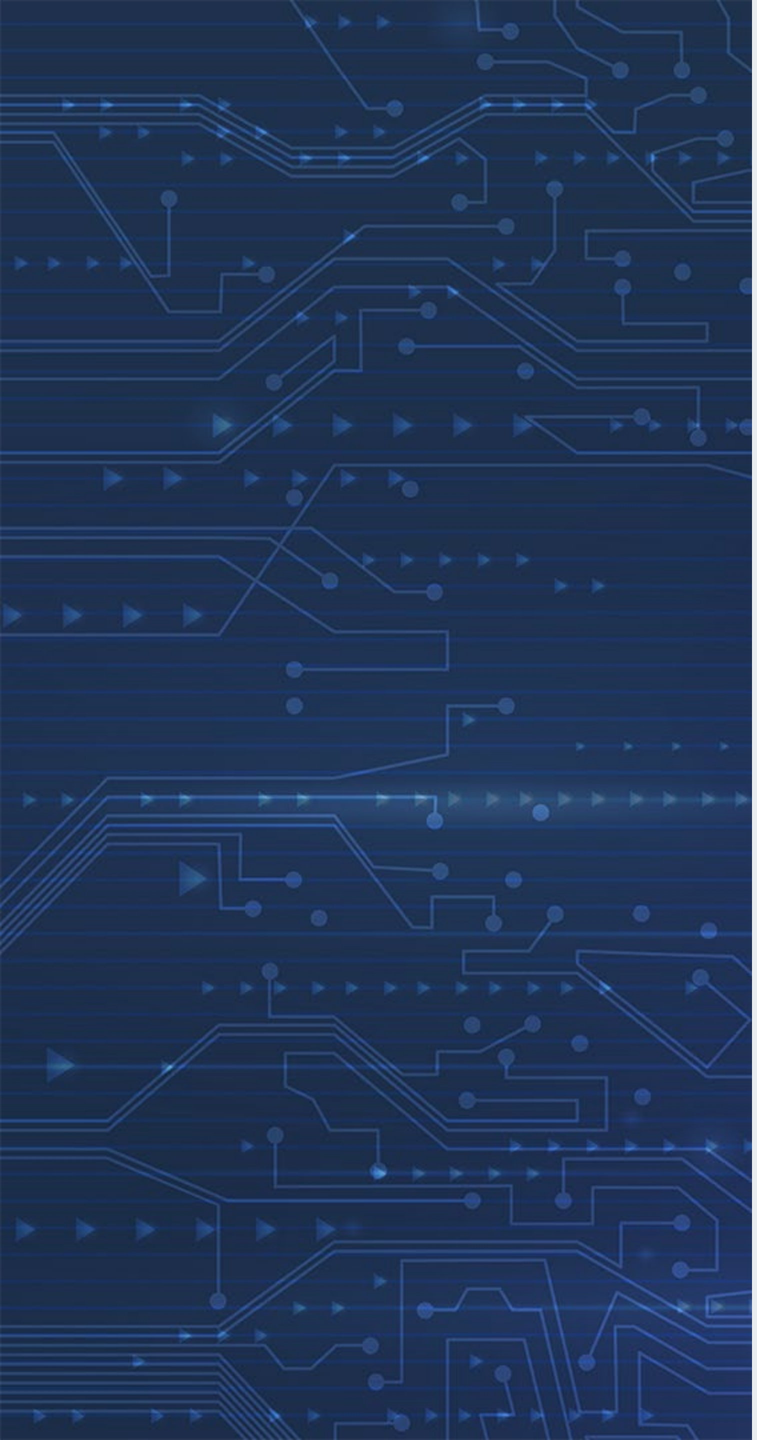
Concepts and Definitions, cont.

Attack surface: The totality of all components of a network that are vulnerable to cyberattack. Attack surface refers to the degree to which a particular piece of infrastructure can be compromised. It is an aggregate measurement of weakness, but the weakest-link theory also applies. It can factor areas of an enterprise, such as physical access points, network interfaces, software and operating systems, remote access and user training.

Time-to-patch: This refers to the duration between the time a vulnerability is discovered by anyone and the moment it becomes fully patched on a system. There are many contingencies that can factor into the time-to-patch such as:

- Which individuals or group discovers the vulnerability
- The vendor’s knowledge of the vulnerability
- The vendor’s willingness to patch the vulnerability
- The priority the vendor gives the vulnerability
- The priority the enterprise gives the vulnerability
- The capability of the vulnerability management program

> “Leadership at all levels of the organization, business/mission owners, and security/technology management teams should jointly create an enterprise patch management strategy that simplifies and operationalizes patching while also improving its reduction of risk. This will strengthen organizational resiliency to active threats and minimize business and mission impacts.” – National Institute of Standards and Technology, SP 800-40 revision 4



PACS Security

Picture Archiving and Communication Systems (PACS) are used to store, retrieve and view medical images, making them enticing targets for cyberattackers

PACS Security

PACS systems consist of:

- Servers
- Workstations
- Storage technologies
- Imaging modalities (X-Ray, MRI, CTI)

PACS systems are critical for diagnosing, care provision and record-keeping. This makes them especially desirable targets for financially-motivated cybercriminals.

- Ransomware
- Sensitive data leaks

Image courtesy of Medicasoft

PACS Vulnerabilities

Common vulnerabilities in PACS technology:

- Access control weaknesses
  - CVE-2012-6693: GE healthcare Centricity PACS 4.0 has predictable default passwords.
  - CVE-2018-17906: Philips iSite and IntelliSpace PACS have predictable default credentials and lack authentication for third party software.
  - CVE-2013-7442: GE Healthcare Centricity PACS Workstation 4.0 and 4.0.1 have known default passwords.
- Internet-facing data storage (on prem and cloud) exposure
  - CVE-2023-40159: Phillips Vue PACS versions previous to 12.2.8.410 allow for information disclosure due to the deserialization of untrusted data without sufficient verification.
- Software and network weaknesses
  - CVE-2021-33022: Certain versions of Philips Vue PACS transmit sensitive data in cleartext.

PACS Mitigations

We want to highlight the following mitigations for PACS systems:

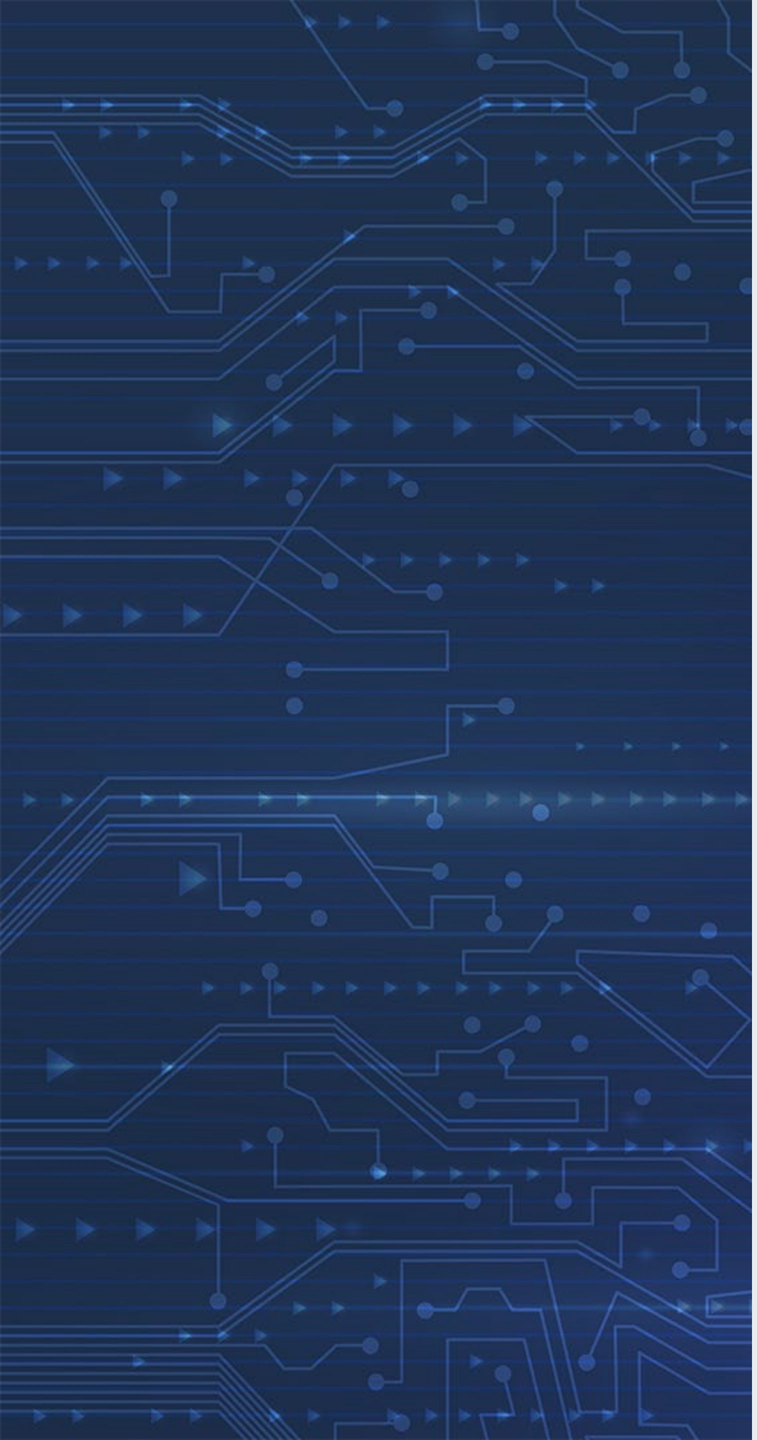
- **Vulnerability management:** Implement a robust, comprehensive and time-sensitive program.
  - Include both CVEs and non-tracked vulnerabilities (**vendor communications is key!**).
- **Data backups:** Iterative, comprehensive, and secure.
  - The 3-2-1 rule is a good place to start.
- **Secure architecture:**
  - Maintain appropriate network segmentation and firewall protection.
  - Isolate sensitive systems.
  - Secure remote access for regular and administrative users (principle of least privilege).
- **Configuration management:** Maintain secure password policy. Replace all default passwords.
- **Endpoint security:** Ensure appropriate coverage and regular updates for security software.

PACS Security Resources

We recommend the following resources for additional information on PACS security:

- Journal of Imaging Informatics in Medicine: "Cybersecurity in PACS and Medical Imaging: an Overview" can be found here.
- National Institute of Standards and Technology (NIST) Securing Picture Archiving and Communication System page can be found here.
  - NIST SP 1800-24: Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector
- HC3 Alert on PACS vulnerabilities can be found here.

Image courtesy of HelpNet Security



DICOM Security

The Digital Imaging and Communications in Medicine (DICOM) standard facilitates the digital storage and transmission of medical images and related information, and is therefore a target for data exfiltration attacks

DICOM Security

DICOM is the global standard for the transmission and storage of medical images.

The first version became available in the 1980s.

DICOM files have a .DCM or .DCM30 extension and ride on TCP/IP.

The official website can be found here.

