Starting an in-house Medical Device Cybersecurity program

Rob Bundick – Director HTM and Biomedical Engineering

Dave Yaeger – Biomed Security Administrator

About ProHealth care

- **Community based Non-profit Healthcare system servicing Waukesha County WI and surrounding areas**
- **2 Hospitals – 377 beds**
- **19+ clinics**
- **Stand alone ER**
- **Regional Cancer Center**
- **Various partnerships with Surgery Centers, Rehab Hospitals etc….**

Biomedical Engineering Department

- **1 Supervisor**
- **1 Admin/Dispatcher**
- **1 Parts Procurement Specialist**
- **1 Biomed Tech**
- **7 Senior Biomed Techs**
- **3 Imaging Techs (2 of which cover Biomed)**
- **4 Senior Imaging Techs**

HTM Department

Healthcare Technology Management

- 1 Director
- 1 Cyber Security Analyst
- 1 Database Analyst (CMMS)
- 1 Medical Device Integration Engineer

Starting a Medical Device Cybersecurity program

- 2015 - Audit was performed and found that Medical Device cyber security was an area at PHC that needed to be addressed. Planning started with IT and Biomed to develop a program
- 2016 - Plan and budget was submitted and was denied.
- 2017 - after identifying an increase in cyber security attacks a more in-depth plan was developed and proposed.

Starting a Medical Device Cybersecurity program

- 2017 - SBAR was developed to justify implementing the new program. Approval was given to start in 2018
- 2018 - Cyber security position is filled. Evaluation of necessary security and utilization tools begin

Biomedical Security Administrator

- How I got here
  - Agfa service engineer
    - Assigned to ProHealth Care
  - Employed as PACS administrator
  - Moved across the hall to the Biomed department as security analyst
    - I already knew all the players in biomed and IT, where the coffee machine and bathrooms were, so I was ready to get started.

Starting a Medical Device Cybersecurity program, cont.

- Become immersed in technical newsletters and cyber reports. FDA and ICS-Cert
  - Go to cyber conferences and attend webinars
    - Imaging and Biomed conferences now have a strong cybersecurity part to them
  - Become a member of MDISS, AAMI, HIMSS, ECRI, and others, both local and national

