Challenges of Implementing HTM Devices into an IT Environment

GREGORY GOLL BS CHTM CBET

MANAGER, PROJECTS AND MEDICAL IMAGING SERVICES DEPARTMENT

WELLSTAR HEALTH SYSTEM

MARIETTA, GA

Wellstar Demographics

- 13 Hospitals
- 21 Imaging Centers (growing)
- 17th Busiest Emergency Room in country,
- 2nd Busiest Emergency Room in Georgia
- One of the largest heathcare providers in Georgia

Something to think about:

"You never fail until you stop trying."

Albert Einstein

Background

- 1985 University of Michigan Health System, Ann Arbor, Michigan
- 2001 Supervisor at Erlanger Health System, Chattanooga, Tennessee
- 2015 McLaren Health System, Mount Clemens, Michigan
- 2017 Wellstar Health System, Marietta, Georgia

Adapting to surprises

- The Covid 19 Pandemic
- Shutting of a major hospital
- Acquiring a new hospital network
- Expansion of a service line

Things to ponder- The ever changing world of IT

- BYOD- Bring Your Own Device, is now a common requirement for many new employees
- BYOD can be dangerous to organizations, as mobile devices may carry malware.
- Device Mobility can reduce operation costs by 40%
- The average cost of a healthcare data breach is now $10.93 million, up from $10.10 million in 2022,
- 95 percent of cybersecurity breaches are caused by human error.
- 43 percent of all breaches are insider threats, either intentional or unintentional.

PACS and EMR there is a difference

- **PACS - Picture Archiving and Communication Systems.** A system based on the universal (Digital Imaging and Communications in Medicine) standard, which uses a server to store and allow facile access to high-quality radiologic images, including conventional film images. Basically PACS stores pictures and associated information.
- **EMR** - **Electronic Medical Records**, which are the digital equivalent of paper records, or charts at a clinician's office. EMRs typically contain general information such as treatment and medical history about a patient as it is collected by the individual medical practice. EMR basically is vital signs and associated information.

Types of Device Security

- **Physical security-**
- Limit physical access to a device or system
- Lock a device to prevent removal
- Controlled access to areas
- **Virtual Security**
- Document OS of system/device
- Anti-virus
- **Other issues**
- Any camera used in a hospital environment

Getting Started: Checking your inventory

- Internal Inventory
  - Your Educational Background
  - Experience
  - Educational Background of Staff
  - Current and Prior Experience of not only your staff, but other departments working with you
  - Certifications

Understanding Basic Components

- Software
- Anti-Virus software local and network administered
- Hardware
- Interface Issues
- Network Limitations
- Network Components
- Network Designs / Topography

Common Ways to expose your equipment and network

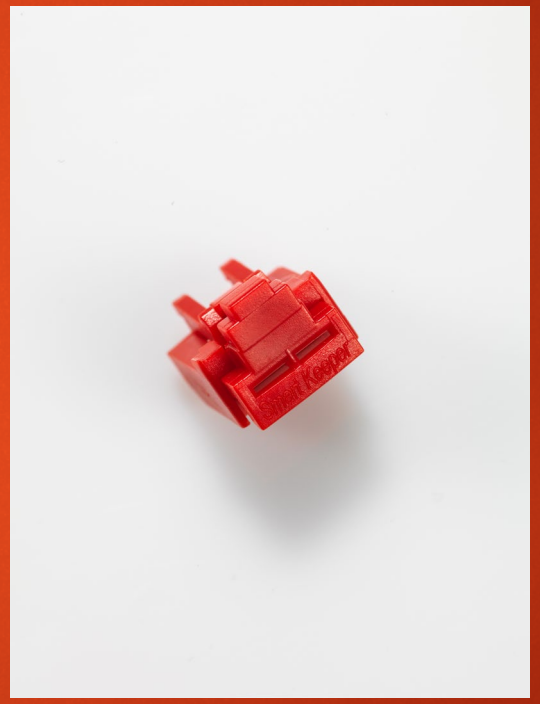
- Outdated and unsupported software will always necessitate additional security considerations, but saying that all obsolete software is a security risk is wrong.
- **Third-party vendors do not utilize the same protection measures**
- Medical Devices with open access to internet
- Unencrypted USB drives
- Open USB ports on any device
- Unauthorized software installations
- Social Media
- Unsecured Laptops (not locked down)

Ways to protect equipment

- Never share service/conguration passwords with users.
- Insure only proper access levels with users.
- Limit access outside hospital network. No Internet unless absolutely necessary on clinical equipment.
- Create an exception list of all IP addresses of Clinical Equipment, this will minimize risks of automatic software updates.
- Lock USB ports either physically or by software.