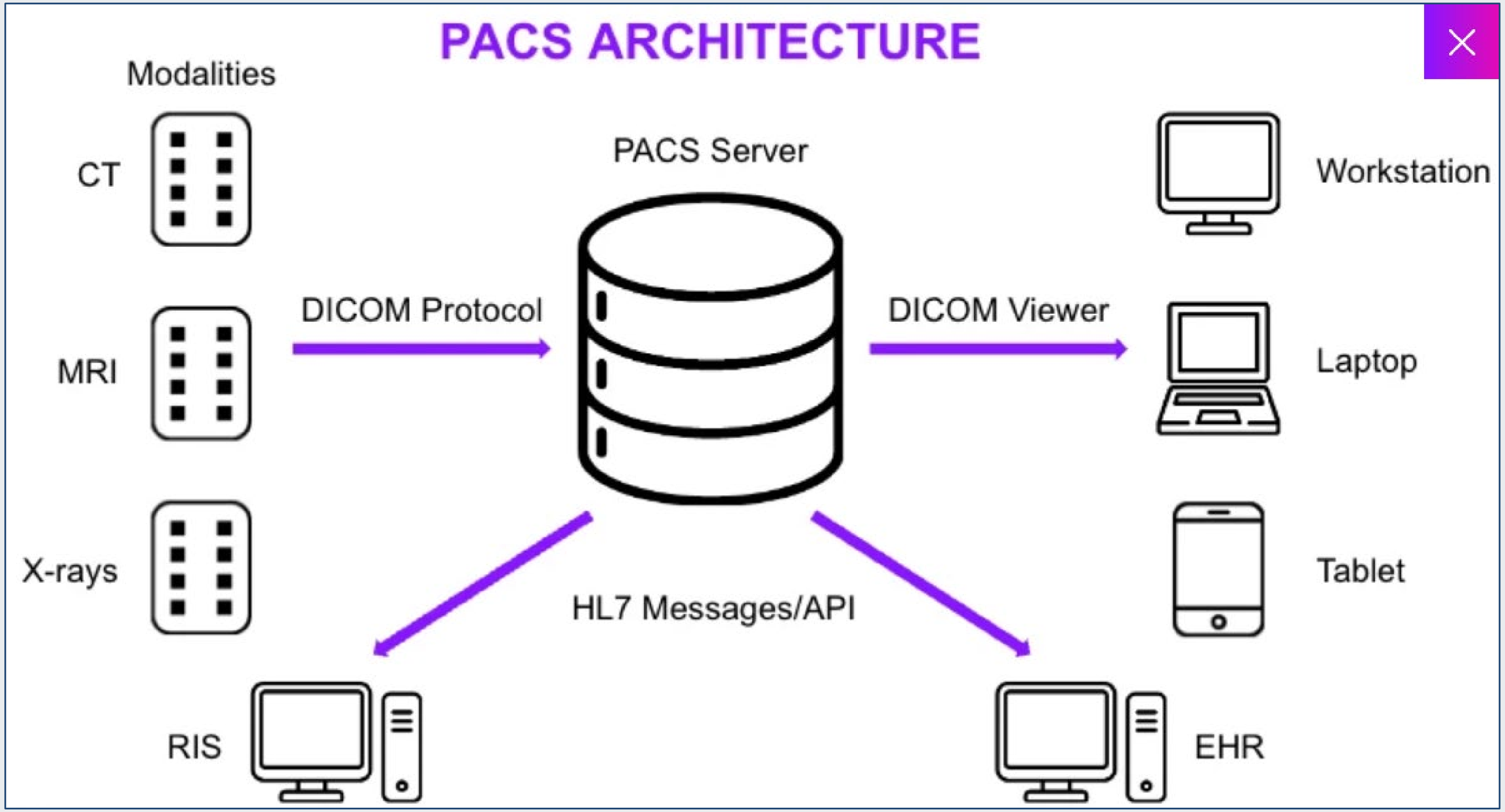


Image courtesy of Claroty

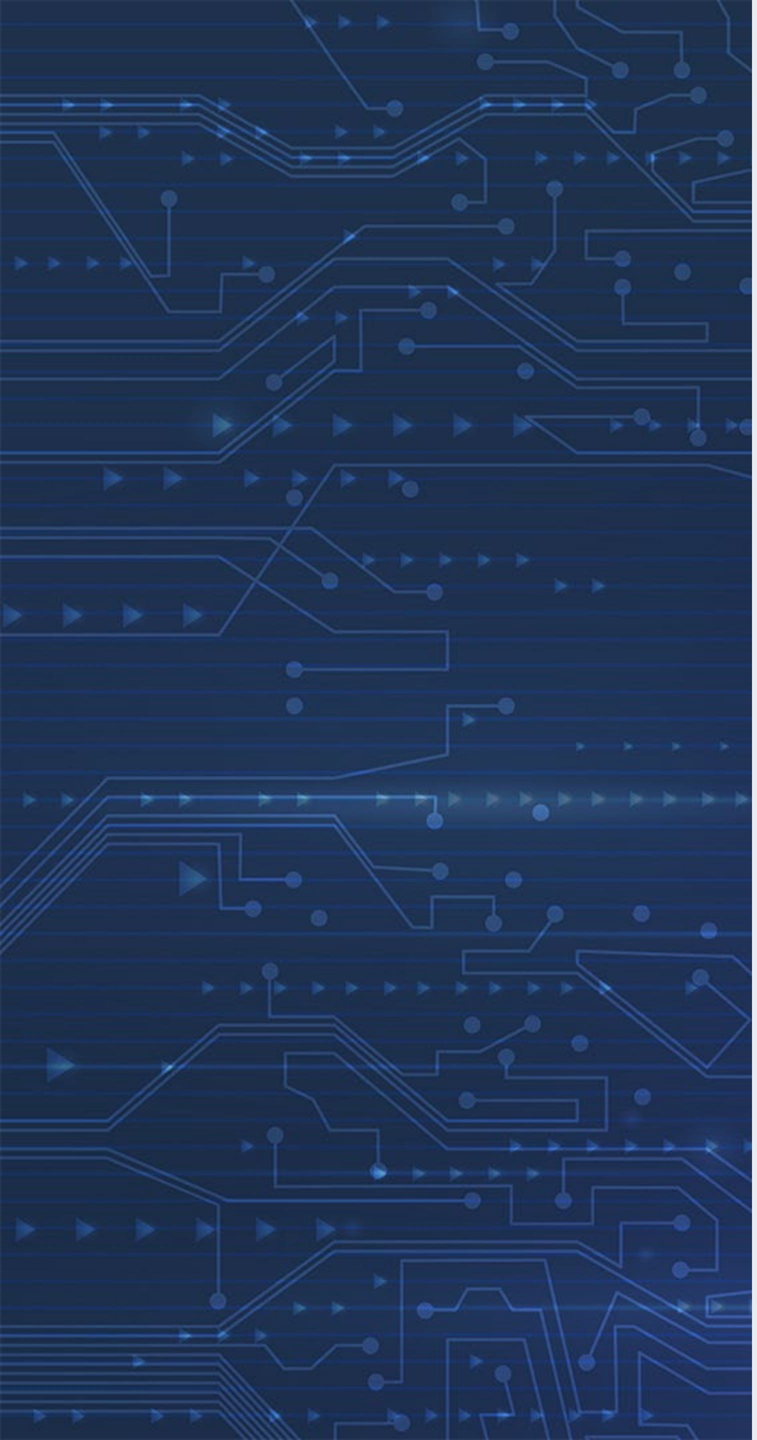
DICOM Security Issues

- What are the potential security issues with DICOM?
  - Issues with specific implementations:
    - CVE-2022-2119: A path traversal vulnerability in all versions prior to 3.6.7 of OFFIS DCMTK's service class provider.
    - CVE-2022-2120: A relative path traversal vulnerability in all versions prior to 3.6.7 of OFFIS DCMTK's service class user.
  - Issues with the protocol:
    - In 2023, a researcher revealed a vulnerability in DICOM’s store service, potentially allowing threat actors to modify or destroy medical images.
      - This vulnerability was identified on more than 3,800 servers across more than 110 countries, exposing the personally identifiable information of over 16 million patients.
        - This included patient names, genders, addresses and phone numbers, and in some cases, Social Security numbers.
      - The brief can be found here.

DICOM Security Mitigations

We want to highlight the following mitigations for the DICOM protocol:

- Ensure all software, including operating systems, applications and hardware that utilizes DICOM, is up-to-date with the latest patches, firmware updates and platform versions.
- **Data backups:** Iterative, comprehensive, and secure.
  - The 3-2-1 rule is a good place to start.
- Secure architecture:
  - Maintain appropriate network segmentation and firewall protection.
  - Isolate sensitive systems.
  - Secure remote access for regular and administrative users (principle of least privilege).
- Disaster recovery plan:
  - Develop and maintain a comprehensive plan to ensure total restoration of critical operations in a timely manner; this should include appropriate, periodic staff training.



Medical Devices

Medical device vulnerabilities represent a significant means by which a healthcare organization can be impacted by a cyberattack

FDA Tips for Medical Device Security

The Food And Drug Administration has a significant role in minimizing cybersecurity risk for medical devices. The FDA fact sheet about their role can be found here. Their basic tips are below:

Protecting your device and personal information:

- Use good password practices for your device. Create a unique password and do not share it with others.
- Keep your device within your physical control.
- Only connect your device to other devices and software if the device manufacturer or your healthcare provider indicate it is okay to do so.
- Keep your device updated.
- Check in with your device manufacturer or healthcare provider about best practices specific to your device.

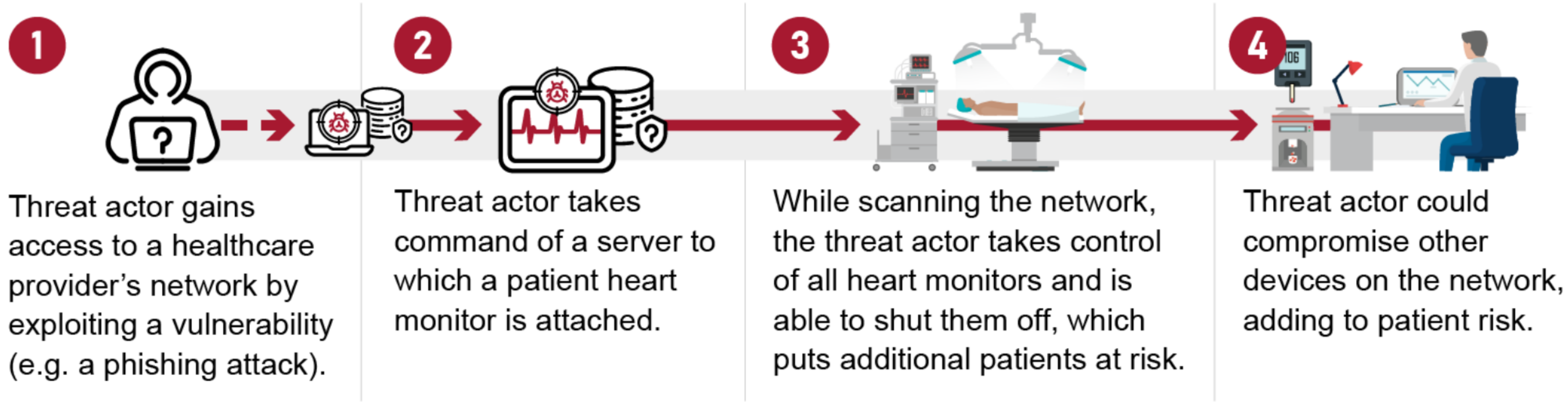
Pay attention to device symptoms that may need to be checked by your healthcare provider or the device manufacturer:

- Contact your healthcare provider or device manufacturer if you see any inconsistencies, or strange behavior from your device.
- Ensure you keep your device up-to-date with any manufacturer-supplied patches, but do not try to apply other fixes to the device yourself. Follow up on any alerts from your device.
- Have a list of questions about your device health ready to bring to your check-up.

For further details on the above recommendations, please see the FDA's website.

Medical Device Vulnerabilities

Figure: Example of a Compromised Medical Device That Can Lead to Disruption of Other Devices on a Hospital Network



1. Threat actor gains access to a healthcare provider's network by exploiting a vulnerability (e.g. a phishing attack).
2. Threat actor takes command of a server to which a patient heart monitor is attached.
3. While scanning the network, the threat actor takes control of all heart monitors and is able to shut them off, which puts additional patients at risk.
4. Threat actor could compromise other devices on the network, adding to patient risk.

Image courtesy of the Government Accountability Office

Medical Device Security

The FDA officially recognized the ANSI/AAMI SW96:2023 standard in 2023.

