

Fortifying the Frontline:

IT Security for Medical Devices and
Corporate Asset Protection



Anthony Siravo, MBA, MSIS
VP, Chief Information Security Officer

Certifications Held:

CISSP, CRISC, CISM, GLEG, GPCS, GCWN, C|CISO, CHPS,
Security+, OSWP, ITIL, CCSA, NSA, PMP, BCCPA, CCSK



ANTHONY SIRAVO

Chief Information Security Officer

INTERNATIONAL CISO
GLOBAL ENTERPRISE
PRODUCT SECURITY

Based in Smithfield, RI

ABOUT ME

Information Security Leader who thrives on the frontline of defense, safeguarding organizational information assets from the relentless threats of the digital world.

My **passion for information security** is not just a career, but a commitment to protecting data integrity, confidentiality, and availability, ensuring that trust and reliability remain the bedrock of our digital interactions.

18+ years of leading teams and architecting strategies that have decisively shaped company outcomes, leveraging my expertise in technology and security.

My **leadership transcends management**, as I actively drive initiatives and skill development that fortify our technological foundations and secure our digital frontiers, ensuring sustainable growth and resilience in an ever-evolving landscape.

\$5.7 billion publicly held Fortune 553 Global Technology Company - Responsible for 240 locations internationally which consisted of IoT/IoMT product and software security as well as corporate enterprise security.

\$3 billion privately held Healthcare System - Implemented a comprehensive enterprise security program from the ground up securing over 26 thousand Medical Devices and 40 thousand enterprise infrastructure assets for 5 large hospitals and over 250 outpatient facilities employing over 25,000 employees and contractors.

To the point board level communicator – Presents to board regularly. Guest speaking engagements for CISO's & CIO's to educate them on current threat landscape with concise recommendations on how to best to protect assets.

CAREER JOURNEY

VP, Chief Information Security Officer
Lifespan
Nov 2015 - Present

VP, Chief Information Security Officer
Zebra Technologies
Oct 2005 - Oct 2015

Chief Information Officer
Bradford Soap Works, Inc.
Jan 1998-Oct 2005

Director of Information Systems
CSC Paymaster
Jan 1996-Jan 1998

FUN FACTS

Married with 2 kids (8-year-old boy / 12-year-old girl)

Hobbies include Home Automation, building retro game arcades, and playing on golf simulator I built.

EDUCATION

Bryant University
MBA, Business Administration
MS, Information Systems

Roger Williams University
BA, Information Systems

AWARDS

Top 100 Information Security Professional Award – 2022/2023/2024 - ONCON ICON

Top 50 Information Security Team Award – 2023 - ONCON ICON

CSO50 Award - 2018 & 2023

Top Global CISO – 2023 CyberDefenseCon



CERTIFICATIONS

CISSP: Certified Information Systems Security Professional – ISC2 [License# 423351](#)
CHPS: Certified in Healthcare Privacy and Security – AHIMA [License# 2396923](#)
GLEG: Certified Law of Data Security & Investigations – GIAC [License# 698](#)
GCPS: GIAC Public Cloud Security – GIAC [License# 190](#)
CCISO: Certified Chief Information Security Officer – EC-Council [License# CC-AS-139](#)
CISM: Certified Information Security Manager – ISACA [License# 1220870](#)
CRISC: Certified in Risk and Information Systems Control – ISACA [License# 1926276](#)
OSWP: Offensive Security Wireless Professional – OFFENSIVE SEC [License# OS-BWA-15810](#)
GCWN: Certified Windows Security Administrator – GIAC [License# 3346](#)
CCSK: Certificate of Cloud Security Knowledge – CSA [License# 737989223494](#)
Security+: CompTIA Security+ [License# PBZ9K5W2WC142RKM](#)
PMP: Project Management Professional – PMI [License# 1597760](#)
CCSA: Check Point Certified Security Administrator [License# Grandfathered](#)
BCCPA: Blue Coat Certified Proxy Administrator [License# Grandfathered](#)
ITIL: Information Technology Infrastructure Library [License# Grandfathered](#)

MEMBERSHIPS & ASSOCIATIONS

InfraGard – Private Sector & FBI Partnership for the protection of U.S. Critical Infrastructure
ISACA – The Information Systems Audit and Control Association
AHIMA – The American Health Information Management Association
ISC2 – International Information System Security Certification Consortium
CSA – Cloud Security Alliance
CIS – Center for Internet Security
PMI – Project Management Institute

CORE COMPETENCIES

- International / Multicultural Experience
- Board Communications / Presentations
- Merger & Acquisition Integration
- SIEM & Vulnerability Management
- HIPAA / HITRUST / SOX / GDPR / GLBA / ISO 27001 / NIST / SOC2
- 3rd Party Security Provider Management
- GRC - Governance, Risk, Compliance
- IoT / IoMT Security
- Penetration Testing
- Regulatory Audits
- Budget / Forecasting
- SaaS / IaaS / Security
- Red / Blue Team
- Office 365 Security
- Data Loss Prevention
- Secure Cloud (Azure/AWS/GCP)
- Product Security
- DevSecOps / Agile
- Network Security
- Offensive Security
- IAM
- Risk Management

5.7B

LARGEST REVENUE PROTECTED

74k

MOST ASSETS PROTECTED

25k

MOST PEOPLE PROTECTED



PROVIDED LEADERSHIP IN COUNTRIES

11

SPEAKING ENGAGEMENTS

Speaker @ Boston Regional Healthcare Compliance Conference
Presented: What Compliance Professionals Should Know About Cybersecurity

Speaker @ Transformational CISO Assembly
Presented: Ransomware Protection & Response
Presented: Balance is Key: Finding a Balance in Convenience for IoT within Security and Privacy

Speaker @ HFMA & NEHIA Annual Compliance & Internal Audit Conference
Presented: Medical Device Security Risks and Mitigation
Discussed the state of healthcare, typical findings in GRC programs, business risk acceptance, and what steps healthcare businesses can take to reduce risks

Panelist @ secureCISO Boston
Discussed the cyber threat landscape that enterprises face; a discussion that goes beyond the textbook and reveals the real paths, strategies, and directions of leaders that defend against the unknown.

Speaker @ RI Dermatology Society 5th Annual Fall Conference - Cybersecurity for Dermatologists
Discussed the current state of the cybersecurity threat landscape as it relates to the medical profession. Detailed how all devices on the Internet of Things (IoT) place providers at risk, at work and at home. Taught audience tools needed to implement good practices to reduce the risk of successful cyberattacks.

Panelist @ American College of Healthcare Executives (AHCE) Cybersecurity Forum
Served as a panel member to discuss how healthcare organizations face significant, evolving cybersecurity risks. Cyber threats are constantly changing, the frequency of attacks is increasing, and the approaches continue to become more sophisticated. This session will provide current information about the latest threats, prevention strategies, and resources available to improve your cybersecurity.