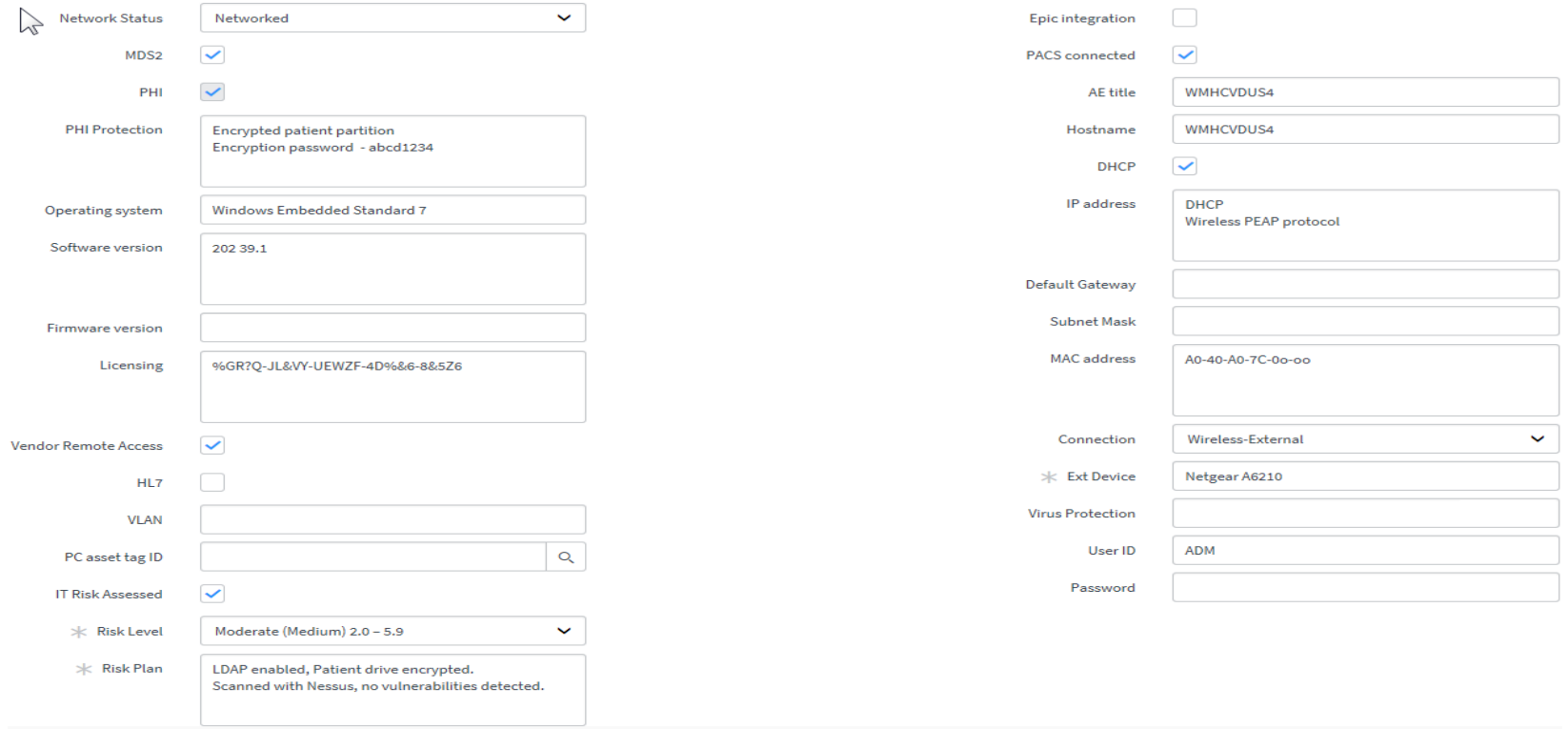
MDISS - MDRAP

- MDRAP can assist in getting a base level vulnerability score for your device
  - Device assessment based on MDS2
- Medical Device Risk Assessment Platform
  - Crowd Sourced Data Commons
  - Device Catalog based on FDA PMA & 510(k)
  - Inventory Upload
    - Matching to FDA catalog