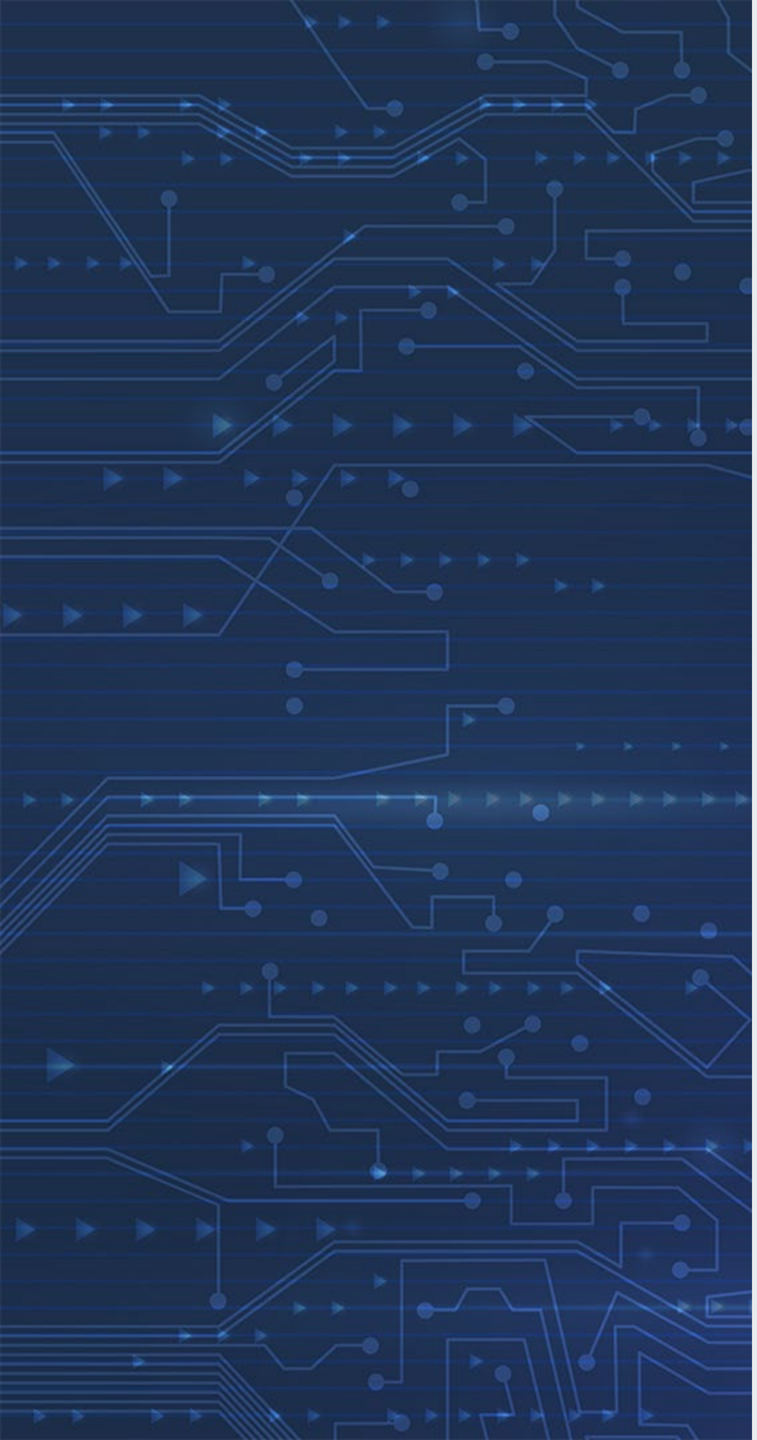
- “These measures provide clearly defined and consistent security standards to help evaluate possible cyber risk associated with new medical devices and emerging technology among vendors. The standards also highlight the need for manufactures to communicate and coordinate with healthcare delivery organizations to assist in the identification and management of security risks.”
- ANSI/AAMI SW96:2023 can be found here.

MITRE: **Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks**

- The document can be found here.

The FDA’s medical device cybersecurity page can be found here and contains an abundance of resources for protecting medical devices and keeping them secure.

The Association for Computing Machinery: “A brief chronology of medical device security” can be found here.



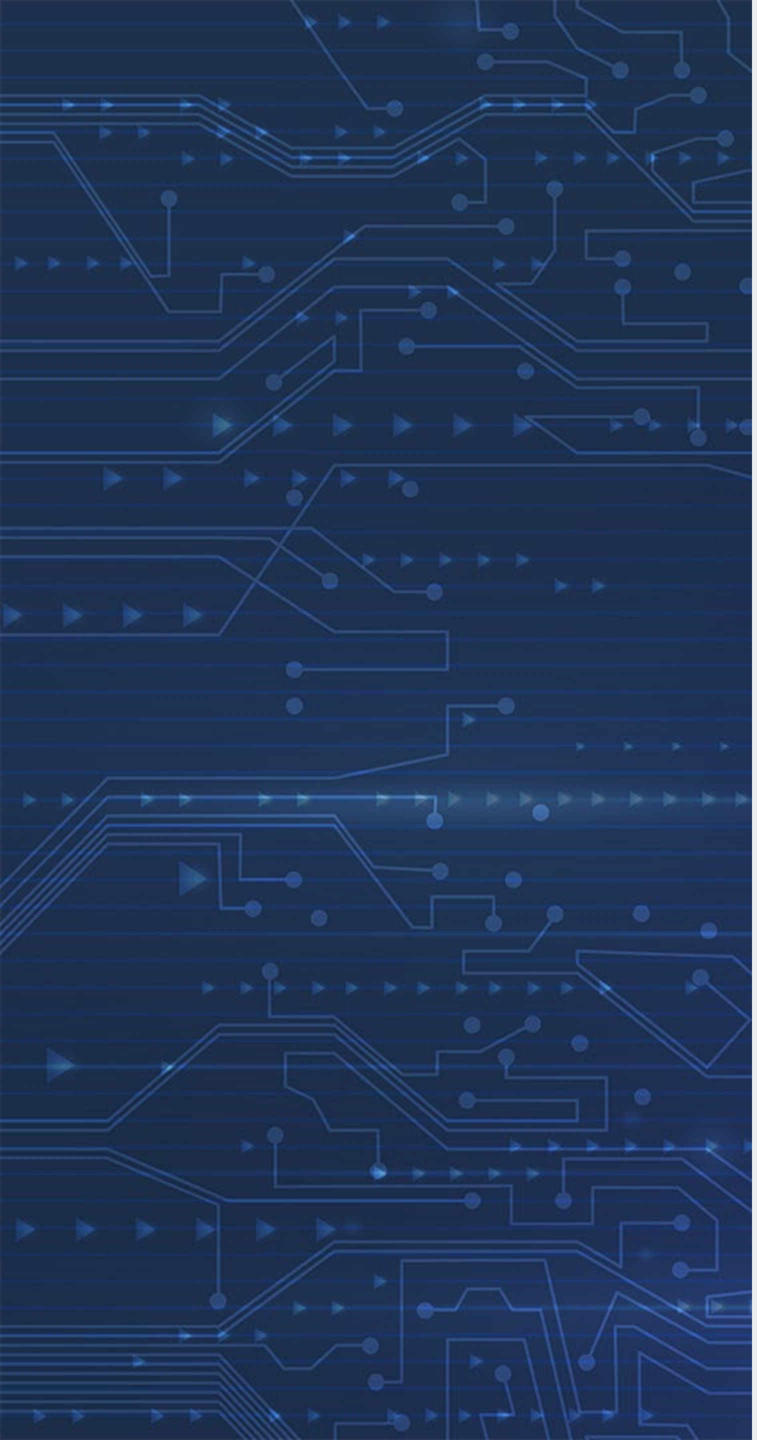
Insulin Pump Security

Remote compromise of an insulin pump has the potential to cause significant health consequences

Insulin Pump Compromise

- Insulin pumps have been known to have exploitable vulnerabilities.
  - Black Hat 2011
    - Jerome Radcliffe: Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System
    - Tools: Arduino, Ham Radios, Bus Pirate, Oscilloscope, Soldering Iron, and a hacker's intuition
  - QED Security Solutions
    - Research by Billy Rios and Jonathan Butts
- Insulin pumps can receive remote commands from an unauthorized user.

Image courtesy of Wired



Pneumatic Tubes

A system for moving containers through hospitals

Pneumatic Tubes

PwnedPiper

- Armis identified nine vulnerabilities in pneumatic tubes produced by TransLogic, which are collectively referred to as PwnedPiper. TransLogic PTS are believed to be present in more than 2,300 hospitals in North America.
- That research revealed that an unauthenticated attacker could gain full control over TransLogic pneumatic tube systems that are connected to the Internet, and then compromise the entire tube network of a hospital.
- The vulnerabilities cover a variety of potential impacts, including password leakage, remote code execution, denial-of-service, and full device compromise. Firmware has been available to address them since August.