Speaker @ RI Medical Staff Association – "Information Security Awareness Rounds"
Educated members on current information security threat landscape. Discussed cyberthreats such as Phishing & Ransomware, as well as risks to healthcare delivery with medical device on the Internet of Things (IoT). Gave guidance on good practices to reduce risk of successful cyberattacks

Current Threat Landscape in Healthcare (2024)



Ransomware and Data Breaches

Ransomware continues to be a dominant threat in healthcare, with a significant increase in attacks over the last five years. These attacks are particularly damaging due to the critical nature of healthcare systems, where even short disruptions can impact patient care, delaying treatments and increasing patient risks. Notable ransomware groups like **Lockbit 3.0** and **BlackCat (ALPHV)** have targeted healthcare institutions, causing operational chaos and financial loss.



Targeting of Medical IoT Devices

The **Internet of Medical Things (IoMT)** poses a growing security challenge. Many connected medical devices, such as **MRI machines, IV pumps, and heart monitors**, are running outdated software and lack essential security features. A large percentage of these devices are highly vulnerable, providing easy access for attackers to sensitive patient data and disrupting life-critical operations.



Third-Party Risks

Healthcare is heavily reliant on third-party vendors, making supply chain attacks a significant risk. The **Change Healthcare** ransomware incident serves as a stark example of how third-party breaches can have a nationwide impact on hospitals, affecting billing, claims processing, and patient care services. Strong vendor risk management strategies are now critical to mitigating this threat.



Nation-State and Hacktivist Attacks

Nation-state actors and hacktivist groups are increasingly targeting healthcare institutions, not only to steal sensitive research data but also to cause widespread disruption. These groups often collaborate with ransomware attackers, leveraging cyber espionage techniques to breach healthcare organizations.



Telehealth and Cloud Security Challenges

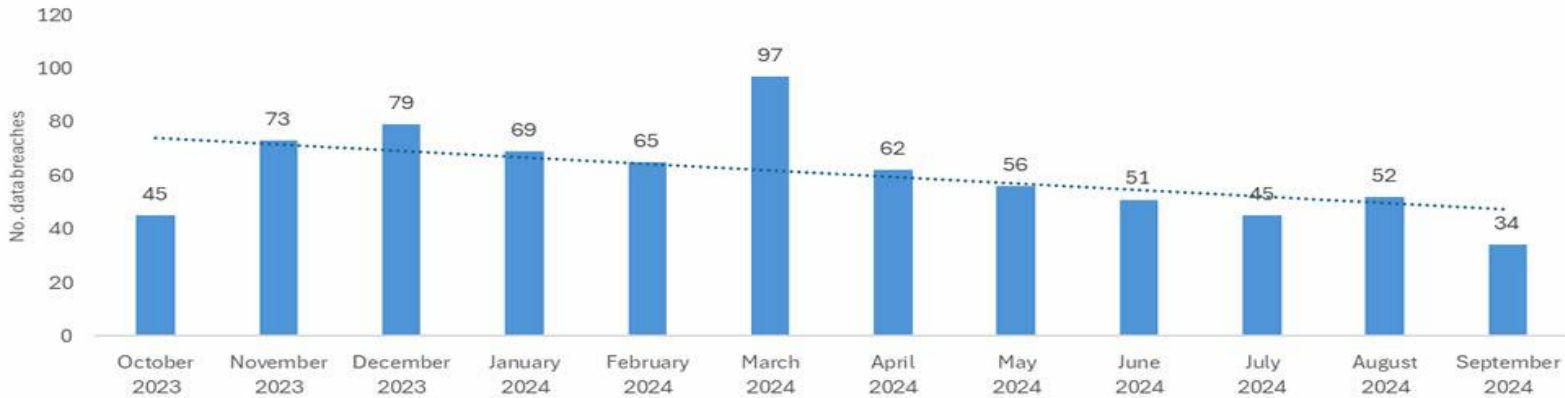
The rise of **telehealth** and **cloud computing** introduces new vulnerabilities. Many healthcare organizations lack the internal resources to fully secure these environments, which makes them susceptible to data breaches and malware attacks. Weak encryption and misconfigured cloud platforms are ongoing concerns.

Sources:

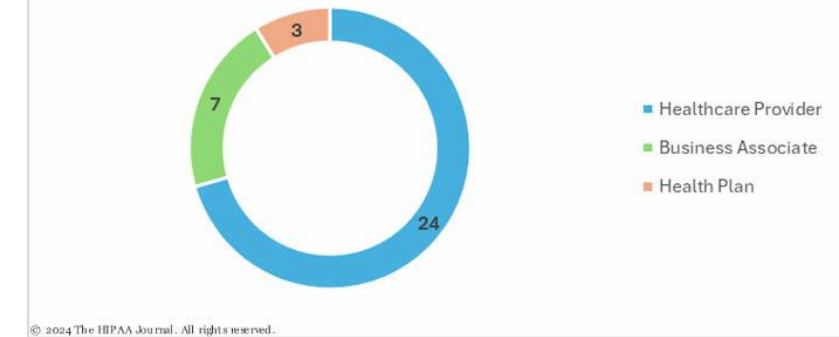
AHA News: "A Look at 2024's Health Care Cybersecurity Challenges"
"BDO: "The Healthcare Cybersecurity Landscape in 2024"
ChartLogic: "Navigating Cybersecurity in Healthcare 2024: Trends & Challenges"
Health-ISAC: "Current and Emerging Healthcare Cyber Threat Landscape"
Palo Alto Networks: "Healthcare Cybersecurity — Three Trends to Watch in 2024"

Healthcare Breaches – Initial access vector: Phishing / Externally Facing Vulnerabilities

