Vulnerability Management Blueprint for the Clinical Environment

Adi Sitnica

STI Template Version May 2018

Vulnerability Management Blueprint for the Clinical Environment

GIAC (GDSA) Gold Certification

Author: Adi Sitnica, adi.sitnica@gmail.com
Advisor: *Jonathan Risto*

Accepted: *March 4, 2021*

Abstract

The industry-standard vulnerability management process is largely inapplicable within clinical settings. Unique medical industry-specific devices and other complexities and limitations, such as vendor-owned and managed systems and regulated and other non-standard hardware, limit the general effectiveness of the process. This document explores a standard clinical footprint and provides guidance (or a 'blueprint') to further developing and maturing the vulnerability management operational model for clinical settings, with the primary goal of risk reduction within the confines of a clinical environment.

1. Introduction

The healthcare vertical has been working to catch up to other industries in information security posture and defense-in-depth maturity, not because of lack of talent or expertise, but because of complexities within the vertical such as lack of security in products, non-technical staff, and non-technical priority for care. Without technology, care can still be provided and is usually the backup process for the vertical when it comes to technology outages. As a result, can we utilize the foundations and lessons learned outside of the healthcare sector to help? Yes, but with a caveat, it is not a one-to-one conversion. The healthcare sector is unique, and so is the clinical environment that it utilizes. According to IBM Security (2019), "For the ninth year in a row, healthcare organizations had the highest costs associated with data breaches at $6.45 million – over 60 percent more than the global average of all industries." That trend also continued in 2020, with an increase of 10.5% over the 2019 study. So what makes up a clinical environment that makes it that hard to protect? First and foremost, the healthcare sector is an industry that has technology secondary to its primary objective, which is patient care. Patient care has to happen whether the technology is there or not; the idea is to utilize technology to support patient care, but it is not a silver bullet, similar to how no singular cybersecurity solution is a silver bullet.

The approach to cybersecurity within a clinical environment has to incorporate the limitations and provide a pathway for implementation that is not overly complex while still keeping the business running, or more precisely, treating patient care as its number one priority. Drastic modifications cannot happen overnight, as technology changes require adjustment, training, and adaptation by the clinical staff that operates the equipment, the maintenance staff that supports the equipment, and the need for the equipment to work as expected for patient care. Unlike other industries where corrections can happen with erroneous data, this can directly impact patients and their well-being in the healthcare vertical. Migrations to newer or different technologies thus have a much more complex pathway and rigor to achieve. Finally, from the vantage of patient care and even the business, if legacy equipment is working for its responsibility or task, why should we make adjustments? This question is vital to understand, as increasing the

security posture of legacy equipment does not always result in buying new equipment. Securing a medical device using Fort Knox mentality implicates the inability to sustain the clinical environment for its primary objective. It is a balance of understanding the context of the operation, the budgetary model, the impact on patient care, both from well-being and financial implications.

Patient data or, more specifically, Protected Health Information (PHI) of an individual within an Electronic Health Record (EHR) contains a digital version of a patient's chart. However, it also includes their medical history, administrative and billing data, diagnoses, immunizations, allergies, and other information from all clinicians involved in a patient's care, which creates an attractive set of data. Healthcare continues to see an uptick in malicious activity, as noted in the IBM Security report and many others, which directly correlates to a healthcare record's value. Comparatively, through a study commissioned by Trustwave (2018), a healthcare record fetches $250.15, compared to payment card details that go for $5.40 or a social security number worth less than a dollar. This significant difference attributes to multiple components of individual data and time-to-act on such data; medical information does not change quickly. For example, if you are diagnosed with a disease, it does not go away the same day. However, if your credit card gets stolen, you can immediately call your bank to report and replace it. Information from a healthcare record also has different values based on circumstances, for example, information on a celebrity or government official versus an average individual. Malicious actors can weaponize that information against the individual (leak the information out) or utilize it for gains, such as creating fake claims with insurers or counterfeit identities to purchase medical equipment or drugs.

Also, a significant shift due to the global healthcare crisis (COVID-19), with organizations moving to remote work, paying ransoms to get data back from ransomware attacks, and the clinical environment landscape is quickly taken advantage of, with high-value and gaps within the clinical setting. To put that into perspective, during a webinar hosted by Aspen Digital (2020), FBI Deputy Assistant Director for the Cyber Division, Tonya Ugoretz, stated that the Bureau's Internet Crime Complaint Center now receives

3,000 to 4,000 cybercrime reports per day, which is up from 1,000 before COVID happened.

As indicated through yearly reporting on the healthcare vertical, Verizon (2020) also aligns with an uptick trend, showing data breaches increased in the sector from 304 in 2019 to 521 in 2020. Financial motive continues to be the primary objective, with ransomware keeping momentum due to organizations in the vertical continuing to pay the ransom, making the industry a preferred target. However, this is only a portion of the narrative; financial success by malicious actors in tandem with the sector "branded as easy targets with obsolete defenses and poor IS and IT organization" (Le Bris & El Asri, 2017) continues to drive the need to improve.

This research does not go into the details of the approval chain of medical devices and the continuous evolution and enhancement of security within, or what other corporations and non-profits like MITRE are doing to help improve medical devices' security posture. Instead, it examines the clinical environment from the vantage of what can be done right now, with the historical and current limitations and gaps.

2. Research Method

The approach to tackling the vulnerability management operational model in a clinical environment requires understanding the clinical landscape. While there are many different healthcare eco-systems: from hospitals and emergency care to urgent and primary care to specialty care and surgery centers, at the foundation, a similar set of processes and medical equipment is utilized, albeit with different scales and expectations related to the technology. For example, in a primary care setting, the loss of technology is not as critical as it may be within a surgery setting, where the use of technology may be vital during active operation. As such, cybersecurity also has a different meaning and approach. The research conducted concentrates on building an environment with various sets of equipment that have different utilizations through the eco-systems and showcasing limitations and actuality within the clinical setting, followed by iterative research to showcase methods towards improvement. A baseline must be set to be measured against, with the expectations being the implementation of various configurations, additive tools,

process changes, and inquisition as a means for reproducible and, more importantly, actionable tasks for the reader. The baseline created via the build of a mock clinical environment tackles a broad set of differential equipment, all with unique challenges. For most, especially non-information security professionals, the idea of tools like Antivirus seems sufficient for such environments when the reality is furthest from that perception. TrapX Research Labs' demonstration in their Anatomy of Attack report (2016) analyzed three incidents in which healthcare institutions were the target of persistent cyberattacks. It included three different clinical environments and devices used as a pivot to attack the organization: an X-ray system, a picture archive and communications system (PACS), and an oncology system. Each had unique scenarios. The fundamental issue is that they cannot be secured in the same manner as the rest of the organization's equipment due to various limitations and complexities, which leads to exploration on how to tackle each set of equipment through a mock lab.

2.1. Background

The mock lab built and utilized mimics a clinical eco-system from the vantage of distinct silos of equipment; however, the design and brainstorming started with a concept, as shown in Figure 1. The concept progression resulted in building out the mock lab. It contains multiple standard Information Technology (IT) workstations, running on a Microsoft Windows Operating System (OS) 10. Health care staff typically use those for various activities surrounding patient data entry, access to collaboration tools, self-service, and access to the internet. The infrastructure that connects them is using a standard network backbone (switch/router, firewall).

On the healthcare side, multiple components make up the eco-system. First, a mobile device (iPad/Laptop), which healthcare staff typically use as a scribe-function, allowing them to stay mobile, move around with technology at their hands, and access data entry across various clinical settings from patient room to room. Second, an audiometer evaluates a patient's hearing acuity. Third, an X-ray workstation that houses modality software connects to either a computed or digital radiography (CR/DR) machine, which converts the X-ray images and digitizes them, sending them to the X-ray workstation for review and processing. Fourth, a drug screening workstation and a

temperature sensor, used by healthcare staff to keep temperature measurements for medications and other medical needs.

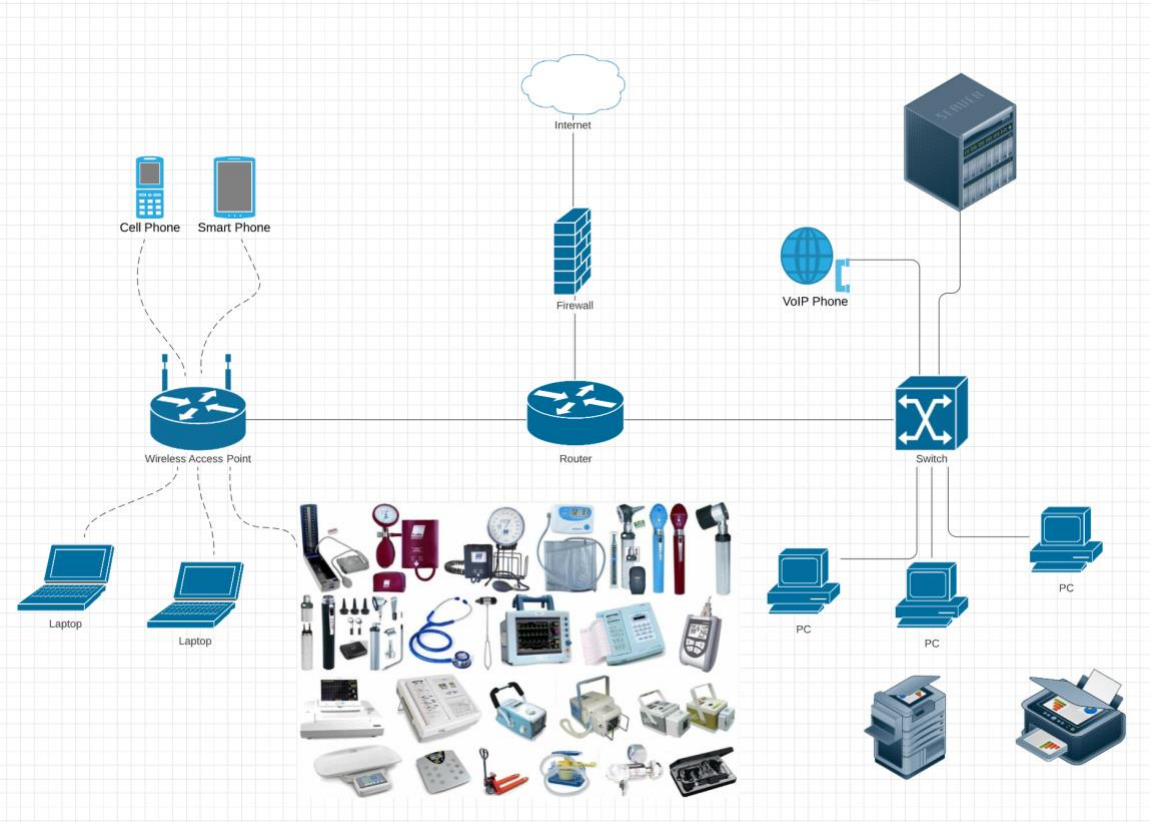


Figure 1 – Clinical Mockup Lab Concept

2.2. Baseline

Developing starting data was accomplished using a baseline for the iterative measures to provide increased value. The clinical environment was set up in a simple manner using a flat network, providing full-spectrum network visibility and access internally and only limiting external access (lax configuration/default) across the firewall. Historically a standard approach for ease of interfacing and connectivity, flat networks are unfortunately still utilized across the healthcare vertical, as described by Rob Bathurst (2015), in addition to accentuating gaps in less secure clinical message protocols (Dameff et al., n.d.). The clinical environment includes basic identity configuration and roles, separating administrative use and user utilization, except those distinct silos of equipment where it was limited, whether contractually or operationally. Overall, the equipment used

the closest options to a default configuration, which included active directory domain join, but without enhanced security policies (GPOs or otherwise). It also contained equipment in workgroups that were not under the purview of organizational IT maintenance. No security tools were part of the baseline outside of standard anti-virus software, where possible, capability-wise and contractual-wise.

2.2.1. Risk Assessment / Security Posture

A risk assessment performed at a high-level showcased gaps in a default baseline setup. It included the network architecture, hardware, and software inventory (asset management), application landscape (generalized for anonymity), security systems (generalized for anonymity except for open source/free tools), configuration, process (basic), and documentation availability. The high-level findings were as follows:

- Secure and insecure equipment on the same network.
- Uneven playing field from the vantage of maintenance such as patching and configuration.
- Anonymized and Administrative logins possible due to limitations with medical software.
- Lack of security hardening for the general operating systems, such as removal of unused services or enhanced configuration to limit the attack surface.
- Lack of security hardening for clinical applications, such as anonymized login and no authentication necessary.
- Lack of mobile device management for equipment with legs and lack of security hardening for both the operating system and its apps, including gaps such as PIN login or direct no password login.
- Utilization of shared user credentials for equipment that is not uniquely assigned.
- Lack of full-stack patching, including security, application, hotfixes, and upgrades/service packs.

- Lack of lifecycle management of equipment.
- Utilization of end of life/support equipment, hardware, and software.
- Inclusion of insecure equipment such as unmanaged hubs, or unmanaged access points, and default configured printers.
- Inability to streamline security via global plane by including equipment managed by multiple independent parties (vendor/manufacturer, 3rd party, internal staff) on the same communications bus.
- Lack of staff training on maintenance and utilization of equipment from an information security perspective.
- Lack of vendor/manufacturer default secure configuration or best practices/documentation to secure equipment readily available.
- Lack of vendor/manufacturer flexibility to support security tools on top of their equipment, invaliding warranty, support, or lack of security expertise for niche medical equipment.
- Lack of information security professionals with expertise and knowledge to secure such an environment without impeding business under the guise of transformation or innovation.
- Lack of training for clinical staff utilizing the equipment.

The approach aligned with the expectations of standard information security hygiene and HIPAA/HITECH requirements to identify vulnerabilities through an organization's risk analysis. Security risk assessment tools such as from The Office of the National Coordinator for Health Information Technology (n.d.) are valuable references when performing risk assessments or understanding the current state.

2.2.2. Vulnerability Scan

A vulnerability scan ran with and without credentials (intrusive & non-intrusive) to set a baseline for common vulnerabilities and exposures. The scan targeted Windows-based endpoints and different operating systems such as Cisco IOS, Linux, Apple iOS,

and Android. The tools utilized were enterprise-grade (hidden) and freely available tools (Nmap/Zenmap, Wireshark).

The first baseline scan was done on the flat network and showcased multiple missing assets and did not match physical asset management tracking expectations. Due to the knowledge of the exact count of assets during the baseline build, a correlation resulted in further understanding of discrepancies. Multiple devices were downstream of the scan, meaning the scan covered the IP subnet (flat network), but it did not scan radio waves on the backend (temperature sensors), nor was it able to pick up on serial/USB-attached components (audiometry equipment). Some of the equipment was filtered, and only an intense scan or NetFlow analysis would showcase further details. A credentialed scan showed more critical vulnerabilities than a non-credentialed scan, in addition to noting restricted or unknown access to 3rd party-managed or vendor-owned equipment.

Without concentrating on the vulnerability management product, the intent is to showcase the equipment's various vulnerabilities, utilizing multiple methods, not merely a vulnerability scan using an enterprise or open-source tool. The E-Book (Kandek, 2015) is a quick high-level guide with further detail on vulnerability management.

The intended driver is to showcase and prioritize the gaps with the system, or more specifically, to reduce easily exploitable vulnerabilities. E.g., for which code or methods are freely available on the internet or against equipment prone to remote attacks, such as internet-facing equipment, as depicted in Figure 2.

	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged
Automated Exploit	0	1	8	10	0	2	0
Easy	0	4	30	11	0	1	0
Moderate	0	0	2	0	0	0	0
Difficult	0	0	5	1	0	0	0
Extremely Difficult	0	0	4	4	0	0	0
No Known Exploit	226	66	787	463	11	4	5

Figure 2 – Windows 10 example of Vulnerability Count Risk Matrix

A visual on open ports/services is vital to understand each piece of equipment from an external and internal perspective, achieved via Nmap/Zenmap, Wireshark, and local capability such as netstat. In this case, the desired output is understanding what ports are externally accessible and what internal ports/services are open. The example

information of interest is similar to locating that a specific piece of equipment shows TCP/23, 139, 445, 3389 open from an external perspective. That allows one to scrutinize each port further and understand what one can do. E.g., if TCP/23 port is open, eliminate telnet as it is a legacy protocol and clear-text, or come up with an alternate strategy if it is required.

Also, an attack tree analysis is an excellent method to help visualize and think about the various scenarios against a piece of equipment, or even take it a step further and use it to prioritize actions based on the calculated cost of an attack. Schneier's (1999) explanation of modeling security threats provides a glimpse into utilization:

> Attack trees provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security. Security is not a product — it's a process. Attack trees form the basis of understanding that process. (Conclusion)

2.2.3. Actuality Assessment

An analysis performed against the mockup lab showcases the boundaries and limitations of the equipment as follows:

1. **Information Technology wired equipment.** (workstation(s), server(s), networking equipment)
    a. This equipment is standard IT with the following general use-cases:
        i. Workstation(s) are for entry gateways to application landscape, data entry, and the internet. The mockup lab uses four of such workstations.
        ii. Server(s) are for infrastructure needs such as Domain Services. The mockup lab uses multiple servers, mainly out of this analysis's scope, except to use its services.

iii. Networking equipment is for the communications requirements for internal and external communication. The mockup lab uses a switch, router/firewall, access point, hub, and mi-fi.

2. **Information Technology wireless equipment.** (iPad, laptop)
    a. This equipment is standard IT with the following general use-cases:
        i. Laptop(s) are for knowledge workers and mobile needs. The mockup lab uses a single laptop.
        ii. iPad(s) are for mobility requirements of staff. The mockup lab uses a single iPad.
3. **FDA-regulated and 3rd party-managed equipment.** (X-ray machine, computed and digital radiography (CR/DR) machine)
    a. This equipment cannot be updated using the standard IT mechanism as it will be out of agreement and warranty if done in such a manner. A specific vendor maintains FDA-regulated equipment under scrutiny to adhere to the applied mechanisms, including validation and testing of equipment for its role under patient care purview. Any deviations from the standard have a direct implication on the agreement with the vendor to support it and its data being correct. The mockup lab uses an outdated workstation connected to a CR machine and a current workstation connected to a DR machine.
4. **Vendor-owned and managed equipment.** (drug screening)
    a. A unique situation where no action can be done with equipment by the customer, as it is wholly owned and maintained by the vendor. The limitations are that it is sitting on the customer's network and requires egress to the internet (to vendor's home-base) for its functionality.
5. **Vendor managed and Customer-owned equipment.** (X-ray viewing station, temperature sensor kit)

   a. Like FDA-regulated equipment, the vendor has strict guidelines concerning configuration and control flexibility, such as assigning network addressing and specific ports. Deviation from the guidelines has implications on warranty and support. The mockup lab uses a vendor-provided temperature sensor and gateway. The X-ray viewing station uses one of the standard workstations under the IT wired equipment purview, with additional software and needs.

6. **Software on top of OS-stack.**

   a. The audiometry hardware plugs in via a serial or USB cable to a workstation under the IT wired equipment purview by adding additional software.

The derivative of boundaries directly impacts the ability to adjust the security posture, whether through patching, configuration change, isolation, or other means.

2.3. Iterative Approach (Quantitative)

The goal is to achieve a baseline set of data followed by an iteration of changes on the security front, providing visibility and reproduction capabilities. The iteration includes segmentation, patching, configuration change, and reproducible actions in one's environment.

3. Data Exposition

The total starting baseline has 24 components, 11 of which are medical components, and the rest are technology components used for communication and foundational layer for software to sit on or as a mechanism to interface to various clinical needs. The concentration is not networking or server-side devices but rather devices with an internet protocol address for this whitepaper. As a result, the asset count target count is 13.

For comparison transparency, an Enterprise VM tool shows 23 assets, a Nmap/Zenmap scan shows 21 assets that responded, and visibility from the network

switch shows 11 assets (current) and 13 assets (a week prior). Due to the discrepancies between systems, further analysis shows the reasoning is multi-fold:

- multiple ports on networking equipment resulted in multiplied results for the same equipment,
- unresponsive equipment (due to intense vulnerability scans),
- incorrect segmentation configuration pulling in equipment out of scope,
- the location of scans (external/internal) was also differential.

Thus the total asset count as intended for this whitepaper is 13, which does not count server-side, network, nor software, as shown in Figure 3.

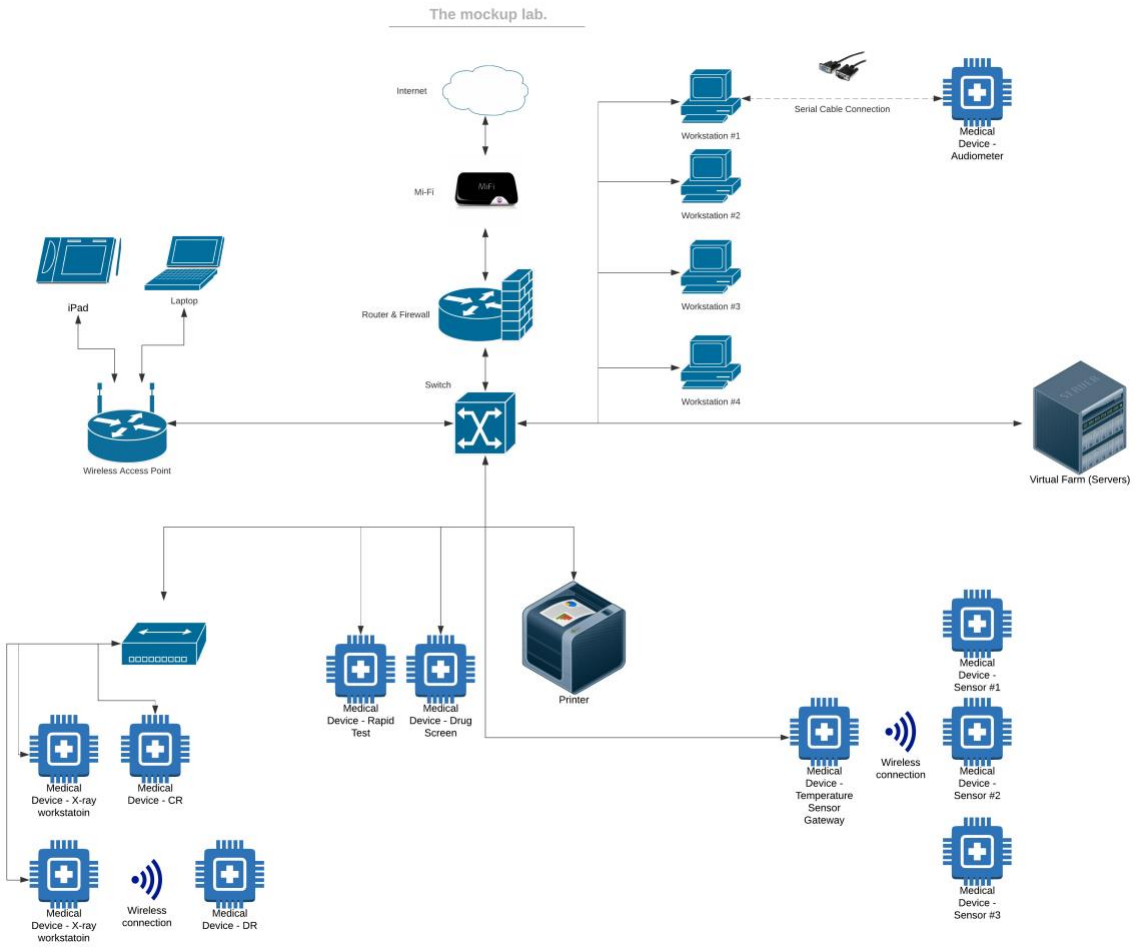


Figure 3 – Actual Mockup Lab

The research does not emphasize physical security or privacy, but both are essential in the overall risk awareness and reduction.

3.1. Baseline Posture (IT wired equipment)

The baseline posture of IT wired equipment is as follows:

- Windows 10 workstations and Xerox printer.
- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: MS Windows 10 Enterprise, Build 1809, and Xerox.
    - KBs installed: OS Patch level February 2020 (Security-only) and N/A for Xerox (firmware-based).
    - Applications: General applications (Office, Browser, etc.) and Clinical applications (Electronic Medical Records (EMR)/Electronic Health Records (EHR) System, Medical Billing (MB)/Revenue Cycle Management (RCM) System).
        - Default install: no patches, service packs, upgrades.
- No host-based firewall restrictions except for the default operating system firewall enabled on workstations. N/A for Xerox.
- No security tools except for anti-virus software enabled on workstations. N/A for Xerox.

3.1.1. Enhancement / Amalgam

The first step is to recognize that this specific silo of equipment (IT wired equipment) is the simplest to enhance because of ownership and full control by the organization. That said, depending on the criticality of clinical workflow, capability execution may differ. To start, unlike a standard laptop used for email and intranet, a clinical workstation will house software that either interfaces with clinical hardware or other software located elsewhere, such as within a data center or the cloud. While the approach is to patch to the same level as the rest of IT equipment, the differential here is the additive clinical software, which requires adding specific patching and configuration

mechanism, as described in Section 3.6. For the instance of the baseline OS, the concentration should lie in the following:

- Patch OS to the latest available level without upgrading to a newer version. Note unsupported versions based on releases and tier of the operating system, which dictate the end of life/support of a specific version. *Be ahead of the end of life/support!*
- Include 3rd party patches and non-security patches, such as Adobe, Java, and Office patches.
- Add specific enhanced group policies (CIS benchmarks) to the operating system (system hardening).
    - Limit access, and enforce strong authentication (MFA).
- Add security software (Anti-Malware, EDR, Continuous Scanning (VM)).
- Enhance the firewall rules from default.
    - Network segment as necessary.
- Add a privacy screen, especially if the equipment is patient-facing, and consider shorter time-frames for locking the screen, including enabling HIPAA-related screen savers.
- Educate clinical staff, via security awareness, to lock equipment at any point when not directly in attendance. Note this may require providing ease of re-authentication methods, else the impact of continually having to re-authenticate would be adverse to the business productivity and cost.
- Update firmware and connect the printer to a remote management interface, allowing streamlined configuration and control.
    - Enable secure print (physically require authentication at the printer, to print).

Each of the additive security enhancements varies in complexity and cost, and the approach should investigate organizations' capability for each and fastest, most

straightforward execution. Instead of adding all of the various security functions and enhancements, have the analysts step back and look into which portion is the easiest to execute, from both timing and budgetary aspects. For example, if the organization already has a patching mechanism, whether Enterprise or as simple as adding a role to a server with Windows Server Update Services (WSUS), then look into enhancing that function to add 3rd party patches or upgrades (such as service packs). In most cases, this is simply a configuration change. However, patch management is a continuous process that requires a standard cycle of testing, validation, and execution.

Organizations should not get stuck on execution with perfection; instead, use the mindset of iterative improvement, which also means tackling multiple concentrations with the intent to improve over time. For example, implementing the entire CIS Level 1 Benchmark for Windows 10 may impact clinical workflows, but a sub-set of the configuration will result in better posture than currently held; thus, choose iterative improvement than no action at all.

Depending on whether an organization's limitations are staff, budget, or time, incorporate those limitations into the plan. Suppose we can add security hardening by investing in labor-only, whereas adding security software requires labor and a budget that is not available. In that case, you can still improve with the limitations handed to you by selecting to pursue security hardening and considering requesting a budget the following budget cycle for security software.

3.2. Baseline Posture (IT wireless equipment)

The baseline posture of IT wireless equipment is as follows:

- Windows 10 laptop and Apple iPad.
- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: MS Windows 10 Enterprise, Build 1809, and Apple iOS 13.3.1.
    - KBs installed: OS Patch level February 2020 (Security-only), roll-up to iOS 13.3.1 (January 2020).

    - Applications: General applications (Office, Browser, etc.) and Clinical applications (Virtualization gateway, EMR/EHR, MB/RCM, Audiometry software).
        - Default install; no patches, service packs, upgrades.

- No host-based firewall restrictions except for the default operating system firewall enabled.
- No security tools except for anti-virus software enabled on the laptop.

Note that mobile devices such as iPads and other tablets make the clinician workflows more effortless and sometimes require such devices to utilize a kiosk mode. This locked-down mechanism specifies what the users have access to or can run, such as a pre-defined set of applications and actions. It pushes the security posture up the stack, towards the application-side, such as authenticating specific applications even though the iPad itself (hardware-level) may not require it.

3.2.1. Enhancement / Amalgam

Unlike wired equipment, wireless equipment is harder to control as traceability is a factor. For the iPad (or any Android-based equipment), control and management mechanisms are not the same and require an additional layer such as mobile device or application management (MDM/MAM). The idea behind it is the same as your standard IT equipment; to control the equipment, force a secure configuration and patching/updates, and provide visibility into the equipment.

The concentration for IT wireless equipment should lie in the following:

- Enroll all mobile devices within an organization in an MDM/MAM system.
    - Setup and configure a Device Enrollment Program (DEP), even without MDM/MAM, for traceability and ownership.
- Patch OS to the latest available level. Note that the rate of EOS/L is higher on mobile devices, requiring upkeep in versioning at a faster pace than standard equipment. Like IT wired equipment, it is even more important to be ahead of the end of life/support with mobile devices.

- Include application updates (iOS app store updates or applicable mobile OS store updates).
- Add a privacy screen, especially if the equipment is patient-facing, and consider shorter time-frames for locking the screen, pending kiosk mode, or similar does not negate the need.
- Add security hardening, which similar to group policies, also have settings/configuration available via CIS benchmarks but use different implementation mechanisms.
- Add security software (Anti-Malware, Continuous Scanning (VM)).
    - Note that the utilization of MDM/MAM can provide a continuous vulnerability/risk stance.
- Segment wireless guest and production, force organizational assets to log into production wireless automatically, or if not available, VPN home, or utilize MDM/MAM functions for application wrapping across a VPN.
- Require unique user authentication other than when it is not possible, such as a kiosk operation where a shared account is necessary. In the latter kiosk operation, limit functionality using a default-deny mentality.
    - Train clinical staff on mobile device security.
    - With shared accounts, enhance security up the stack to account for the limitations, including a whitelist type-approach, by allowing only the exact required functions and nothing else.

Like the approach with IT wired equipment, wireless is directionally the same, except the management functions require different mechanisms. The criticality choice depends on the utilization of IT wireless equipment. In the case of a laptop, the only difference between it and a stationary workstation is location, which is mobile. In most cases, laptops have a 1:1 use, meaning that a laptop typically has only one assigned individual. On the other hand, multiple users often use an iPad within a clinical environment, frequently requiring shared accounts. As a result, the device's security is

going to be laxer, and that the emphasis on security should aim towards the applications the device accesses. The big concern surrounding mobile devices is if the data, such as PHI/PII, is stored locally, which may not be under the protection of physical security of a location. Therefore, it is more susceptible to loss of hardware, resulting in the need for remote wipe or forced encryption to limit or lower the risk with lost assets.

As with the iterative approach, consider the differences between security on a laptop and iPad, and work backward to understand capability. For example, one can leverage the same patching mechanism (WSUS) to patch a Windows 10 laptop; however, one cannot utilize the identical solution for iOS or Android without additional modules or products. The priority should lie in the visibility and management of such equipment using MDM/MAM. Depending on the organization's size, there are solutions available freely, as well as paid. Cost should never be a deterrent for security posture, as all security functions can be done free of cost (minus labor), albeit with different results, and this holds valid for MDM/MAM as well.

Once the capability is within the organization to be aware, and in control of mobile devices (i.e., MDM/MAM), the next step should be in alignment with the operational model of IT wired equipment. However, the prioritization might be different due to the limitations and needs of mobile equipment such as iPads.

3.3. Baseline Posture (FDA-regulated and 3rd party-managed equipment)

The baseline posture of FDA-regulated and 3rd party-managed equipment is as follows:

- X-ray machine and CR/DR equipment.
- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: MS Windows 7 Standard, Build 1809.
    - KBs installed: N/A.
    - Applications: Clinical applications (X-ray software, Communications/Storage Bus).

    - Default install: no patches, service packs, upgrades.
- No host-based firewall restrictions except for the default operating system firewall enabled.
- No security tools.
- No local password authentication through application shortcut.
    - Able to log into the system with administrative rights without a password.
- Remote access software required for 3rd party to maintain equipment remotely, introducing additional vulnerabilities.

3.3.1. Enhancement / Amalgam

There is a common misconception that because the equipment is FDA-regulated, we cannot implement security enhancements akin to our standard IT equipment, or for that matter, 'touch' the equipment. That is the farthest from the truth, as medical equipment that is FDA-regulated is under continuous scrutiny, which requires both the manufacturers and healthcare organizations to play a role in securing the equipment. Further detail and guidance provided by the U.S. Food & Drug Administration (n.d.) states, "The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product lifecycle, and incentivize changing marketed and distributed medical devices to reduce risk."

The difference in approach versus standard IT equipment is understanding boundaries and capabilities. From the business perspective, if medical devices, whether they are FDA-regulated or not, work as intended for patient care, then adjusting those devices further is not in the interest of patient care, but rather patient privacy, organizational security, or compliance motivations. Adding functions or modifying the configuration of FDA-regulated equipment can have a negative impact, especially if a 3rd party maintains that equipment. Changes or utilization of internal tools that the 3rd party does not have access to creates a complex landscape to support. The first action is to

understand the 3rd party management duties, followed by understanding flexibility with FDA-regulated equipment. The involvement of both parties is key to a successful improvement, again from the iterative approach perspective. Each manufacturer that obtains FDA approval will have best practices from a cybersecurity perspective and specific information on what is validated to work with or is known to have no impact on its equipment. Examples include particular patches that do not break the X-ray mechanism or security tools known to work without adverse impact. These are key to understand when taking this journey to improve the security of the FDA-regulated equipment. It is not just the manufacturers or the FDA, but a combined effort for medical device cybersecurity, as described by U.S. Food and Drug Administration (n.d.).

The concentration as such should be as following:

- Understand manufacturer best practices in cybersecurity and obtain information on what security tools or actions (such as system hardening) are available to have been validated to work with the FDA-regulated equipment.
  - Align to those best practices as a first step in the iterative approach.
- Based on the output of manufacturers' details, work with the 3rd party to implement said functions. Examples include approved patches or security tools.
  - If no security enhancements (tools or configuration) are approved, work with the manufacturer to improve this aspect.
    - If this is limiting due to time-investment from an organizational perspective, consider alternate vendors or isolate equipment entirely from the rest of the environment, thereby eliminating or drastically reducing the ability to pivot or utilize less secure equipment to attack other organizational equipment.
- A critical need will require dedicated equipment for testing and validation. Since the 3rd party manages the equipment, utilize them to perform this testing with your organizational enhancements, such as adding internal tools (WSUS, AV,

etc.). Document the ask and iterative steps, as if a failure is detected, traceability of actions is crucial.

- Dictate connectivity and process, through the 3rd party, on how to set up and maintain this equipment. The 3rd party that supports this equipment will most likely require remote access to this equipment, which opens up additional vulnerabilities on top of the limitations already noted with the equipment. Force a secure mechanism aligning to the standard organizational solution for such 3rd party access.
- Incorporate medical devices into IT lifecycle management, replacing or upgrading equipment. If the organization has no funding for such activities, provide costs associated with the upkeep of equipment in a segmented fashion due to the limitations of keeping legacy hardware or software.
    - The cost of continuing business is not free, as maintenance is a factor, especially if supporting in a segmented fashion where standard costs (at scale) are not available.
- Do not assume FDA-approved equipment is a black box with no flexibility, as that is furthest from the truth.
    - Utilize the relationships and partner on improving the security posture for the good of the patient.

3.4. Baseline Posture (Vendor-owned and managed equipment)

The baseline posture of vendor-owned and managed equipment is as follows:

- A drug screening machine. Built-in computer running Windows 8.
- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: MS Windows 8; workgroup.
    - KBs installed: OS Patch level February 2018. (Security-only)
    - Applications: General applications (N/A) and Clinical applications (hidden).

        - Default install: no patches, service packs, upgrades.
    - No host-based firewall restrictions outside of the default firewall enabled.
    - Local administrator login enabled with weak or no password.
    - Standard AV installed.
    - No standard lifecycle maintenance, including patching, except virus definition file updates (automated)
    - No vulnerability assessment/continuous scanning.

3.4.1. Enhancement / Amalgam

Unlike other silos of equipment, the vendor-owned and managed equipment is almost entirely out of the organization's control, except the vendor's selection. As such, the selected vendor should be a partner who is willing to work with your organization to improve the security posture mutually. The concentration should be as following:

- Discuss partnership with the vendor to enhance security.
    - Request service-account or access to perform a credentialed scan and share results with the vendor.
        - Set up a cadence of the scan and operational model on actions based on results.
    - Work with vendor to create a patch cadence, either through internal IT means or through a mechanism via the vendor.
        - Make a note of internal cost as an additive if using internal mechanisms.
- Discuss enhancement of baseline configuration.
    - Enhancement of local login without a password or a weak password.
    - Enhancement of implementing security hardening (suggest CIS benchmarks, which are free).
        - Suggest testing and validation at own cost, with sharing of results.

- Obtain information on necessary communication.
    - Whitelist only the necessary communication.
    - Segment devices into Vendor segment/VLAN, with only necessary communication.
        - Validate the mechanism with the vendor.
- Discuss adding security software.
    - Point to HIPAA/HITECH guidance and healthcare vertical precedence.
    - Offer to install security software from the internal organization and share results if the vendor is not willing or unable to support it.
    - Make a note of internal cost as an additive if using internal mechanisms.
    - Explain the mutual benefit of increased security; direct value on investment for the vendor/manufacturer.
- Segment equipment on a unique network, allowing only the necessary communication. Eliminate the capability to communicate with any other network.
- Update response plan on findings and issues beyond contractual language.
    - What to do in case ransomware or a virus is detected?
- Train clinical staff to report suspicious or abnormal behavior, even on medical devices that the IT team may not have direct input/troubleshooting.
    - Update incident response processes to include non-managed clinical equipment details.

3.5. Baseline Posture (Vendor-managed and customer-owned equipment)

The baseline posture of vendor-managed and customer-owned equipment is as follows:

- A temperature sensor. Built-in computer running Debian-based Linux.

- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: Debian 9.5.
    - Security Updates installed: None.
    - Applications: Gateway host.
        - Default install.
- No host-based firewall restrictions outside of the default firewall enabled.
- No standard lifecycle maintenance, including patching.
- No vulnerability assessment/continuous scanning.

3.5.1. Enhancement / Amalgam

The priority task is to ensure the organization's selection criteria of a vendor is one with a partnership in mind. A vendor that only sells and is unwilling to listen, help and partner is one to skip.

Understanding the total scope cost is vital for the business. The cost of a product may be negligible when related to the costs required to secure the equipment. In the case of a temperature sensor, due to the limitations of the equipment, an access point (AP) is required. In this specific case, the vendor does not have the ability to allow a standard IT AP without re-architecting their design. Instead, they provide an AP, which inherently does not have the same enterprise capabilities for maintenance and control, resulting in a worse security posture and requiring the organization to implement additives to enhance the security. In general, many different medical devices require the same approach, of which there are two key factors:

1. Approach each new vendor with questions surrounding flexibility and capability in alignment with your organizational security and technology posture and needs. If a vendor does not have the capability, look towards alternate vendors or understand the risk (via a device risk assessment) and additive cost to secure and maintain the environment if none are available.

2. The total cost of ownership of such equipment is not merely the purchase but also the operationalization with such equipment's security, requiring a protective bubble to be formed at the organization's expense to utilize the equipment. For example, a $5,000 device can cost $25,000 because of the need to create a new segmented network and add new workflows for maintenance that do not align with IT at-scale solutions.

Furthermore, suppose expertise is not available within the organization, which then requires investment with an outside party to support the investigation and analysis of this equipment, in alignment with the organization's needs. In the mock lab scenario, the expertise is available, and further research of the equipment shows the following:

- Security Updates are available. However, contractual obligations and support of the equipment must secure vendor approval when installing such patches; otherwise, the risk shifts to the organization entirely.
    - Consider the patient impact as the focal point to decision-making.

3.6. Baseline Posture (Software on top of OS-stack)

The baseline posture of software on top of OS-stack equipment, which is customer-owned and maintained, is as follows:

- A Windows 10 workstation.
- Patches are not up to date for OS-level, nor Application-level (3rd party patches).
    - OS Version: MS Windows 10 Enterprise, Build 1809.
    - KBs installed: OS Patch level February 2020 (Security-only).
    - Applications: General applications (Office, Browser, etc.) and Clinical applications (Audiometry software).
        - Default install: no patches, service packs, upgrades.
- No host-based firewall restrictions except for the default operating system firewall enabled.
- No security tools except for anti-virus software enabled.

- Due to the serial interface with the medical hardware, install the additional services required.
- Adjustments are required to the standard IT equipment's security posture to allow software on top of the OS stack.

3.6.1. Enhancement / Amalgam

Contrasting the rest of the silos of equipment, software on top of OS-stack is an additive layer (software) to already managed equipment. The approach can either be simple, by working with currently managed and secured equipment or complex by introducing specific needs that require configuration adjustments, such as reducing security for the equipment to work. An example can be requiring telnet or FTP. The concentration, therefore, should be as follows:

- There is an introduction of additional software, which most likely requires a direct relationship with the vendor to obtain patches. Patches, fixes, and upgrades are only available from the vendor directly, requiring packing them for consumption through standard IT tools.
- Applications introduce new vulnerabilities, such as SQL Express as part of its function or an FTP server.
    - New vulnerabilities require new ways to secure the equipment, including additional toolsets or configuration. Standard security protection mechanisms can be used but may need to include exclusions for software via Anti-Malware or other security tools.
- Testing and validation go beyond a simple vulnerability scan. A simple vulnerability scanner will not be able to scan the medical device due to its serial-to-USB connection, and therefore is not directly on the network.
- Due to the utilization of USB, specific approvals require allowing USB connectivity for a storage device for this particular case if security blocks USB by default.

4. Recommendations and Implications

As shown in Section 3, no matter the equipment or limitations, there are ways to improve the security posture, depending on the return on investment. The output shows that treating all equipment in the same manner is adverse to the security posture and provides a false sense of confidence. One cannot expect to drastically reduce the risk within a standard clinical environment with a singular resolution or simplified standardization, such as 'patch everything' (Williams, 2019) or 'it has anti-virus' mentality. There are too many complexities and differences within the environment, even when not accounting for the clinical workflow variance, differences between services rendered (surgeries, urgent care, primary physician, etc.), and operational capability.

It is of utmost importance for organizations to understand their environment, starting with asset management or inventory of authorized hardware and software, and to recognize the limitations of the Information Technology and Security capability. In utopia, the organization's tools would work flawlessly, each technology capability would have subject matter experts, and funding, resources, and time would not be an issue. In reality, most healthcare vertical organizations are limited in staffing, funding, and, most importantly, the capability to make drastic changes without patient impact. Unless built from the ground up with security in mind, retrofitting legacy solutions or solutions without information security after-the-fact is a complicated and expensive task. The primary reason is the impact on patient care in operation, which requires appropriate testing, validation, and confirmation. A replica development environment will not be available in most cases, further increasing the intended changes' complexity. Even if successful from the testing and validation phase, adjustments to the clinical workflows, or support thereof, requires extensive training of non-technical staff. In the end, clinical staff is there to take care of the patient, not troubleshoot technology.

As such, the steps taken have to be iterative. One must adjust any new technology and projects to undertake the secure approach, looking to understand the incoming changes appropriately and fitting them into the appropriate blueprint path, found in the Appendix. This way, an organization can draw a line in the sand to approach the problem systematically. That is, any net-new objectives are to undergo a secure-first approach

using the blueprint as guiding rails while the legacy environment takes a different tactic, prioritizing patient care first, the business, and security to plan improvement or transition.

Security becomes exponentially more expensive in the latter phases, whether through the complexity of implementation or as a result of an incident, so the organization's mentality has to change from 'we will secure it afterward' to 'make sure it is secure before going into production.' Do not chase perfection, but rather compromise through the positive approach, reinforce the benefits, and praise the overall team. The focus should then be to improve with the options presented iteratively, and the expectation should be continuous improvement, with patient care as the priority.

Information Security needs to become the enabler, not the department of 'no.' To achieve this does not come overnight, but via cultural change, positive attitude, synergy, and partnership. Broad-spectrum understanding of the business and clinical needs, not just technology, is a must, and approaching every problem with how to, instead of cannot. For a successful transformation, use the people, process, technology methodology, and the blueprint in the Appendix as guidance.

4.1. Recommendations for Practice

To re-iterate the various silos of equipment within a clinical environment as an outcome of this research, they are as following:

- IT wired equipment
- IT wireless equipment
- FDA-regulated and 3rd party managed equipment
- Vendor-owned and managed equipment
- Vendor-managed and customer-owned equipment
- Software on top of OS stack

The approach for each is unique, and as such, the strategy to resolution is also. While underlying information security builds upon the foundational aspect, the process is unique to the healthcare vertical and the silo of equipment. If there are opportunities to

combine silos, consider them. Otherwise, the importance is to understand the incoming service/solution and to differentiate them from the different silos of equipment in terms of capability. For example, suppose one can perform all the typical security activities on the equipment. Treat it in a standardized manner, such as your own IT equipment, which should be the most secure of all in terms of capability and actionability. To visualize the approach, please reference the blueprint in the Appendix.

4.2. Implications for Future Research

The healthcare vertical continues to evolve from the security vantage. While historically, physicians are usually the founders within the healthcare sector, not technology professionals, the shift to the internet of things and interconnectivity is driving technology to be the catalyzer to new organizations.

A lot of investment added increases the medical devices' security further as they are becoming more digitized, acting as what one would refer to today as the internet of things (IoT). However, the market is still prioritizing decreasing the cost rather than increasing the security. As such, competition and need are not around increased security but the reduction of cost. The result is smaller gains on the information security front.

These complexities within the healthcare vertical, coupled with additional characteristics detailed in research from McLeod and Dolezel (2018, p.65), are prime for further investigation to scrutinize the equipment needs in alignment with today's world of technology, keeping up with security and innovation, while driven by the organizations and not manufacturers.

5. Conclusion

A specific end-state envisioned from the security vantage resulted in additional findings. A few other items came to light while establishing a mock lab and performing analysis and research on the intended equipment. These included further technical and non-technical issues, such as the inability to recognize which equipment would fail during intensive scanning, other equipment becoming unresponsive, and performing research and analysis actions on a connected lab. From the non-technical aspect, a few

additional drivers came to light, such as validation of changes that required non-technical users to perform validation and impact to workflows, which required a finesse between engineering and non-engineering to accomplish the tasks. The end-state was proven as desired, and the Appendix is the aggregation of the information; however, the approach ended up being more complicated than anticipated. The result confirms that a standard and fixed approach to vulnerability management will fail and that one must take into account the various clinical environment limitations and adapt accordingly.

References

Aspen Digital. (2020, April 17). Combatting Cybercrime During COVID-19. Aspen Institute. Retrieved from https://www.aspeninstitute.org/blog-posts/combatting-cybercrime-during-covid-19/

Dameff, C., Bland, M., Levchenko, K., & Tully, J. (n.d.). Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives. University of California, San Diego. Retrieved from https://acsweb.ucsd.edu/~mbland/pestilential_protocol.pdf

IBM Security. (2019). Cost of a Data Breach Report 2019. Retrieved from https://www.ibm.com/security/data-breach

Kandek, W. (2015). Vulnerability Management for Dummies (2nd Edition) [E-book]. John Wiley & Sons, Ltd. Retrieved from https://www.qualys.com/forms/ebook/vulnerability-management-for-dummies/

Le Bris, A., & El Asri, W. (2017). State of Cybersecurity & Cyber Threats in Healthcare Organizations: Applied Cybersecurity Strategy for Managers. ESSEC Business School. Retrieved from http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68. https://doi.org/10.1016/j.dss.2018.02.00

Rob Bathurst. (2015, September 24). Why Healthcare Network Security Must Be a Top Priority. Retrieved from https://healthitsecurity.com/news/why-healthcare-network-security-must-be-a-top-priority

Schneier, B. (1999, December). Attack Trees. Schneier on Security. Retrieved from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

The Office of the National Coordinator for Health Information Technology (ONC). (n.d.). Security Risk Assessment Tool. Retrieved from https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

TrapX Research Labs. (2016). TrapX Investigative Report Anatomy of Attack. TrapX Software. Retrieved from https://trapx.com/trapx-labs-report-anatomy-of-attack-medical-device-hijack-medjack/

Trustwave. (2018). Trustwave Global Security Report. Retrieved from https://www.trustwave.com/en-us/resources/library/documents/2018-trustwave-global-security-report/. Last Accessed: October 7, 2020.

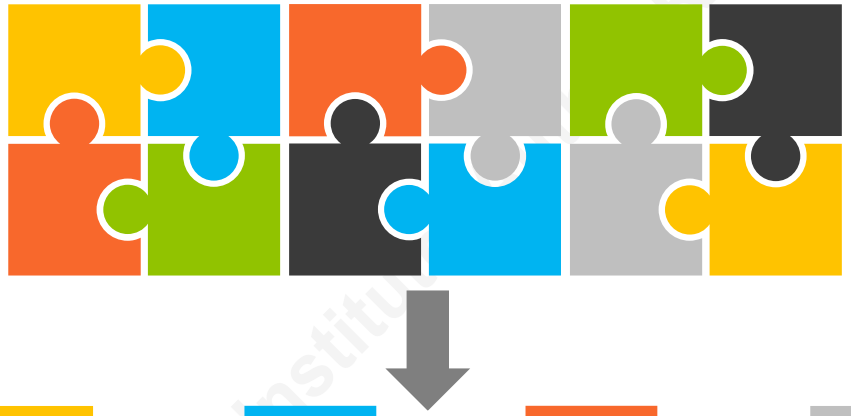
U.S. Food & Drug Administration. (n.d.). The FDA's Role in Medical Device Cybersecurity, Dispelling Myths and Understanding Facts. Retrieved from https://www.fda.gov/media/123052/download

Verizon. (2020). 2020 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/. Last Accessed: December 22, 2020.

Williams, J. (2019, April). Why Your Vulnerability Management Strategy Is Not Working - and What to Do About It. SANS Institute: Information Security Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/membership/38938

Appendix - Blueprint

All equipment treated the same.



IT wired equipment	IT wireless equipment	FDA Regulated	Vendor-owned and managed	Customer-owned and vendor managed	Software on top of OS stack
• Standardize	• Device Enrollment Program	• Build relationship with vendor	• Network segmentation	• Select vendor with partnership mindset	• Understand patch, hotfix and version update cycles with vendor
• Include non-security patches & hotfixes	• Mobile Device / Application Management	• Obtain best practices from vendor (security)	• Establish partnership with vendor (mutual support for security)	• Understand total cost of ownership	• Understand software requirements and impact to standard IT equipment
• Security Hardening (CIS Benchmarks)	• Security Hardening (CIS Benchmarks)	• Obtain dedicated test equipment	• Understand communication requirements	• Work with vendor to resolve vulnerabilities	• Limit less secure configuraiton changes to specific equipment
• Enhance firewall ruleset	• Force application updates	• Enhance 3rd party communication and support protocols	• Restrict to only required communication		
• Add security software	• Keep up with OS updates, security patches, and hotfixes	• Lifecycle management of equipment	• Work to add security software		
• Continously scan against changes in posture	• Require unique user authentication	• Do not assume FDA governed equipment is a black box with no flexibility	• Work to add security hardening		
• Improve privacy	• Continuously scan against changes in posture		• Request access to scan equipment		
• Train clinical staff (security awareness)	• Train clinical staff on mobile device security differences		• Explain mutual benefit of increased security posture		
• Update firmware and prefer central management					

Silos of equipment – each approach differs based on capabilities and limitations