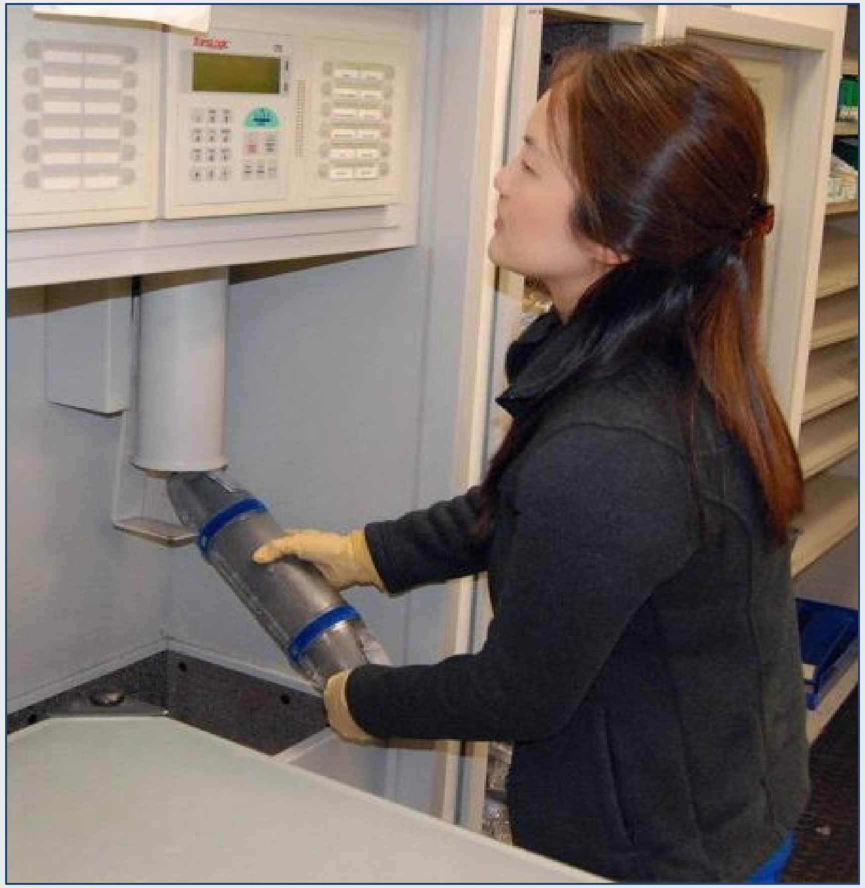
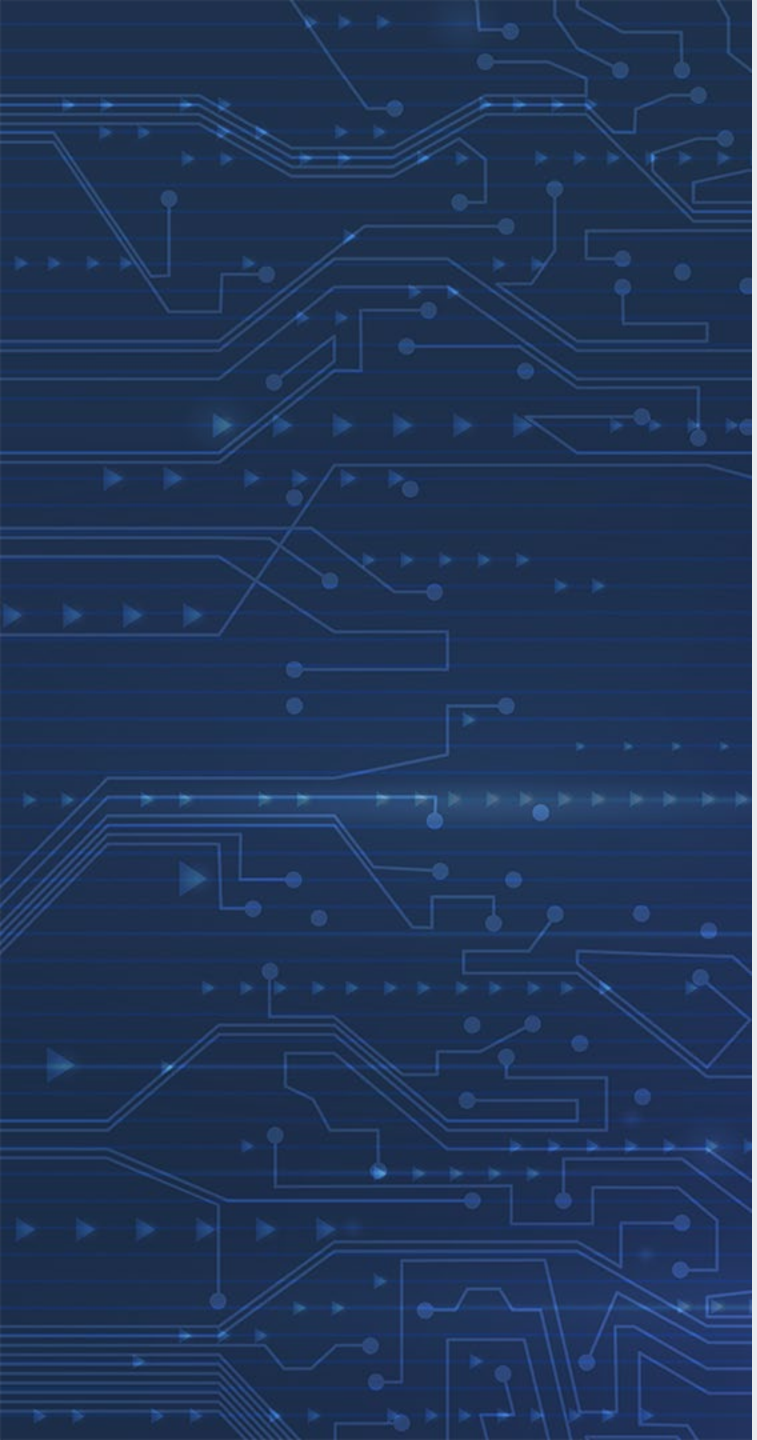


Image courtesy of ThreatPost



Electronic Health Record Systems

Medical care providers need access to records to diagnose and treat patients. Records also need to be protected, as the personal information in them can be used for fraud.

Electronic Health Record System Security

- A health record can include a comprehensive record of a patient's health history, diagnoses, treatments, medications, allergies, and test results.
- An electronic health record (EHR) is designed to improve patient care, enhance communication between healthcare providers, and reduce errors.
- Without access to health records, care often cannot be provided.
  - Cyber threat actors know this!
- Unauthorized access to electronic health records can facilitate identity theft and other forms of financial fraud.
  - Cyber threat actors know this!