Healthcare Data Breaches of 500 or More Records

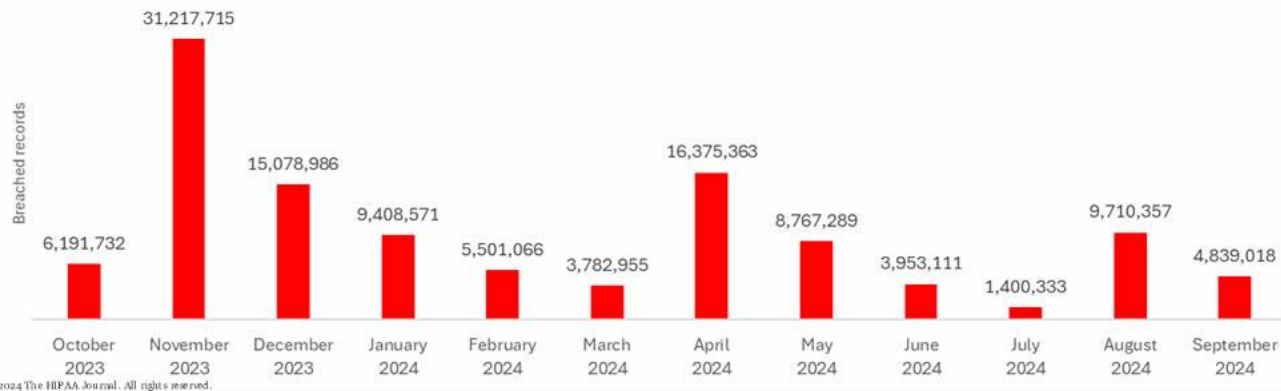


Data Breaches at HIPAA Regulated Entities
Sept 2024

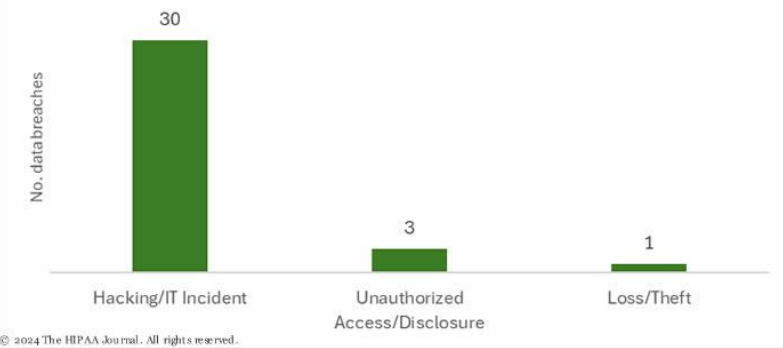


➤ **So far in 2024, 531 data breaches of 500 or more records have been reported to OCR. In the first half of 2024, data breaches were reported at a rate of 67 a month. In the second half of 2024, data breaches have been reported at a rate of 44 a month.**

Records Compromised in Healthcare Data Breaches



Causes of Healthcare Data Breaches
Sept 2024



Largest Healthcare Breaches Under Investigation from OCR (24 Months)

- 1) **Change Healthcare, Inc.** - 100 million individuals !!!!!!!!!!!
- 2) **Welltok, Inc.** – 14.7 million individuals
- 3) **Kaiser Foundation Health Plan, Inc.** – 13.4 million individuals
- 4) **HCA Healthcare** – 11.2 million individuals
- 5) **Maximus, Inc.** – 9.1 million individuals
- 6) **PharmMerica Corp** – 5.8 million individuals
- 7) **HealthEC LLC** – 4.6 million individuals
- 8) **HealthEquity, Inc** – 4.3 million individuals
- 9) **Reventics, LLC** – 4.2 million individuals
- 10) **OneTouchPoint, Inc.** – 4.1 million individuals



Internet of X Things (IoXT): Understanding Device Risks

With the explosion of internet-connected devices, it's crucial to understand the risks these devices pose to the network.

- **General IoT Devices**

- Smart cars, Internet-enabled appliances, printers, HVAC controls, surveillance cameras, and communication systems.
- These devices often lack security features by default, making them easy targets for attacks.

- **Internet of Medical Things (IoMT)**

- A subset of IoT, focused on medical devices like infusion pumps, MRI machines, X-rays, and CT scanners.
- These devices, if compromised, can have life-threatening consequences in healthcare settings.

- **Industrial Control Systems (ICS) and SCADA**

- Systems used in critical infrastructure like power grids, water supply, and gas pipelines.
- A breach can have widespread consequences, affecting large geographic areas and critical services.



Security Controls - IS Managed Devices

Workstation Security Controls

- **Next-Generation Antivirus (“NGAV”):**
CrowdStrike Falcon Prevent
- **Endpoint Detection and Response (“EDR”):**
CrowdStrike Falcon Insight
- **Managed Detection and Response (“MDR”):**
CrowdStrike Falcon Complete
- **Managed Threat Hunting (“MTH”):**
CrowdStrike Falcon OverWatch
- **Threat Analysis / Malware Sandbox:**
CrowdStrike Hybrid Analysis
- **Hard Disk Encryption:** Microsoft BitLocker
- **Application Whitelisting:** Carbon Black App Control
- **Patch Management:** Ivanti UEM
- **Malicious Email Reporting & Triage:**
Cofense Phishing Detection and Response
- **Forensics/eDiscovery:** OpenText EnCase

Windows Server Security Controls

- ***All Above Workstation Security Controls Included***
- **Patch Management:** Ivanti UEM & PatchLink
- **Data Loss Prevention – At Rest:** Varonis

Network Security Controls

- **Log Collection / SIEM:** SecureWorks Taegis
- **Vulnerability Scanning:** Qualys
- **Network Authentication:** Aruba ClearPass
- **Patch Management:** SolarWinds
- **Firewalls:** Cisco ASA / Cisco FTD
- **IDS/IPS:** Cisco FirePower
- **Web Filtering:** zScaler
- **Network Access Control:** Forescout
- **AI / Behavioral Analytics / Insider Threat:**
DarkTrace Enterprise Immune System

Mobile Device Security Controls

- **Mobile Device Management:**
Microsoft MDM
- **Multi-Factor Authentication:**
Microsoft MFA
- **Privacy Controls:**
Microsoft Conditional Access Rules

Non-IS Managed devices only have read-only access to O365 (Web Mail / Word / Excel / OneDrive)

Security Hardening

CIS Benchmarks: Workstations / Network

IS Managed Devices – Vulnerability / Patching Standard

HARDWARE AND SOFTWARE VULNERABILITY MANAGEMENT STANDARD

Lifespan Vulnerability Remediation Standards:

Lifespan’s information security team uses the designation of **Critical** and **Non-Critical** to categorize vulnerabilities and corresponding remediation time frames. These designations correspond with CVSS ratings published by NIST at <https://nvd.nist.gov/>. The direct link to search the NVD is <https://web.nvd.nist.gov/view/vuln/search>. The CVSS Base score will be used to determine criticality.

Since end of life software is no longer patched and maintained by the vendor, the implication is that there are unpatched vulnerabilities and the software should be removed from the environment in the same timeframe as a critical vulnerability.

The Lifespan security stack is a core component in the protection of Lifespan data. If the tools within the security stack fall behind, it provides less than optimal defense against vulnerabilities. Therefore, the software and hardware that comprise the security stack should be updated in the same timeframe as a critical vulnerability.

Vulnerability	Lifespan Information Security Category	Required Remediation Schedule
Immediate Threat	Critical	Immediately
End of Life	Critical	30 Days from End of Life Announcement
End of Life	Critical	30 Days from New Version
CVSS 7-10	Critical	30 Days from NIST Rating
CVSS 0-6.9	Non-Critical	90 Days from NIST Rating

Epic vulnerability notices do not directly correspond to NIST CVSS ratings. The chart below provides the ability to determine the appropriate Lifespan Information Security Category and criticality above.

		Corresponding Lifespan Risk Rating			
		High	Medium	Low	Negligible
Epic Impact	High	Non-Critical	Non-Critical	Non-Critical	Critical
	Medium	Non-Critical	Non-Critical	Non-Critical	Non-Critical
	Low	Non-Critical	Non-Critical	Non-Critical	Non-Critical
	Negligible	Non-Critical	Non-Critical	Non-Critical	Non-Critical
		Negligible	Low	Medium	High
		Epic Exploitability			

Prior to the deployment (“Go Live”) of On-Premise (Lifespan) Production server, network, workstation, and/or software systems, all critical vulnerabilities that have a National Vulnerability Database (NVD) published date older than thirty (30) days of an IS Project’s Go-Live date must be remediated prior to Go-Live.

The specific hostnames and IP address of network assets required to be scanned must be provided by the Requestor within the Ivanti Service Request/Task requesting the Go-Live scan. Requests that do not include an asset list will be cancelled.

Security Controls – Non-IS Managed Devices (IoT/IoMT)

Network Security Controls

- **Vulnerability Scanning:** Qualys
(Unauthenticated Only)
- **Web Filtering:** zScaler
- **Network Access Control:** Forescout
- **AI / Behavioral Analytics / Insider Threat:**
DarkTrace Enterprise Immune System

IoMT Devices – Vulnerability / Patching



Vendor Security Risk Assessments (VSRA): A Collaborative Approach

Vendor security assessments are a critical step in protecting your organization's assets.

Facilitation of Risk Assessments

- Administer risk questionnaires and conduct interviews with vendors to evaluate their security posture.
- Leverage a trusted third-party partner to assist in the assessment process.

Collecting Critical Security Documents

- Gather vendor policies, including SOC 2 Type 2 attestations, to review their security controls.

Reporting and Actioning Risks

- Present identified vendor risks to the internal security team for mitigation or acceptance.

Leveraging Community Insights

- Use collective intelligence from previous vendor assessments to inform decisions.

NIST Standards for Consistency

- Assessments adhere to NIST standards, ensuring a robust, standardized approach to vendor security.

Vendor Security Risk Assessments (VSRA) – NIST/HIPAA/COBIT

Control Question #	NIST SP800-53 R4: Control #	HIPAA CFR Control Reference(s)	COBIT 5.0	Control Name	Security Questions:
Access Control					
AC-1.1	AC-1	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(1)	DSS02.02 DSS05.02 DSS05.04 DSS05.05 DSS05.06	Access Control Policy and Procedures	Are there formally documented policies and procedures for access control? If yes, please attach.
AC-2.1	AC-2	164.308(a)(3)(ii)(A) *From AC-13 164.308(a)(3)(ii)(B) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.308(a)(5)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii)	DSS05.04	Account Management	Do you have a process for managing accounts, including - creating, modifying, monitoring, and deleting/disabling accounts?
AC-2.2					Are accounts reviewed on a periodic basis? If yes, include timeframe in comment.
AC-2.3					Have all guest, shared (other than Admin/Root), or group accounts been removed or disabled?
AC-2.4					Are account managers notified when accounts are no longer required, when users are terminated or transferred, or when individual access requirements change?
AC-2.5					Is approval from an authorized signer required before provisioning accounts?
AC-3.1	AC-3	164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iv)	DSS05.04	Access Enforcement	Does the information system verify the rights of a user to access the information system? (Access Control Lists, Group/Role membership?) If yes, detail how the access is enforced in the comment.
AC-3.2	N/A			Access Enforcement	Does the information system support role-based account management and access controls (RBAC)?
AC-3.3	N/A			Access Enforcement	If RBAC is supported, can a customer administrator create/customize unique roles and permissions.
AC-4.1	AC-4	164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.310(b)	DSS04.07 DSS05.02 DSS05.04 DSS05.05	Information Flow Enforcement	Is the flow of sensitive information secured between interconnected systems? (Firewall rule sets - iptables, proxies, encrypted tunnels.)

Vendor Security Risk Assessments (VSRA) – NIST/HIPAA/COBIT (cont.)

Control Question #	NIST SP800-53 R4: Control #	HIPAA CFR Control Reference(s)	COBIT 5.0	Control Name	Security Questions:
Audit and Accountability					
AU-1.1	AU-1	164.312(b)	ME2.5 DSS05.04	Audit and Accountability Policy and Procedures	Are there formally documented audit and accountability procedures for this information system? If yes, please attach.
AU-2.1	AU-2	164.308(a)(5)(ii)(C) 164.312(b)	ME2.5 DSS05.04	Audit Events	Is the information system actively auditing events such as access to patient information, login/logoffs, account creation, etc.? If yes, please detail the events captured in the comment.
AU-2.2					Are the audit logs captured sufficient for incident response and system and user performance/investigation?
AU-3.1	AU-3	164.312(b)	ME2.5 DSS05.07	Content of Audit Records	Does the system create audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event?
AU-4.1	AU-4	164.312(b)	ME2.5 DSS05.07	Audit Storage Capacity	Have you evaluated the audit storage capacity of this information system and determined that it is adequate?
AU-5.1	AU-5		ME2.5 DSS05.07	Response to Audit Processing Failures	Does the information system generate an alert that notifies the team in the event of an audit processing failure?
AU-6.1	AU-6	164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.308(a)(4)(i) 164.308(a)(5)(ii)(C) 164.312(b)	DSS02.02, ME2.5 DSS02.04 DSS05.07	Audit Review, Analysis, and Reporting	Do you review the audit logs for indications of inappropriate or unusual activity and report those incidents to authorized personnel?
AU-7.1	AU-7	164.308(a)(1)(ii)(D) 164.312(b)	DSS02.02, ME2.5 DSS02.04	Audit Reduction and Report Generation	Does the information system provide the capability to generate customizable audit reports?
AU-7.2					Does the generation of an audit report alter the original content or time stamp of the audit record?
AU-8.1	AU-8		ME2.5	Time Stamps	Are the audit logs time stamped? (Date and Time)
AU-9.1	AU-9		DSS02.02 DSS02.04 DSS05.03 DSS05.05, ME2.5	Protection of Audit Information	Does the system/application protect audit information from unauthorized access, modification, and deletion?

Hardware Risk Assessments (HRA) – IoMT Example

Risk Rating Overview								
Environment: ██████████ Thermal Printer								
Environment: On-premises ██████████	Users: 20	HRA Purpose: New Hardware	Total Devices: 8	Internet Access Required: No	VPN Tunnel Required: No	Authentication Method: Local Authentication	Data Encryption at Rest: Unknown	Data Encryption in Transit: No
Product / Service:	Risk Rating						Threshold	
██████████ Thermal Printer	High: The assessment identified few controls that are implemented and aligned with industry best practice. Remediation activities should be identified and planned with corrections implemented as there is a high likelihood of an imminent breach						Hardware Review of ██████████ ██████████ Thermal Printer	
Risk Rating Summary	<p>The web interface of the thermal printer is vulnerable to a cross-site scripting (XSS) vulnerability, as input fields on the configuration section are not sanitized. This could allow any user to access the configuration section on the administrative panel and able to inject XSS code. Any user who accesses the status of the printer will be affected by the script and may potentially steal their cookie and session information from their browser.</p> <p>The thermal printer allows access to the administration web console without authentication, enabling users to make unauthorized changes to the system, make the device inaccessible in the network, and lead to propagating malicious activities in the wider organization network.</p> <p>The ██████████ Thermal Printer is also vulnerable to a remote file inclusion (RFI) attack, which may lead to executing various sensitive functions on the server that compromise the server or creates a backdoor on the network.</p> <p>The ██████████ Thermal Printer is currently configured to transfer data using the FTP protocol, allowing any user in the network to launch a packet capturing tool and grab sensitive information such as user credentials and sensitive documents in plain text.</p> <p>FTP anonymous login is enabled, which allows anyone in the network to access the server and export sensitive files from the server. In addition, malicious files can be uploaded and renamed with the existing file.</p> <p>The FTP server is also vulnerable to an FTP server bounce attack, making it possible to force the remote FTP server to connect to third parties using the PORT command that allows intruders to use local network resources to scan other hosts, making it appear that the attack comes from inside the network.</p> <p>The FTP Server's TLS authentication implementation has a flaw that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.</p> <p>The ██████████ Thermal Printer's SNMP community string is changed, allowing any user in the network to obtain system information such as open ports and running services and can perform targeted attacks based on the information gathered.</p> <p>The ██████████ Thermal Printer is vulnerable to a cross-site request forgery (CSRF) attack on the web application, which could allow malicious users either inside or outside the network to capture credentials or cookies of the application.</p> <p>The ██████████ Thermal Printer is vulnerable to unauthorized changes through the use of the JetDirect service. ██████████ was able to change the display name of the printer to ██████████ and identified various other tools that are capable of reading all the print files and write malicious files to the thermal printer.</p>							

Hardware Risk Assessments (HRA) – IoMT Example (cont.)

	<p>The [REDACTED] Thermal Printer is vulnerable to a denial-of-service through an open 4000-port (remote-anything service). Sending a large input of arbitrary data to the service can render the server non-responsive to any user (Including legitimate users).</p> <p>In addition to the high rated findings mentioned above, multiple medium and low rated vulnerabilities were identified on the [REDACTED] Thermal Printer, including an expired SSL certificate and management of the thermal printer using the CUPS printing service.</p> <p>[REDACTED] requested remediation of the identified vulnerabilities from the vendor. In response to the vulnerabilities related to FTP and other insecure protocols, the vendor states There are no plans to disable the FTP or HTTP protocol on the print server. The FTP server stores limited data and is only used for "print protocol". A password can be configured for FTP, HTTP, and SNMP services on the print server as an additional level of security. Further, the vendor has declined to remediate all other vulnerabilities identified.</p>
Risk Rating Recommendation	<p>[REDACTED] should configure the Thermal Printer to perform input validation to protect against XSS vulnerabilities, ensure that the administrative page of the webserver is accessible only after authentication, change the default community string of the SNMP protocol on the printer, implement multiple security measures to mitigate CSRF attacks, password protect the server, and configure the server to Validate all input variable parameters that was sent from the client side. Further, [REDACTED] should configure a password for the FTP, HTTP, and SNMP services on the device.</p>

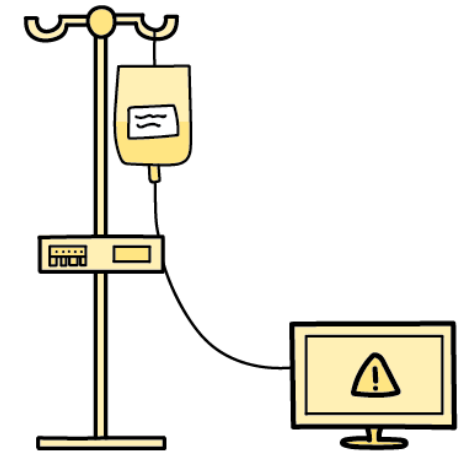
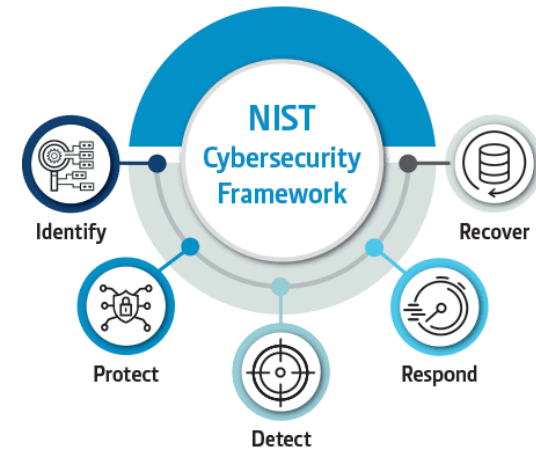
Hardware Risk Assessment (HRA): Exposing the Hidden Dangers

All new device types that have never been introduced into the production environment undergo a Hardware Risk Assessment. The key components of the HRA process include:

- **NIST-Based Assessments**
 - Evaluations are conducted based on the NIST industry standards to ensure compliance and security.
- **Vulnerability Scanning**
 - Perform vulnerability scans to detect potential security weaknesses.
- **Penetration Testing**
 - Conduct penetration tests to simulate real-world attacks and uncover vulnerabilities.

Common Issues Found During Assessments:

- **99% Critically Fail**
 - The vast majority of devices critically fail initial assessments due to serious vulnerabilities.
- **Default Usernames/Passwords**
 - Many devices come with default user credentials, posing a significant security risk.
- **End-of-Life (EOL) Operating Systems**
 - Devices frequently run outdated operating systems no longer supported by security patches.
- **Lack of Encryption**
 - No encryption for data in transit or at rest, even when Protected Health Information (PHI) is in scope, raising HIPAA compliance concerns.
- **Riddled with Vulnerabilities**
 - Devices are often loaded with vulnerabilities, making them easy targets for exploitation.



Vendor Collaboration Challenges: Overcoming Post-RA Obstacles

Engaging with vendors post-HRA can be difficult, as many lack the resources or understanding to resolve security issues.

- **Unresponsiveness and Lack of Security Expertise**

- Many vendors lack a dedicated security team or fail to integrate security into their product's lifecycle.
- Familiarity with common security standards, like OWASP, is often missing, leading to misunderstandings.



- **Reluctance to Fix or Prioritize Issues**

- Vendors frequently rely on third-party developers, making it difficult to prioritize security fixes.
- Security concerns often take a back seat to product features and functionality.

- **Misinterpretation of Regulations**

- Some vendors incorrectly cite non-existent FDA regulations as a reason to avoid implementing security patches.

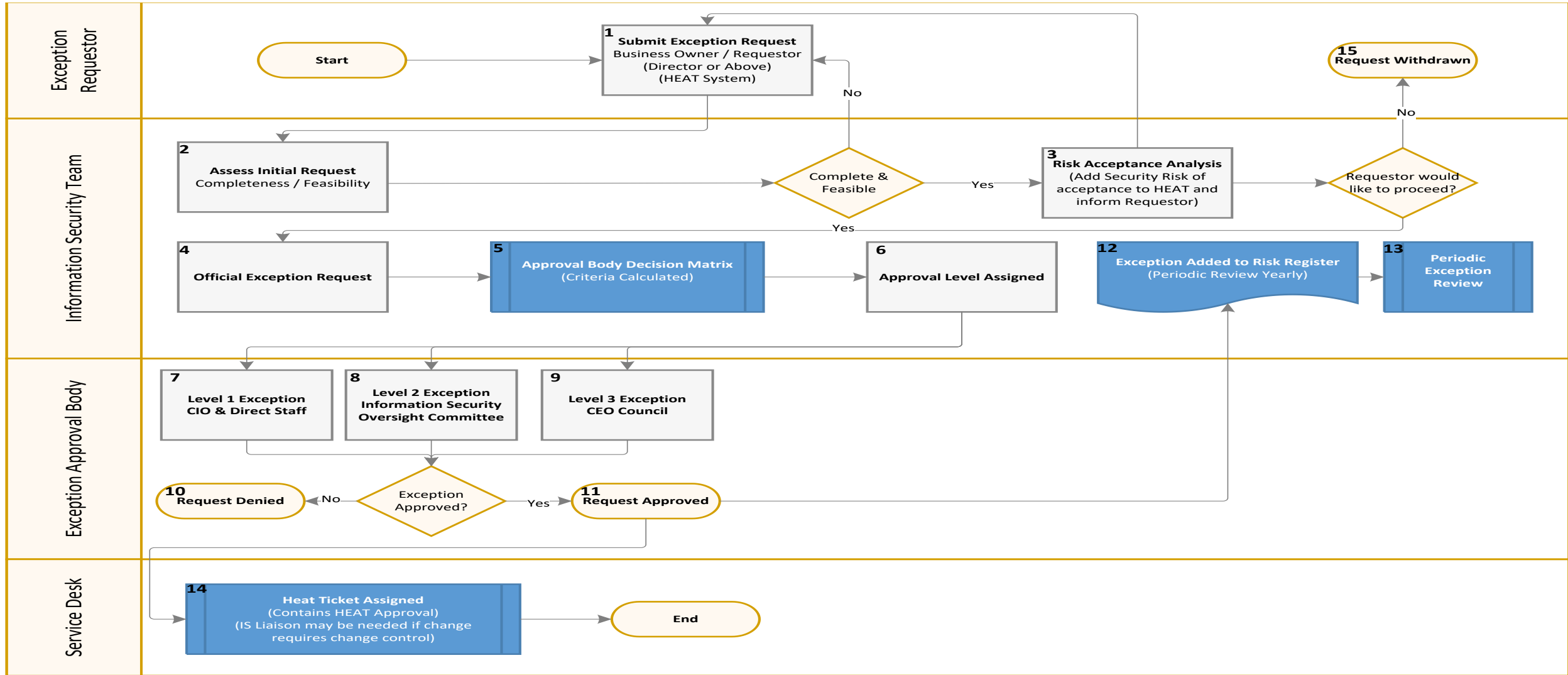


- **False Marketing Claims**

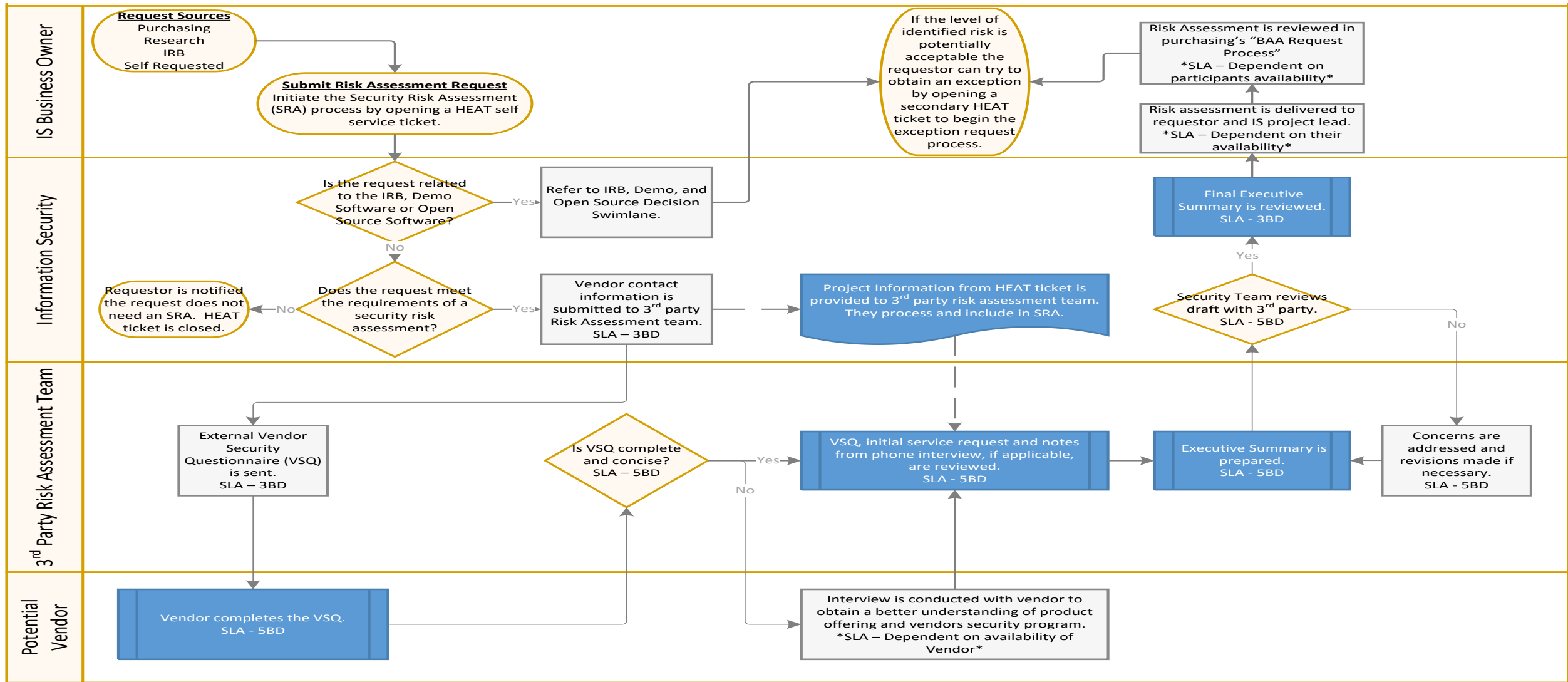
- Despite significant vulnerabilities, vendors often promote their products as “secure” and “HIPAA compliant,” creating a false sense of security.



Information Security Risk Assessment Process



Information Security Exception Request Process



Business Risk Acceptance: Balancing Security and Operational Needs

When device risks can't be fully mitigated, business leaders must make tough decisions to accept certain risks.

- **Formal Risk Acceptance Process**

- A structured process involving three committees, each composed of business leaders, reviews and approves risk acceptance based on the severity of the risk.

- **Limited Vendor Choices**

- Often, there are few or no alternative vendors for critical devices, forcing the acceptance of risks to maintain essential care functions.

- **Healthcare's Operational Imperative**

- In many cases, healthcare providers must accept insecure devices to ensure that critical medical functions are maintained.

- **The Reality of Insecure Devices**

- Despite clear vulnerabilities and ease of exploitation, some devices may still be deployed on the network, as healthcare needs outweigh the security risks.

Security Balance: Managing Insecure Devices in Critical Environments



Do We Tell the Business "No"?

Refusing to allow insecure devices may not be practical, especially when critical operations are involved. The goal is to find a balance between business needs and security risks.



Insecure Devices on the Network

Now that these devices are on the network and handling sensitive information (PHI, confidential data), how do we mitigate these risks effectively?



Segmenting the Network

Implementing network segmentation can help contain attacks or ransomware to a specific group of vulnerable devices.



Encapsulating Security

Isolate insecure devices on separate network segments with tailored access controls and monitoring. Alternatively, consider if full network segmentation is even feasible for the organization.

Can the Business Manage Network Segmentation?

- **Flat Network Reality**
 - Some businesses may not be equipped to manage complex network segmentation. In such cases, a flat network may seem more practical, but this introduces additional risks.
- **Vendor Device Hardening Issues**
 - Vendors often fail to harden devices or shut down unused ports, leaving vulnerabilities exposed. However, they typically provide a list of necessary ports.
 - **Example:** Many devices come with Telnet enabled, even though it's not required for day-to-day functions.




Implementing Security in Flat Networks

Port-Level Restrictions

- Centrally Managed Restrictions:** Implement centralized, port-level restrictions across flat networks to block unnecessary and insecure protocols (e.g., Telnet, SMB, HTTP Auth) on devices that don't need them.
- Whitelist Functionality:** Allow only systems that require specific protocols to bypass these restrictions, ensuring essential devices can still operate securely.

Blocking Insecure Devices by Default

- Any new device connecting to the network with insecure protocols is automatically blocked.
- Devices must either go through a formal exception process or be hardened before reconnecting.

 INSECURE PORT	
21 FTP	File Transfer Protocol (FTP) sends the username and password using plaintext from the client to the server.
23 TELNET	All information to & from the host on a telnet connection is sent in plaintext & can be intercepted by an attacker
25 SMTP	Simple Mail Transfer Protocol (SMTP) is the default for sending email messages. Since it is unencrypted, data contained within the emails could be discovered by network sniffing.
37 TIME	Time Protocol, may be in use by legacy equipment and has mostly been replaced by using port 123 for Network Time Protocol (NTP).
53 DNS	Domain Name Service (DNS), is still used widely.
80 HTTP	Hyper Text Transfer Protocol (HTTP) is the basis of nearly all web browser traffic on the internet. Information sent via HTTP is not encrypted and is susceptible to sniffing attacks
143 IMAP	Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing
445 SMB	Server Message Block (SMB), is used by many versions of Windows for accessing files over the network. Files are transmitted unencrypted.
389 LDAP	Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from servers to clients. Since LDAP is not encrypted, it is susceptible to sniffing and manipulation attacks.

What Can We do? Solution: Centrally Managed Port-Level Restrictions

Active Inspection and NMAP Scanning

- During active device monitoring, NAC performs an **NMAP scan** to enumerate open TCP/UDP ports, running services, and gather operating system details.

Example: Detecting Telnet (TCP/23)

- If **TCP/23 (Telnet)** is detected during scanning, the device's **MAC address** is added to a NAC-managed list called 'All Current Open Telnet Hosts'.
- From there, custom policies are triggered to control access for that device.

Example: Blocking Telnet Communication

- A specific rule can block **all Telnet communication** to that host, except for the vulnerability scanning appliances.
- This is achieved by applying an '**Endpoint ACL (Access Control List)**' directly to the switch port interface, enforcing strict control over vulnerable services.
- **Whitelist for Exceptions:** Approved devices requiring Telnet are managed through a predefined whitelist for exceptions.

```
root@kali:~/home/spect# nmap -SV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.00 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:13c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1068/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5800/tcp  filtered vnc-http
5900/tcp  filtered vnc
9929/tcp  open  nping-echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/

Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```



```
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open  http
443/tcp   open  https
445/tcp   filtered microsoft-ds
2000/tcp  filtered cisco-sccp
4343/tcp  open  unicall
5060/tcp  filtered sip
```


Stopping Ransomware Outbreaks

Blocking Ransomware-Spreading Ports

- For IoT/IoMT devices, all **non-essential ports known to spread ransomware** (e.g., **SMB/RDP**) are blocked across the network, reducing the risk of ransomware propagation.
- **Future Variants:** Although ransomware variants will continue to evolve, once the necessary port requirements for devices are known, all others can be systematically blocked to harden the network

PORT

3389

SERVICE

RDP REMOTE DESKTOP
PROTOCOL

PORT

139

SERVICE

SMB NETBIOS

PORT

445

SERVICE

SMB SERVER MESSAGE
BLOCK

PORT

23

SERVICE

TELNET

PORT

5900

SERVICE

VNC

Ransomware Kill Switch: Rapid Containment of Threats

Quick Containment with NAC Integration

- The **Network Access Control (NAC)** platform, integrated with existing network infrastructure, acts as a kill switch, rapidly applying **Access Control Lists (ACLs)** to block both inbound and outbound communication on common ransomware ports and protocols.
- This strategy helps to quickly contain, and isolate systems targeted by ransomware.



Your private data is no longer private

- **Widespread Data Breaches:** Major breaches like Experian and Equifax breaches have exposed vast amounts of personal data.
- **Private Data Exposed:** Sensitive information such as social security numbers, birthdates, cell phone numbers, and addresses are now accessible to attackers.
- **Shift in Privacy Paradigm:** The changing landscape where once-private information is no longer secure.
- **Phishing Tactics Evolve:** Attackers use available personal information to authenticate themselves or trick victims in phishing attacks.
- **Increased Vulnerability:** Accessibility of private data makes individuals more vulnerable to identity theft and fraud.
- **Authentication Challenges:** Difficulty in protecting identities when personal data is widely available to attackers.
- **Awareness and Vigilance:** Be more vigilant and skeptical, especially when personal information is used in communications.



Lock/Freeze all 4 credit agencies (Equifax / Experian / Transunion / Innovis)!



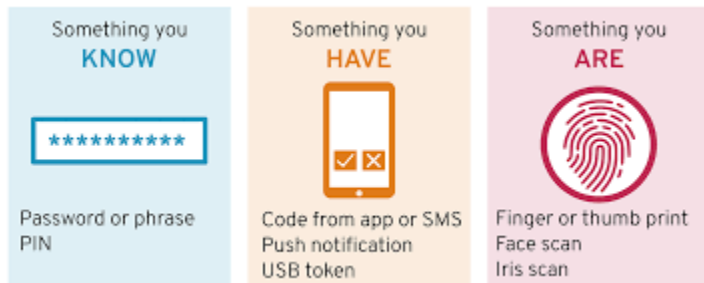
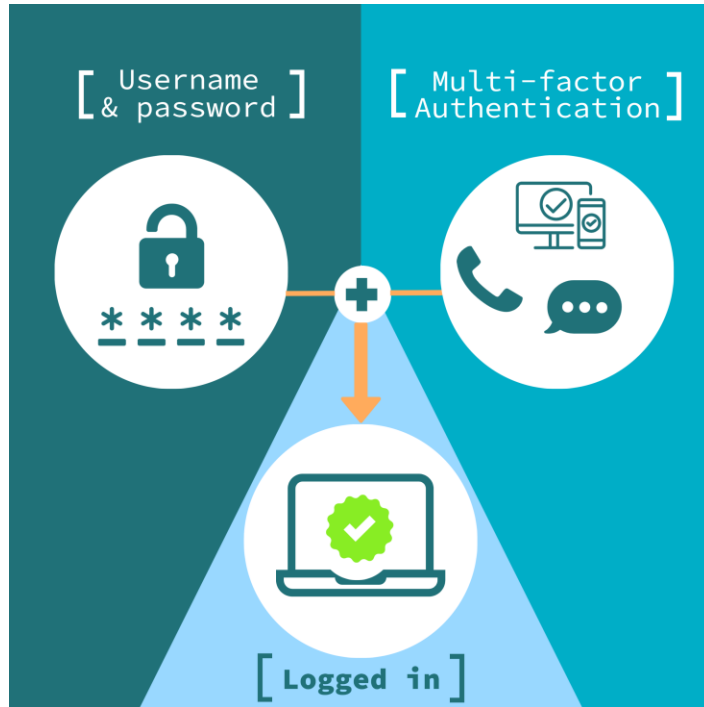
The Equifax Breach – A Global Settlement

- \$575,000,000+ settlement
- Free credit monitoring and identity theft services
- Strong data security requirements

➔ Learn more: ftc.gov/Equifax

Source: Federal Trade Commission | FTC.gov

Multi-Factor Authentication (MFA)



- Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity in more than one way when logging into an account. Instead of just entering a password, which can be guessed or stolen, MFA adds extra steps like using an authentication app or inserting a physical security key (such as a FIDO key). This makes it much harder for someone to break into your account because they would need access to multiple things that only you have. It's like adding extra locks to a door, making it more secure.

MFA Hierarchy

The Consumer Authentication Strength Maturity Model (CASMM)

Rank	MFA Type	Examples	Phishing Resistant	Vulnerable to
10	PASSWORDLESS	WebAuthN, FIDO2, YubiKey	Yes	Hardware Compromise, Force
9	CERTIFICATE-BASED AUTHENTICATION	Smart Cards, Client Certificates	Yes	Certificate Theft, Loss of Secure Storage Medium
8	WINDOWS HELLO FOR BUSINESS	Windows Hello for Business	Yes	Biometric Data Theft, Spoofing, Device Compromise
7	APP-BASED CODELESS 2FA	Some Microsoft Auth	No	MFA Fatigue Attack, Malware, Force
6	BIOMETRIC AUTHENTICATION	Fingerprint, Face ID	No	Biometric Data Theft, Spoofing
5	APP-BASED 2FA CODES	Authenticator, Authy	No	Malware
4	SMS-BASED 2FA CODES	Any SMS-based auth	No	SIM-Swapping
3	PHONE CALL-BASED 2FA	Phone call with code	No	SIM-Swapping, Phone Number Spoofing
2	EMAIL-BASED 2FA	Email with code	No	Email Account Compromise
1	EMAIL-BASED LOGIN LINKS	Email with logon link	No	Email Account Compromise

MFA (Multi-Factor-Authentication)

Bypass “Session/Token Theft” Protection

The 3 current ways of stopping today's MFA Bypass issues are as follows which we could install along side MS Authenticator for a backup method:

- **Certificate Based Authentication: (IS Managed / Hard to Manage Non-IS Managed Systems)** This requires the IT Department to install a Certificate that they manage on any device you wish to use for things such as email. That means even for your personal computer, you would need this certificate installed if you were to want to see corporate resources such as email. Your credentials won't work without this certificate, and the certificate only works on the piece of hardware that it is issued to.
 - This is not easy to deploy and manage for your organization. It is in most cases “Free” except for labor by utilizing your company's existing PKI (Public Key Infrastructure).
- **Windows Hello for Business sign-ins: (IS Managed Computer's Only)** Using a PIN, or Biometrics such as fingerprint or camera. Requires specific hardware with TPM and specific camera or fingerprint reader to use those functions.
- **FIDO2 Security Keys (YubiKeys):** Users need to possess this physical hardware-based key to gain access to their system.



Cost: \$25-\$105 each depending on model
Source: Yubico www.yubico.com

What can Compliance do to help?

Cybersecurity & Compliance Collaborative Approach



- **Support a Culture of Security Awareness**

- Actively promote security as a shared responsibility across the organization.
- Encourage training programs that educate employees on best practices, such as phishing awareness and secure password usage.

- **Enforce Compliance with Security Standards**

- Ensure that the organization adheres to established security frameworks (e.g., NIST, HIPAA, ISO).
- Hold teams accountable for maintaining these standards and help identify gaps during audits and assessments.

- **Encourage Vendor Due Diligence**

- Advocate for thorough vendor risk assessments, ensuring that third-party vendors meet security requirements.
- Push for remediation efforts when vendors fail to meet compliance and help ensure that insecure devices are addressed.



What can Compliance do to help?

Cybersecurity & Compliance Collaborative Approach



•Monitor Risk Acceptance Processes

- Ensure that risk acceptance decisions are properly documented and justified, especially when insecure devices are allowed on the network.
- Verify that there is a formal risk acceptance process in place and that it is being followed.

•Participate in Incident Response Planning

- Help the security team ensure that there are well-documented incident response plans, including for ransomware outbreaks.
- Confirm that these plans are tested regularly through tabletop exercises or simulations, and validate compliance with regulatory requirements.

•Advocate for Network and Device Hardening

- Encourage regular audits of network segmentation, port restrictions, and access controls.
- Help ensure that systems and devices are hardened according to security best practices by pushing for compliance audits of configurations.



What can Compliance do to help?

Cybersecurity & Compliance Collaborative Approach



- **Report and Track Vulnerabilities**
 - Ensure that any discovered vulnerabilities are properly tracked and managed through the vulnerability management process.
 - Promote regular auditing of systems to verify that vulnerabilities are patched in a timely manner.
- **Collaborate with Information Security (IS) Teams**
 - Foster open communication and collaboration between audit/compliance teams and IS security teams to ensure alignment in security objectives.
 - Assist in identifying where compliance and security overlap, helping the IS team address regulatory and business requirements efficiently.
- **Have Compliance target audits of security that are outside the responsibility of the IS Security teams.**
 - When IS is not responsible for patching IoMT devices, but the responsibility lies with a department or the vendor, audits should verify whether the necessary patching is being performed. Additionally, the audit should check whether the department is managing the vendor relationship effectively to ensure security obligations are met.



Questions?