Physical Locks for RJ45/USB

www.connectivitycenter.com



Desk Top and Lap Top Locks

Understanding Your Departments Internal Boundary

- How far does your department currently work in the Information Technologies Environment?
- Is your IT services in-house, contracted or a mixture?
- What are the limitations of your access into the IT Environment?
- What is your relationship with your IT provider?
- What is you employers limitations into the IT Environment? (do they pull their own cables/ install networks)
- Who assigns/controls IP addresses

Meeting attendance

- Find out what routine IT planning meetings occur
- Are there other issues contected to these planning meetings?
- Understand the topic of the meeting and how it does or does not impact Imaging devices.
- Get engaged with especially IT security.

Process for requesting IT support/ project involvement

- Is there a formal process for requesting IT support in a project/installation.
- Who determines the priority of a request?
- What is the process for requesting cable pulls or network jack activation. Who actually pulls cables?
- Is there a lead time for building interfaces?
- Does IT create their own separate budget?

Software/ IT information Support

- Secure any software and license documentation immediately.
- Any loss of software licenses can directly effect future vendor support and potential additional cost.
- Storage area should have limited access/ ideally securely locked.
- Make a backup copy of any software if possible and create a secondary storage area, separate from primary storage area.
- Document software revisions, IP address, anti-virus type, and any other important information in equipment record.
- Document as many of the network relationships as possible.

Hardware Requirements

- Specifications in writing
- Operating System Software
- Who supplies what in writing
- Issues of using OEM and alternative suppliers (Cisco verses Nortel)
- Mix and match components
- Can identical components be purchased through hospital sources verses vendor (example printers)

Vendor Security

- What is the process needed to add a vendor to your accounting/purchasing department?
- Who is in charge of processing agreements with a vendor?
- Insure vendor and any staff are properly registered with your hospital.
- Who is in charge of processing agreements with a vendor?
- Make sure there is an agreement as to what information a vendor/provider can access.

Security- ask the questions (HIPAA)-

Heath Insurance Portability and Accountability Act

- Will there be any interface to a PACS / EMR?
- Will patient data with unique identifiers be stored on the devices?
- Is remote physician access needed?
- Who owns any computers used for remote access?
- What is the hospital policy for remote access to patient information by clinical staff?

In House Testing

- Purchase test equipment
- Development of in house testing area
- Allow others to use the area if needed
- Request network connections
- Obtain secure location for any important information
- Define process for securing copies of software and backup configurations
- Look to reuse important components to save cost

Testing area example

The difference between opportunity and a dead end.

- Most common pitfalls of ending up supporting IT the wrong way.
  - Supporting devices which are not directly connected to a patient or providing support to a physiological system.
  - Assuming support roles without supporting funding.
  - Working as a system administrator, focused on the clinical side of application. Assigning logins, fixing connection issues, etc.
  - Taking on any support outside the skill set of your staff, never assume you can find a perfect new employee.

Watch for Good Opportunities

- Solarwinds – network monitor
- Palo Alto - network monitor
- BrainsGate – stroke treatment system

Planning Stages

- What is the purpose of the equipment being replaced?
- Has anyone involved clinical staff?
- What is the support requirements of the new equipment?
- What is the budget for the equipment and on going support?
- How critical is the equipment to daily operation?
- Are there any long term support issues?
- Data storage needs?
- Has a system administrator been determined?

There is no such thing as a free puppy, beware of reuse!