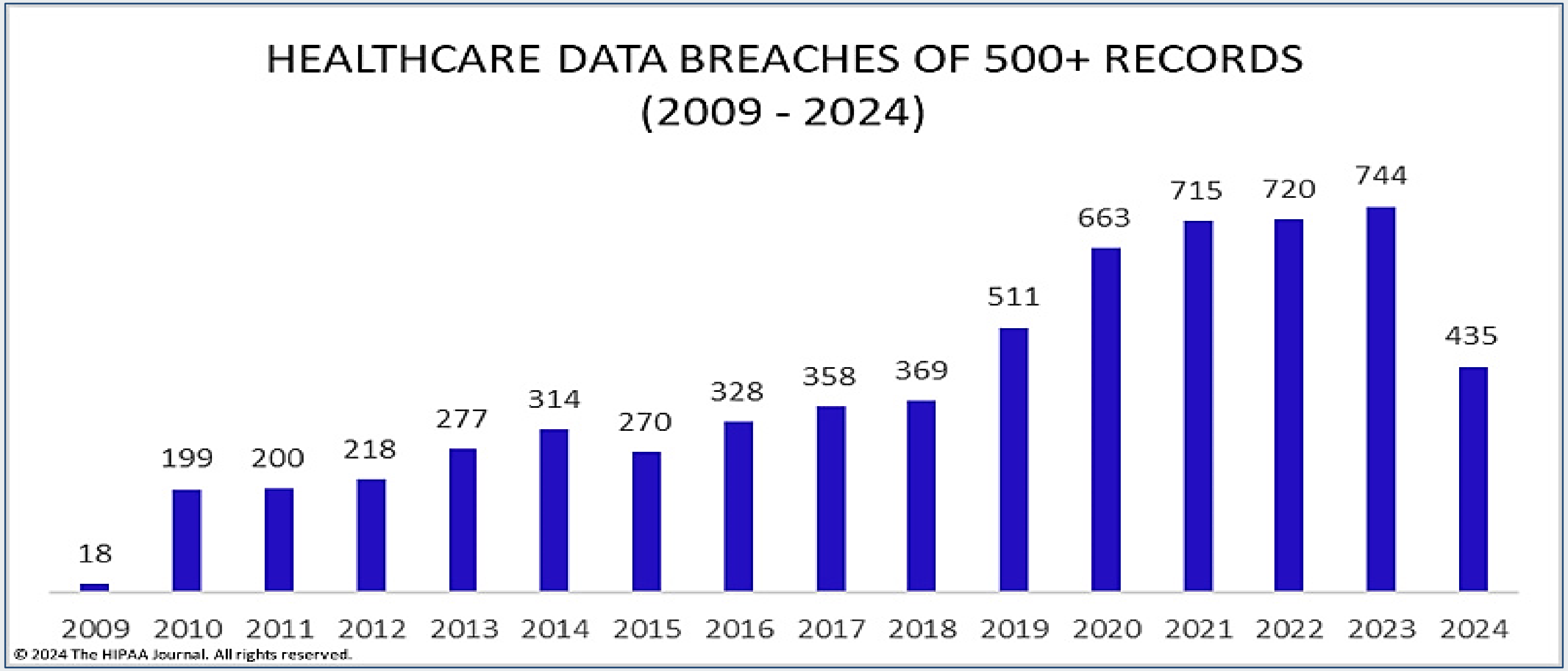
HIPAA Identifiers

There are eighteen “identifiers” considered protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA) as listed below:

- Name
- Address
- All elements (except years) of dates related to an individual
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL (address)
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image
- Any other characteristic that could uniquely identify the individual

Electronic Health Record Breaches

How many breaches of U.S. healthcare records (500 or more record breaches) have occurred since 2009?



© 2024 The HIPAA Journal. All rights reserved.

Image courtesy of HIPAAJournal

Electronic Health Record Breaches, cont.

How many individuals have been impacted by U.S. health records breaches since 2009?

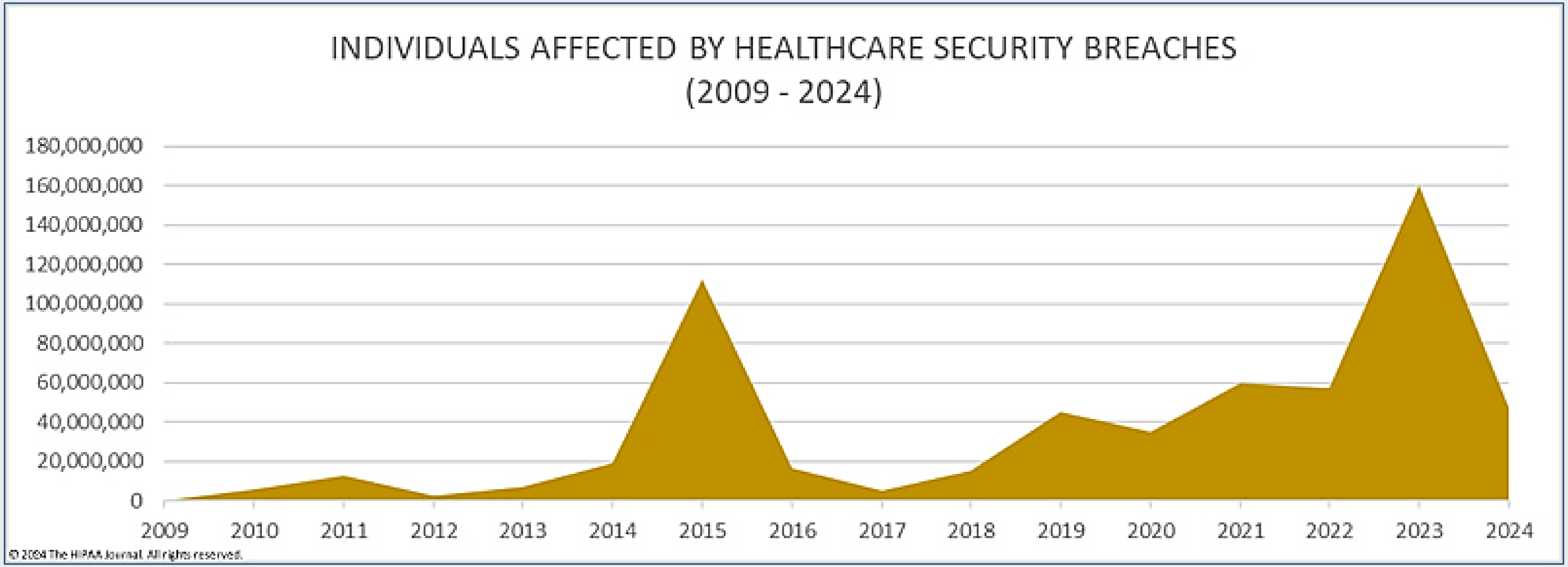


Image courtesy of HIPAAJournal

Electronic Health Record Security Vulnerabilities

Example vulnerabilities in EHR platforms:

- CVE-2016-6272 – An XPath Injection vulnerability in the Epic MyChart platform allowing for unauthorized information disclosure.
- CVE-2021-36385 – A SQL Injection vulnerability in Cerner Mobile Care 5.0.0 that can allow for remote unauthenticated attackers to execute arbitrary SQL commands.
- CVE-2015-2899 – A heap-based buffer overflow in versions of Medicomp MEDICIN Engine prior to 2.22.20153.226.

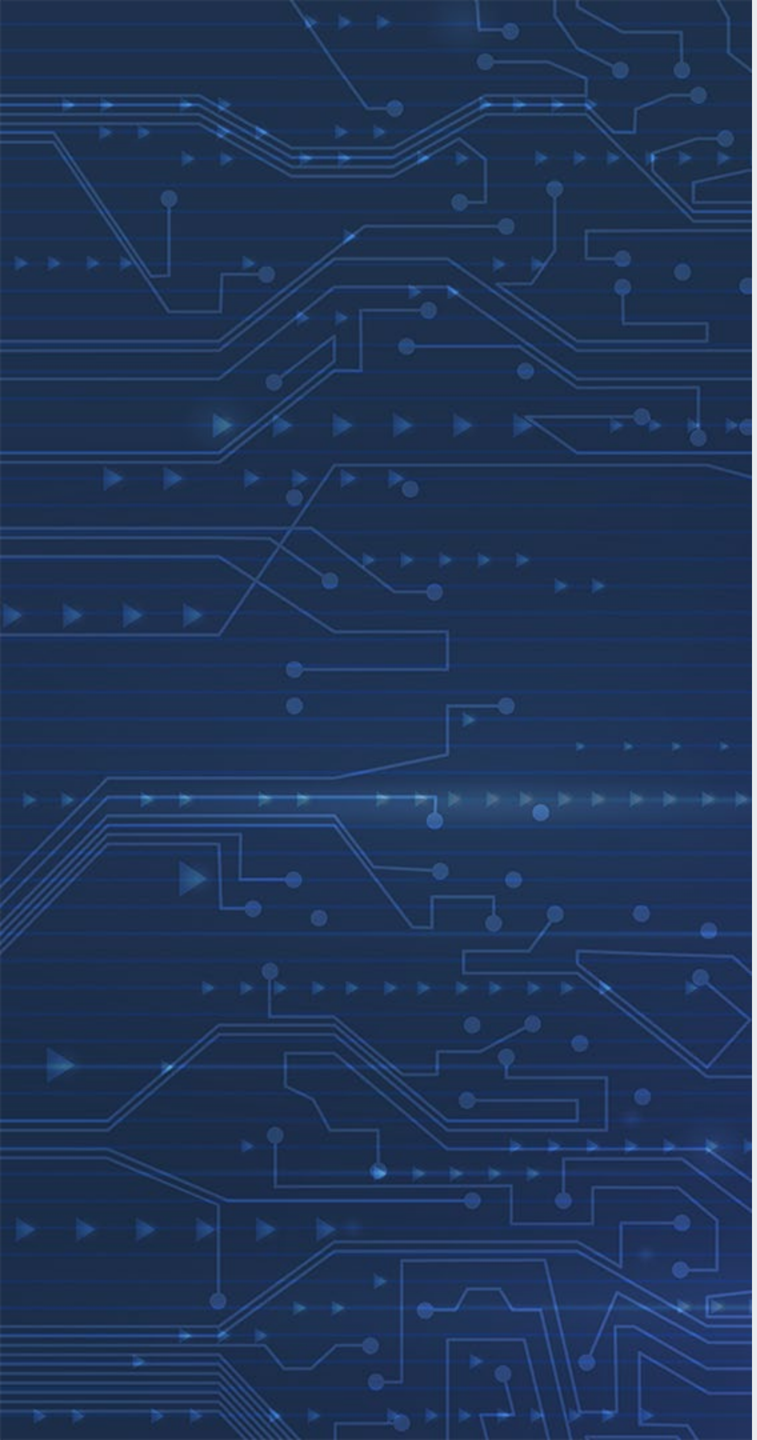
Vulnerabilities in dependent platforms:

- CVE-2023-50164 – This is a path traversal vulnerability in all Apache Struts versions prior to 2.5.33 and 6.3.0.2.
- CVE-2023-22071 – A PL/SQL privilege escalation vulnerability in the PL/SQL component Oracle Database versions up to 19.20/21.11.

Electronic Health Record Security Mitigations

We want to highlight the following mitigations for electronic health record systems (same as PACS):

- **Vulnerability management:** Implement a robust, comprehensive, and time-sensitive program.
  - Include both CVEs and non-tracked vulnerabilities (**vendor communications is key!**).
- **Data backups:** Iterative, comprehensive, and secure.
  - The 3-2-1 rule is a good place to start.
- **Secure architecture:**
  - Maintain appropriate network segmentation and firewall protection.
  - Isolate sensitive systems.
  - Secure remote access for regular and administrative users (principle of least privilege).
- **Configuration management:** Maintain secure password policy; replace all default passwords.
- **Endpoint security:** Ensure appropriate coverage and regular updates for security software.



Artificial Intelligence

Artificial intelligence requires access to large data sets and is dependent on specific algorithms, creating additional risk for the health sector

Artificial Intelligence Uses in the Health Sector

How has the health sector begun to use artificial intelligence?

- Diagnosis and clinical decision support to patients:
  - Analysis of imaging and early detection
  - Treatment recommendations
- Clinical trial optimization
- Chatbots, virtual nurses, and other virtual health assistants
- Precision medicine
- Predictive analytics:
  - Disease risk assessments and prediction
  - Anticipated patient outcomes

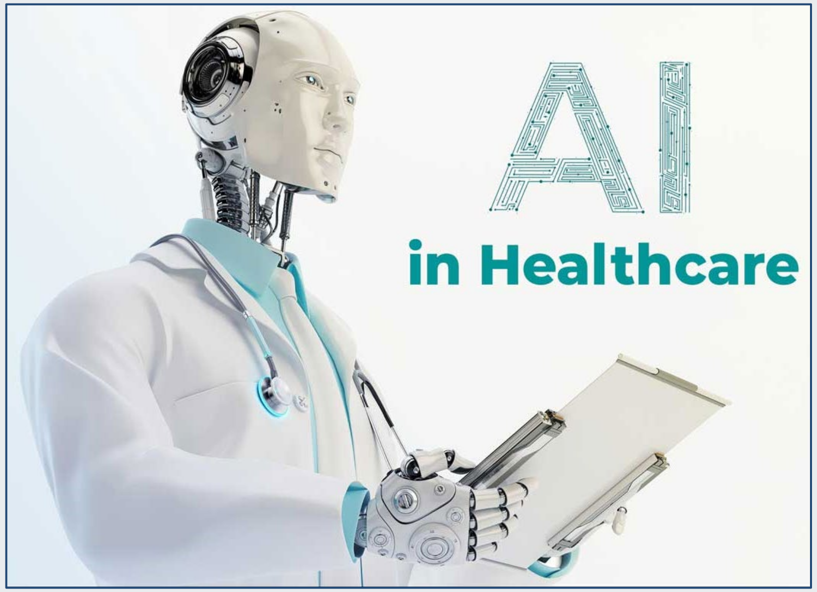


Image courtesy of Healthcare Business Club

Artificial Intelligence Security Risks

What does the health sector's adoption of AI mean for cybersecurity risk?

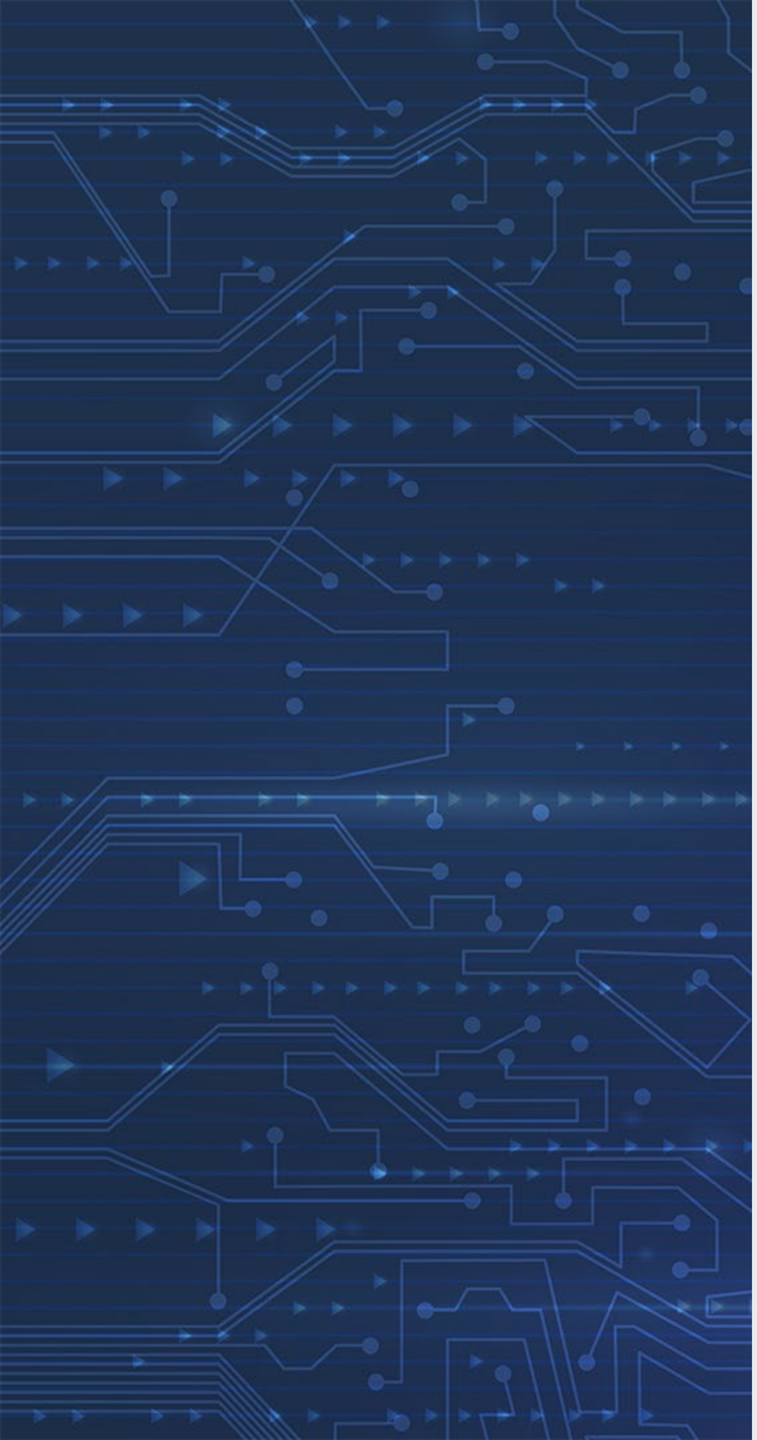
- Data security becomes a greater concern, especially data leakage and data manipulation.
- Model poisoning can skew AI outputs:
  - False positives/negatives when it comes to diagnosing.
- Supply chain attacks can compromise components of AI systems.
- The possibility for intellectual property theft can entice cyber threat actors.