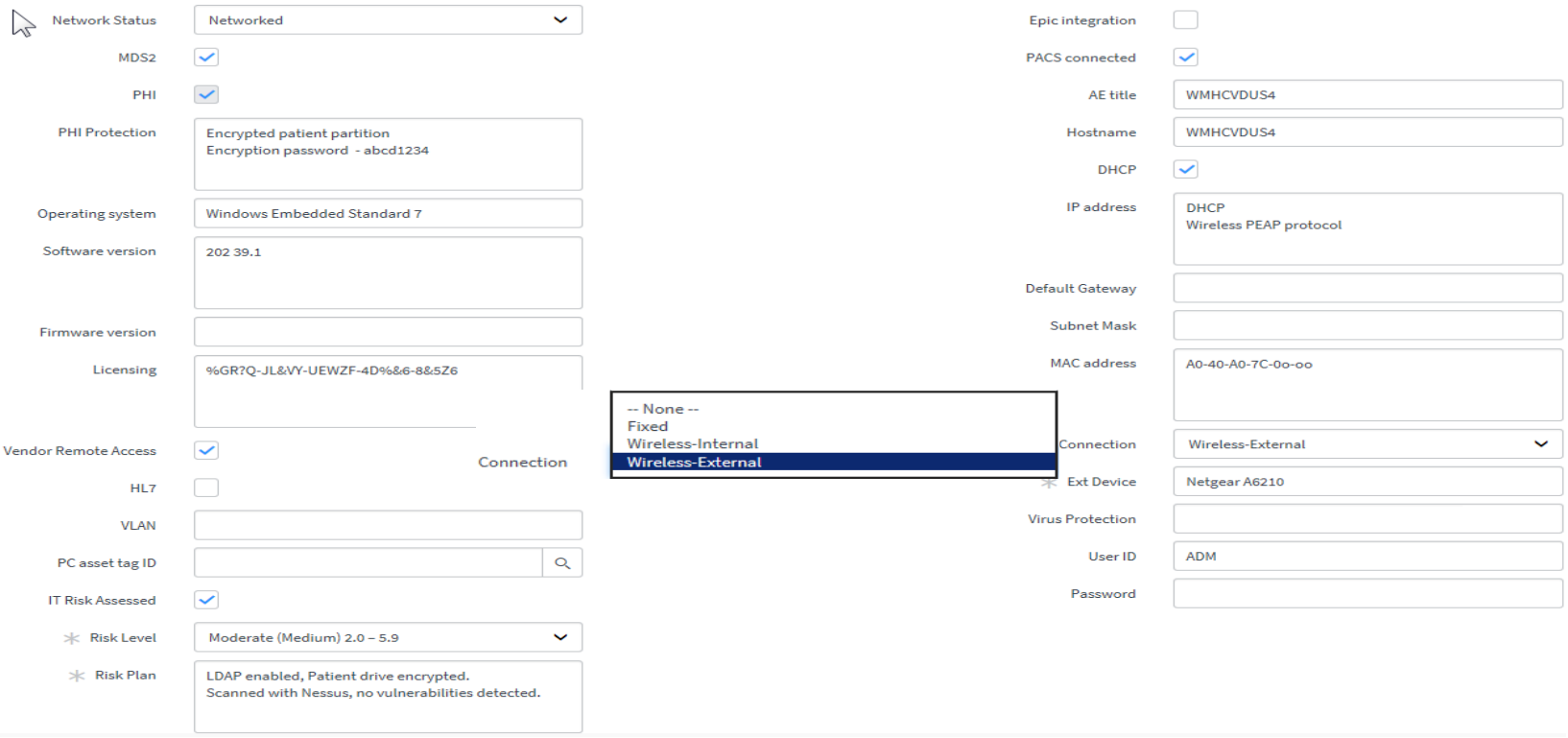
Starting a Medical Device Cybersecurity program, cont.

- Started data collection in our CMMS for *networking* details
  - Outside the norm for medical device inventories

CMMS Informatics page



CMMS Informatics page



Starting a Medical Device Cybersecurity program, cont.

- The first thing that all experts agree on in creating a successful medical device cyber security process is an ***accurate medical device inventory.***
  - How can this be accomplished?
    - What things need to be inventoried?
      - Systems vs. individual items

Starting a Medical Device Cybersecurity program, cont.

- CMMS is capable of a parent/child relationship for assets
  - Security application found 4 IR devices where we knew we had only 2 scanners

MD/IOT discovery application

- Identified and requested proposals from IOT security companies in collaboration with IT
  - Asimily
  - CloudPost Networks
  - VirtaLabs
  - ZingBox

Future plans and goals

- Creating and implementing a process for new equipment being purchased
  - OS upgrade path
    - Expect device ownership to span two Windows OS versions
      - Windows 7 will end of life on January 14th, 2020
    - Security Patching strategy
    - MDS2 analysis (risk scoring) prior to purchase
      - MDRAP can assist in this process

Future plans and goals

- Creating and implementing a process for new equipment being purchased
  - OS upgrade path
    - Expect device ownership to span two Windows OS versions
      - Windows 7 will end of life on January 14th, 2020
    - Security Patching strategy
    - MDS2 analysis (risk scoring) prior to purchase
      - MDRAP can assist in this process

Future plans and goals, cont.

- Our department reports up through materials management
  - Capital equipment analysis committee
  - Biomed signs off on every Capital purchase request
- Application capabilities to show utilization statistics to assist in procurement decisions

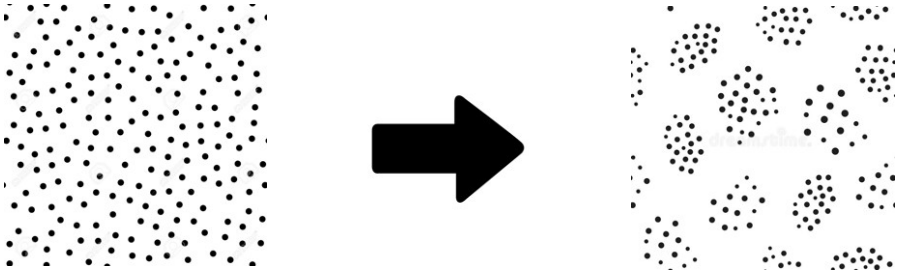
Future plans and goals, cont.

- Implement new software as soon as possible
  - In accordance with vendor recommendations
- Develop process for patching and Virus protection within devices
- Point of site security (user log in, USB Locks, change admin (routine) passwords, etc..)
  - Keep passwords in CMMS
- Develop routine monitoring and preventive plans/process

Future plans and goals, cont.

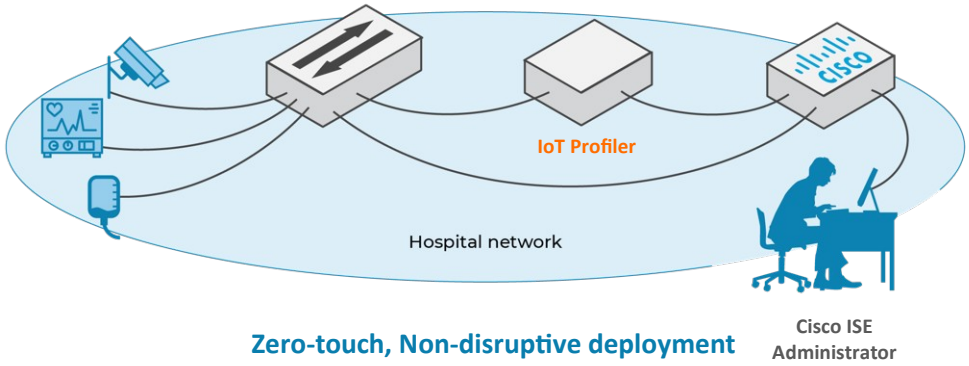
- Starting a process of micro-segmentation in coordination with our IT team members
  - The application that we are implementing can assist in this by showing the “normal” and “abnormal” network traffic for devices
    - Analyzing internal (east/west) and external (north/south) traffic over a period of time
    - Watching for traffic outside these patterns

IoT – SEGMENTATION & SECURITY



Scattered IoT Assets

Organized Micro-segments



Zero-touch, Non-disruptive deployment

IoT Profiler

enables IoT orchestration via Cisco ISE

asset discovery & tracking

- identify, classify and inventory IoT assets
- enrich asset records with contextual data
- relay IoT context to ISE

micro-segmentation

- define 'security groups' in ISE using IoT context
- network admission policies based on IoT 'security groups'
- organize assets dynamically in context-aware micro-segments

policy definition

- learn normal device behaviors
- apply principles of least privilege to IoT assets
- generate ACLs to only allow trusted behaviors

security enforcement

- detect deviations from expected baseline
- surgically block malicious connections
- isolate and quarantine the device

Protecting Medical Devices – Microsegmentation

Learn

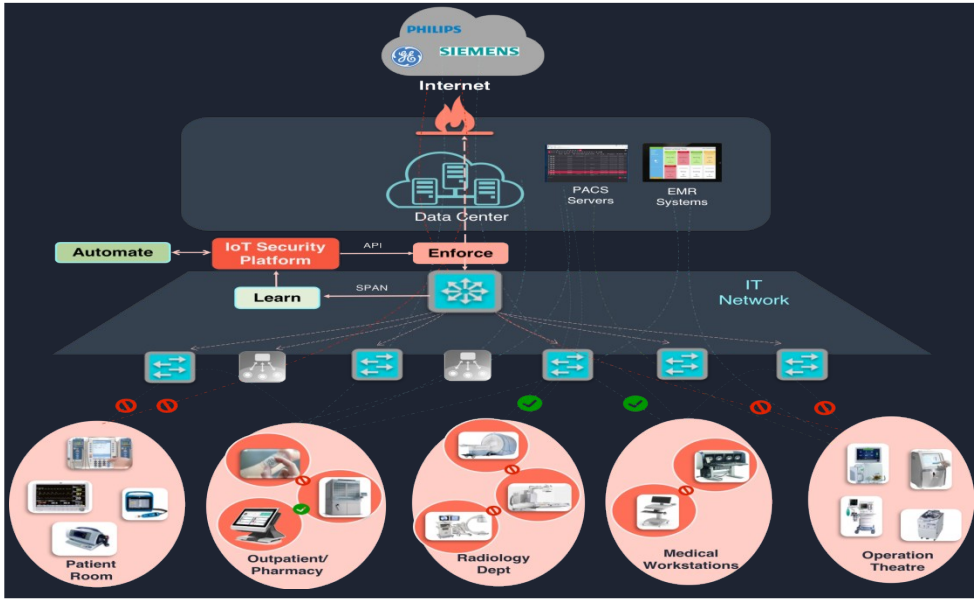
Solution passively learns and discovers devices and insights using ML/AI based algorithms gleaning data from network traffic

Grouping

Solution fingerprints the discovered devices, profiles them based on make/model and classifies them into groups and sub-groups

Automate

Solution automates policy generation based on real-time device flow analysis and behavioral baselining of profile and device flows.



Enforce

Solution programs the network enforcements points such network access and distribution switches, routers and firewalls

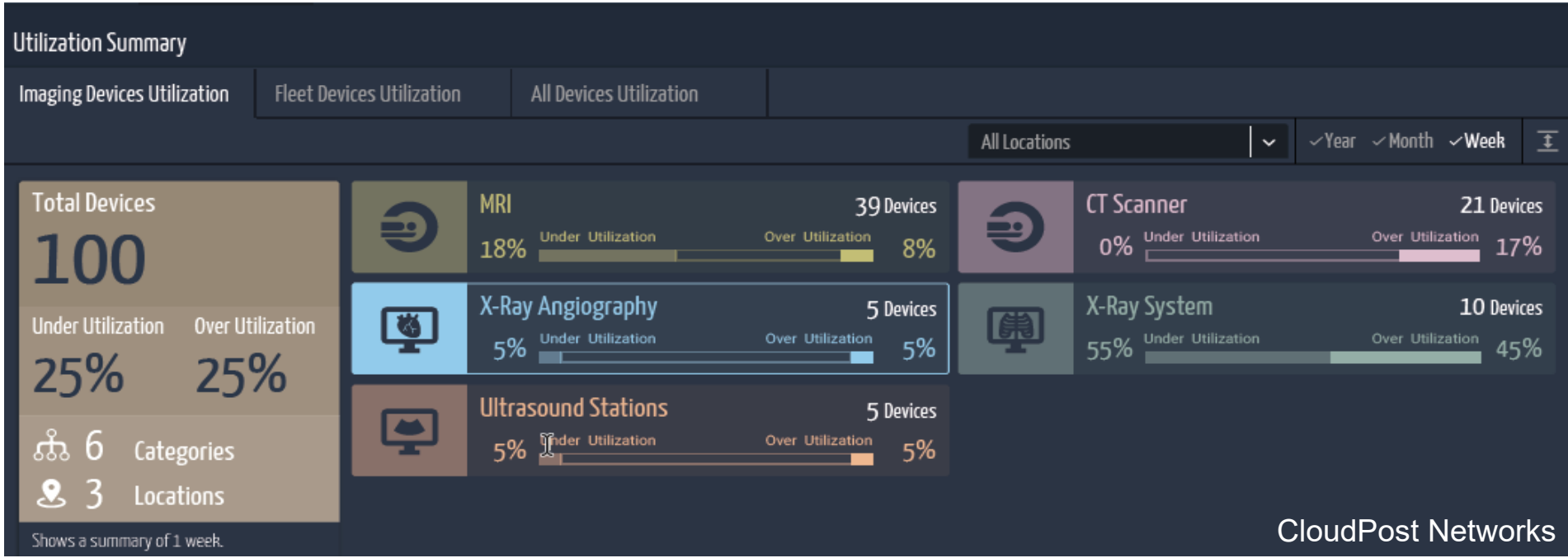
Segmentation

Solution programs segmentation polices such allowing intra-vlan traffic and blocking vlan-to-vlan communication on switches

Microsegmentation

Solution programs micro segmentation polices on device connected network interface (wired or wireless) such as allowing specific destination/port/protocols and deny unwanted internal & external destinations

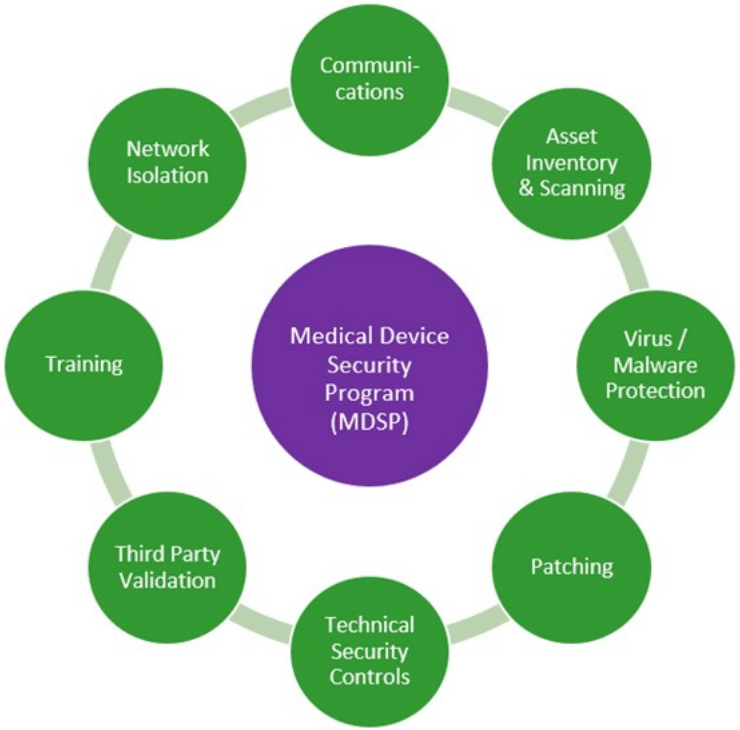
Medical Device Utilization



Medical Device Utilization

- Utilization views: Weekly

Establish a Formal Medical Device Security Program (MDSP)



- Medical device security more than technology
- Establish the people, process, and technology in a formal MDSP that:
  - Aligns with industry standards
  - Incorporates your existing security program
  - Defines roles and responsibilities
  - Outlines tools and resources
  - Documents specific metrics and procedures
  - Establishes a multi-year road map
  - Maintains as accurate an **inventory** as possible

Define Roles

***R**esponsible: The team or individual performing the activity.*
***A**ccountable: The team that is accountable and can approve/deny.*
***C**onsulted: The team that contributes to the activity or provides feedback.*
***I**nformed: The team that needs to know about the activity.*

MDSP Category	Information Security	Information Security Steering Committee	Information Technology	Biomedical Lab	Manufacturers	Purchasing	Clinical Departments
1. Communications	C R	R		C	I	C	C
2. Asset Inventory & Scanning	C I			R A	I		I
3. Virus / Malware Protection	R A C		R	A R	R A C	I C	
4. Patching	R A C		R	A C	R A C		
5. Technical Security Controls	R A C			A R	A C I		
6. Validation	C	R A		R A	I	C	I
7. Training	C	R A		A C			C
8. Network Isolation	A C		R C I	A C	I		

Samples of security incidents

- Taken from Healthcare IT News website
  - www.healthcareitnews.com
  - **Employee error exposed Blue Cross patient data for 3 months**
  - **Ransomware attack breaches 40,800 patient records in Hawaii**
  - **Phishing attack breaches 38,000 records at Legacy Health**
  - **417,000 Augusta university health patient records breached nearly one year ago**
  - **Third-party vendor error exposes data of 19k patients for 2 months**

David.Yaeger@phci.org

Robert.Bundick@phci.org