- Be absolutely certain of condition of any device you plan to reuse.
- Make sure the technology is current.
- Watch for free left over equipment, will it meet all of the current and future needs.
- Just because you can does it mean you should? (reusing similar components from different vendors)

Budget Issues

- Has the budget already been set?
- Early involvement in the Budget process, define your internal issues/costs.
- Define all components of support, Software License, Installation requirements for hardware, and any changes required to facility including network connections and network closets.
- Data conversion requirements for legacy data.

Vendor Software/Support

- What is the installation requirements. (Hardware)
- Is vendor remote access needed?
- What is the operating system (OS)?
- How long has this been used? Any pending end date for OS?
- Any future plans for future upgrades to OS?
- What is the anti-virus, in any installed? (Hospital update process)
- Upgrade path/ever green to keep current.
- **Remediation of software conflict issues.**
- Annual support costs? Hourly Time/Materials cost?
- License costs for expansions?

Disposal Concerns

- How is patient data removed completely from a retired device/system?
- Are medical device CPU's uniquely identified?
- How is disposal of a retired hard drive managed?

Tools for Wireless Spectrum Survey

- Metageek-Chanalyzer Pro/cost $500
- Signal Hound/cost $1000
- Spectrum Analyzer/ cost $8000 – $30,000

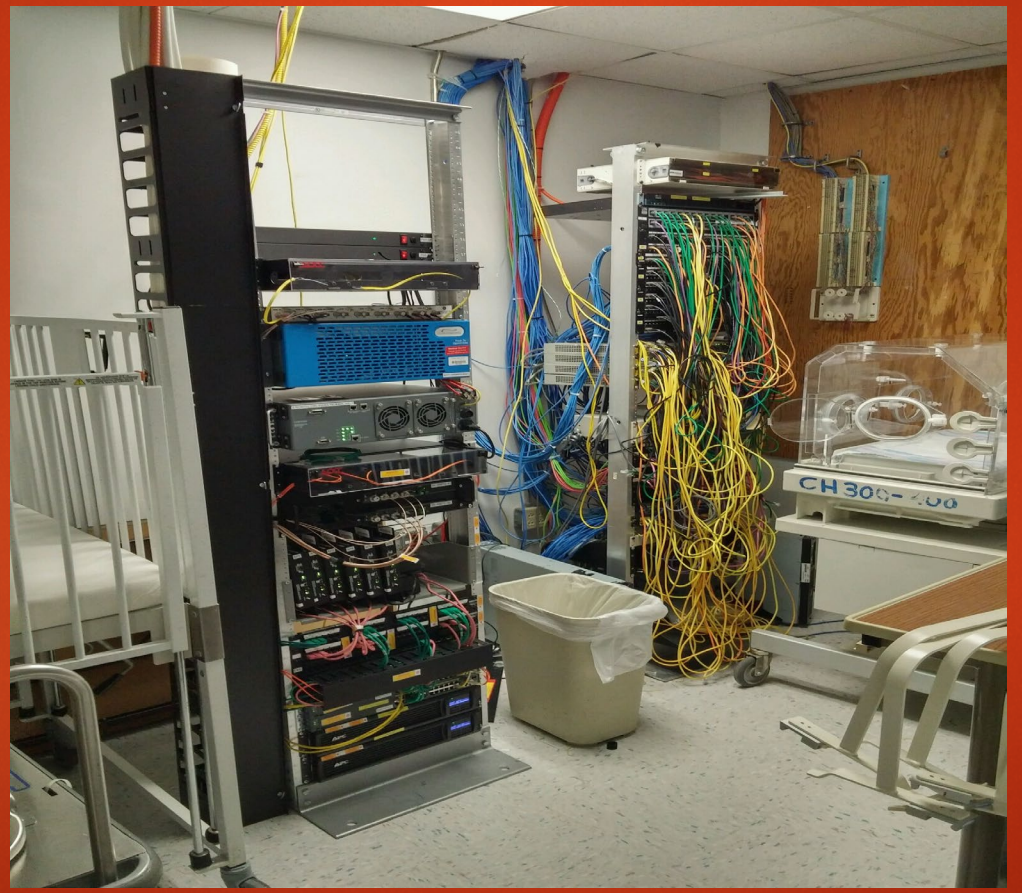
Site Survey- expect surprises

In House Site Survey

- Insure all Blueprints are the latest version and that all people involved in the process have the same version.
- Define Locations of all Network Closets
- Make sure each person at this stage has the power to make decisions.
- Locate challenging areas

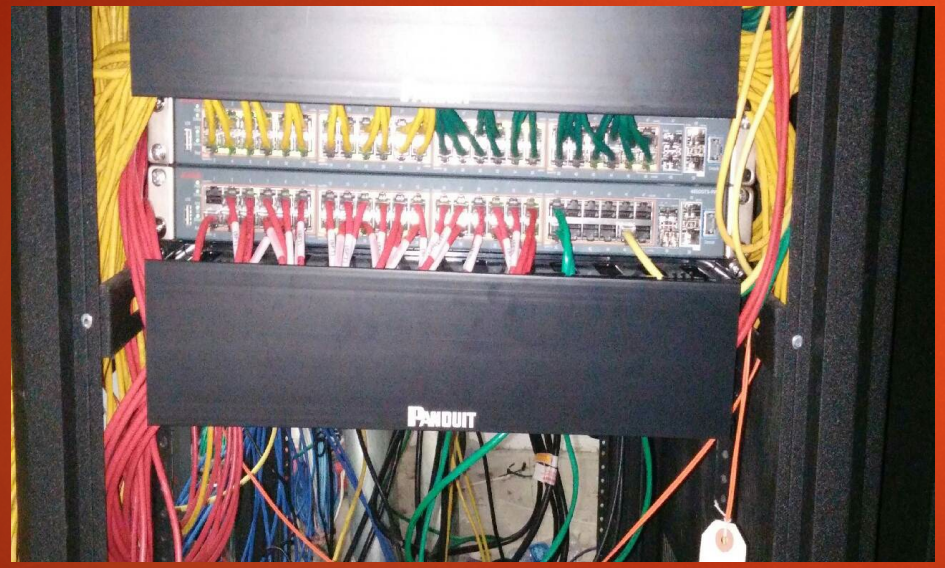
Network design considerations
Redundant coverage

Beauty and the Beast

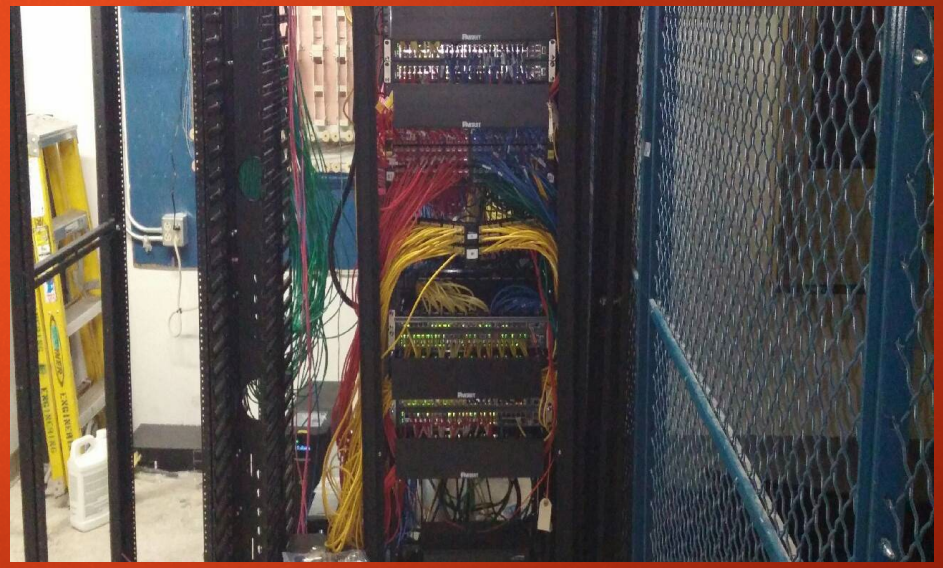


Network Setup Details

Patch Panel Details



The complete rack



Challenging Area

Lost in translation

Questions?

Please scan QR code to submit a survey for this session.

Thank You!