Image courtesy of Forbes

Artificial Intelligence Security Mitigations

How to mitigate cybersecurity risks related to artificial intelligence used in the health sector?

- Data protection and security become extremely important:
  - Implement robust data security measures, such as strong encryption, controlled access, and data loss prevention techniques.
- AI model validation and monitoring:
  - Validate AI models to ensure accuracy and reliability and monitor for poisoning or evasion attacks.
- Secure supply chains:
  - Vet third-party AI components and suppliers to minimize risks
  - Vendor security assessments
  - Contractual agreements



Defense and Mitigations

What can be done generally to keep the health sector secure?

Zero Trust

Definition: Operating a cybersecurity defensive posture with the idea that no implicit trust should granted to users or assets. (Superseding a strictly perimeter-based defensive model.)

- **Core principles:** Trust but verify → Never trust. Always verify.
- Challenges to the health sector:
  - Complexity of healthcare IT environments.
  - Demand for access by non-technical patients.
- Critical zero trust measures:
  - Identity and access management
  - Network segmentation
  - Endpoint security
  - Data protection

Resources:

- Cybersecurity & Infrastructure Security Agency: Zero Trust Maturity Model
- National Institute of Standards and Technology: SP 800-27 Zero Trust Architecture

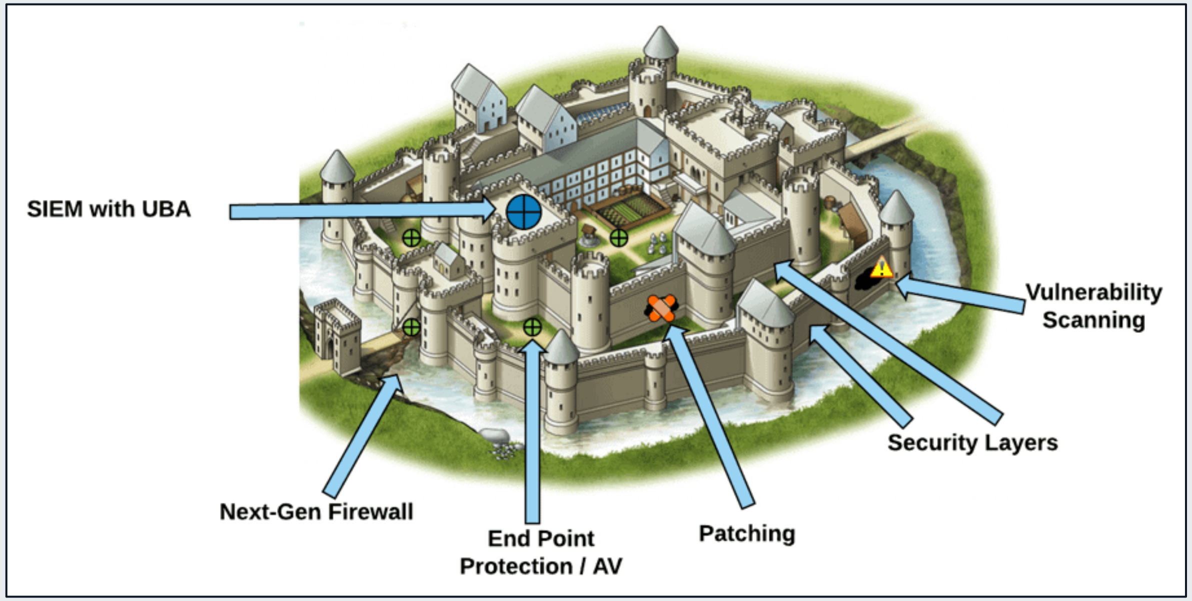
Defense-in-Depth

Definition: The integration of people, technologies and policies to establish layers of defensive measures to protect against cyber threats.

Core principles:

- Layered security
- Redundancy

- Challenges to the health sector:
  - Complexity of healthcare IT environments.
  - Need for legitimate remote access.
- Critical defense-in-depth defensive measures:
  - Identity and access management
  - Network segmentation
  - Endpoint security
  - Data protection



The castle is often used to illustrate defense-in-depth. *Image courtesy of Atmosera*

Resources:

- National Institute of Standards and Technology: Measuring the Effectiveness of Defense-in-Depth Postures

Staying Secure

Government resources:

- DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
- FBI Cybercrime: https://www.fbi.gov/investigate/cyber
- FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
- FDA: Medical Device Information: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- H-ISAC White Papers: https://h-isac.org/category/h-isac-blog/white-papers/
- 405(d) Resource Library: https://405d.hhs.gov/resources
- HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- HHS Cyber Performance Goals: https://hphcyber.hhs.gov/performance-goals.html

Ransomware Mitigations and Defense (Source: FBI)

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or -recognized scheduled tasks for unrecognized “actions.” (For example, review the steps each scheduled task is expected to perform.)

Image courtesy of Acronis

Ransomware Mitigations and Defense

- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.

Ransomware Mitigations and Defense, cont.

- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Free Cybersecurity Services and Tools

In addition to following the mitigations, HC3 recommends organizations review and utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting https://www.cisa.gov/free-cybersecurity-services-and-tools.

Image courtesy of CISA

Conclusions

Vulnerability management will continue to be important moving forward.

- The concept of the weakest link always applies.
- A healthcare organization must secure **both** its healthcare-specific technologies as well as its universal technologies, if it wants to minimize cyber risk in a meaningful way.
  - Cover both CVEs and non-CVEs:
    - Maintaining a comprehensive asset inventory.
    - Vendor communication is going to be critical for vulnerabilities not assigned a CVE.
- Patching speed (time-to-patch) is only going to become more important.

Data protection will continue to be important moving forward.

Protecting data is only going to get more critical:

- Protect it with encryption and access control.
- Back it up (3-2-1 rule).

Reference Materials

References

HHS HC3: Picture Archiving Communication Systems (PACS) Vulnerabilities
https://www.hhs.gov/sites/default/files/pacs-vulnerabilities.pdf

Aplite: Millions of Patient Records at Risk - The Perils of Legacy Protocols
https://i.blackhat.com/EU-23/Presentations/EU-23-Yazdanmehr-Millions_of_Patient_Records_at_Risk.pdf

Seagate: What is a 3-2-1 Backup Strategy?
https://www.seagate.com/blog/what-is-a-3-2-1-backup-strategy/

Medical Device Cybersecurity: What You Need to Know
https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

MITRE: Next Steps Towards Managing Legacy Medical Device Cybersecurity Risks
https://www.mitre.org/sites/default/files/2023-11/PR-23-3695-Managing-Legacy-Medical-Device%20Cybersecurity-Risks.pdf

References, cont.

FDA: Cybersecurity
https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

A Brief Chronology of Medical Device Security
https://dl.acm.org/doi/pdf/10.1145/2890488

CISA: Zero Trust Maturity Model
https://www.cisa.gov/zero-trust-maturity-model

NIST: Zero Trust Architecture
https://www.nist.gov/publications/zero-trust-architecture

NIST: Measuring and Improving the Effectiveness of Defense-in-Depth Postures
https://www.nist.gov/publications/measuring-and-improving-effectiveness-defense-depth-postures

? Questions

FAQ

Upcoming Briefing

- October 17 – Living-Off-the-Land Attacks

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. 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. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and 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.

Alerts and Analyst Notes

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

Threat Briefings

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.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV