Managing Cyber Attacks

Best practices for planning, handling, and reporting cyber attacks.

Objectives

1. To bring BET technicians and managers up to speed on what is actually happening to hospitals regarding network security
2. To give a breakdown on what is going on in the field today.
3. To give a brief history of attacks against hospitals
4. To inform as to the technologies available for network security
5. To outline a course of action and give a plan to minimize risk
6. To outline best practices for inhouse operations

Who I am / Where do I work?

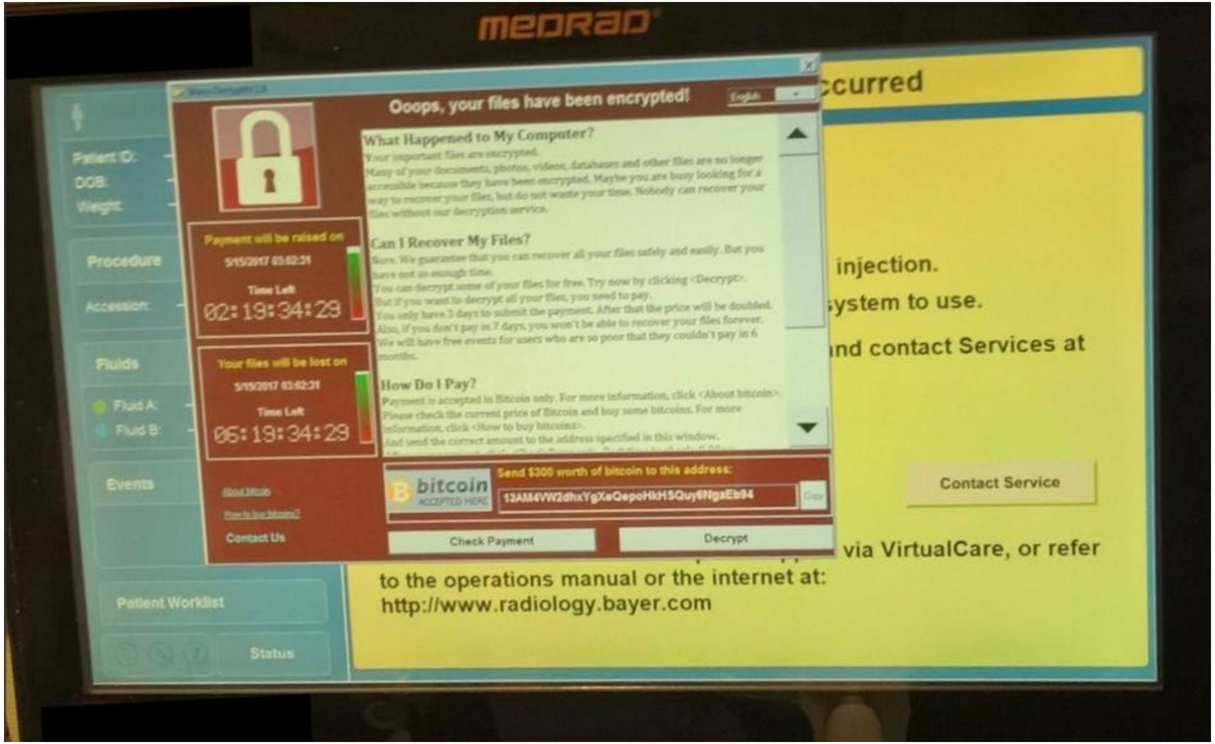
Garrett Seeley - Associate Professor of Biomedical Equipment Technology, Texas State Technical College, Waco, Texas.

- □ Education: MS-Information Technology, BS Biomedical Electronics, USAMEOS Graduate, CompTIA A+ and Network +
- □ Experience: 12 years in field of Biomedical and Radiology services, 13 years of education at the college level.
- □ My Employer: TSTC - graduates over 50 technicians annually, 30+ are dual degree, Biomedical and Medical Imaging.
  - □ Students are trained on actual equipment, over 3 million worth of used medical equipment including Ultrasound machines, Mammography, Rad/Fluoro, CT, and MRI systems -
  - □ Total costs are about $20,000 for 2 years of training. Placement is over 90% - We place nationwide - 254.867.4885

What is all the fuss about?

This is from a Forbes article (5/17/17) titled: Wannacry ransomware hit real medical devices

Bayer Medrad confirmed two reports from customers in the U.S. with devices hit by the ransomware. If a hospital's network is compromised, this may affect Windows-based medical devices connected to that network.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.

Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29

Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

ccurred

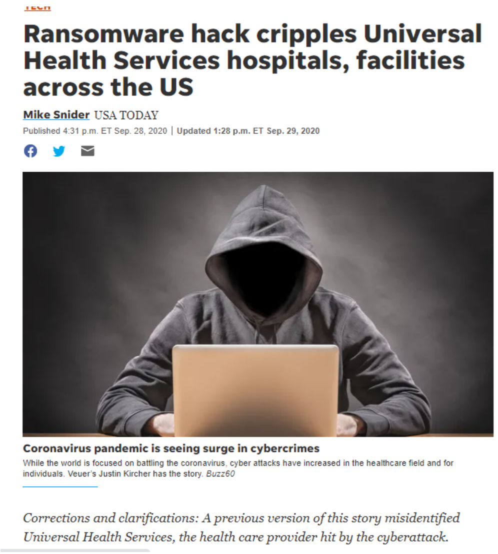
injection.

system to use.

and contact Services at

via VirtualCare, or refer to the operations manual or the internet at:
http://www.radiology.bayer.com

Here is what happened most recently:



TECH

Ransomware hack cripples Universal Health Services hospitals, facilities across the US

Mike Snider USA TODAY

Published 4:31 p.m. ET Sep. 28, 2020 | Updated 1:28 p.m. ET Sep. 29, 2020

Coronavirus pandemic is seeing surge in cybercrimes

While the world is focused on battling the coronavirus, cyber attacks have increased in the healthcare field and for individuals. Veuer's Justin Kircher has the story. *Buzz60*

Corrections and clarifications: A previous version of this story misidentified Universal Health Services, the health care provider hit by the cyberattack.

- The USA Today reports that a UHS facility shut down computer systems and went to paper protocols due to a Ryuk ransomware attack on 9/27/2020.
- Forbes reported that the first death due to ransomware attacks occurred on 9/10/2020.
- This is part of the c-suite water cooler conversations
- PHI now has a street value

TECH • CYBERSECURITY

Ransomware attack on a hospital may be first ever to cause a death

BY ROBERT HACKETT

September 18, 2020 2:09 PM CDT

What attacks are out there?

Indirect Attacks:

- Viruses and Trojans
- Ramsomware, cyrptolockers
- Spyware and Keyloggers

Direct attacks:

- DoS / access attacks
- Intrusions - scanning / probes
- Social Engineering and Theft
- Logins compromised or brute force attacks

Remember we have Hipaa rules

Planning: Who to talk to about this

OEM - Get their support and involvement - Approach this problem with them, not against them.

IT Security team - Be a part of their actions. Talk to them often

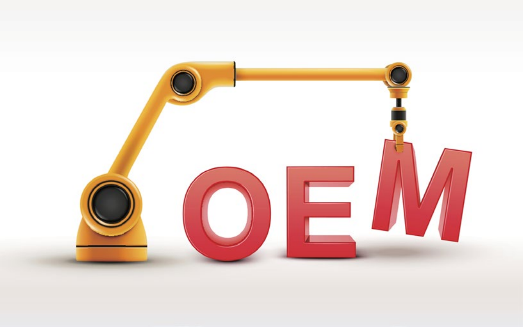
IT Networking team - Get to know them. Make them part of your team.

Risk Management _ Work with them outside of incidences. Get involved with purchasing from a IoMT (Internet of Medical Things) perspective,

TEAMWORK
Cooperation is always nice until
someone gets kicked in the head

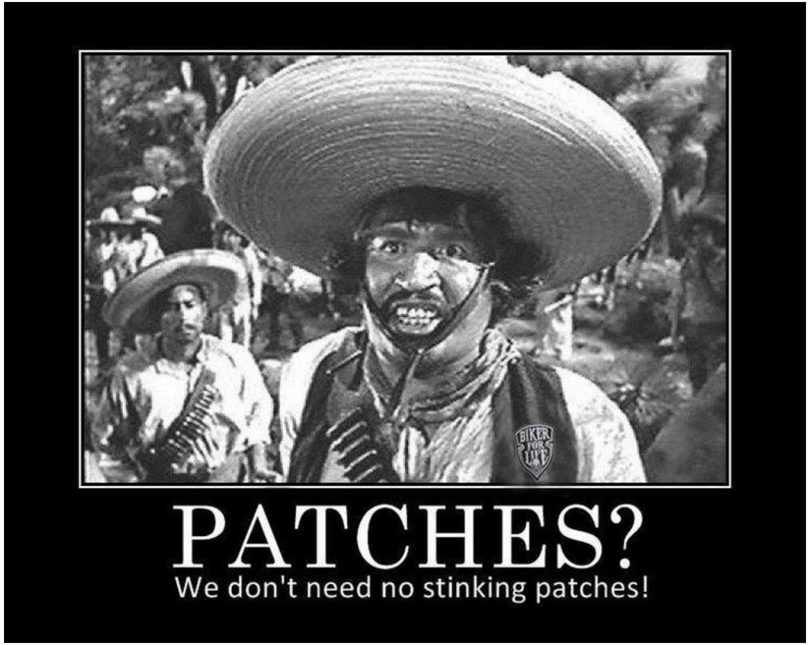
Things to ask the OEM to support security

- Windows Updates - install OEM verified Windows Patches.
- Disable Flash, Choose / Limit Web page access.
- Disable Front facing USBs - Get rid of Flash Drives - limit direct access
- Track Logins and Operating System versions- Track liabilities
- Ask about sharing permissions - Turn off simple file sharing unless required
- Get involved with Cyber Security settings, the Risk Management, and Capital Equipment Purchases. Only buy things with security approaches built in.
- Learn about Embedded vs bolt on security.



OEM needed to verify the Patches

- Work with OEM's to verify software revisions you have and what patches are the most up to date.
- Microsoft of course recommends "Automatic Update" Be careful with Auto Update. This can interrupt operations
    - They may cause the system to shut down
- Yes, we need these "Stinking Patches"
- If it's not verified, it's a "do at your own risk" - you may face a "you break it, you bought it" - Use a system as a sandbox.



Flash, Java, ASP & other glaring security holes

- Java uses a user security permissions (set by their login) to access the entire system
  - It is not very secure - got out of date easily
  - Buttons can be programed to do nearly anything
- Disable if possible - ask the OEM
- FYI: Flash is gone as of end of 2020 - uninstall Flash Player per Adobe

- Shockwave and Flash give similar system access.
  - This is so bad that modern browsers use HTMLv5.2 or better to get around it
  - Solution: update browsers, uninstall software

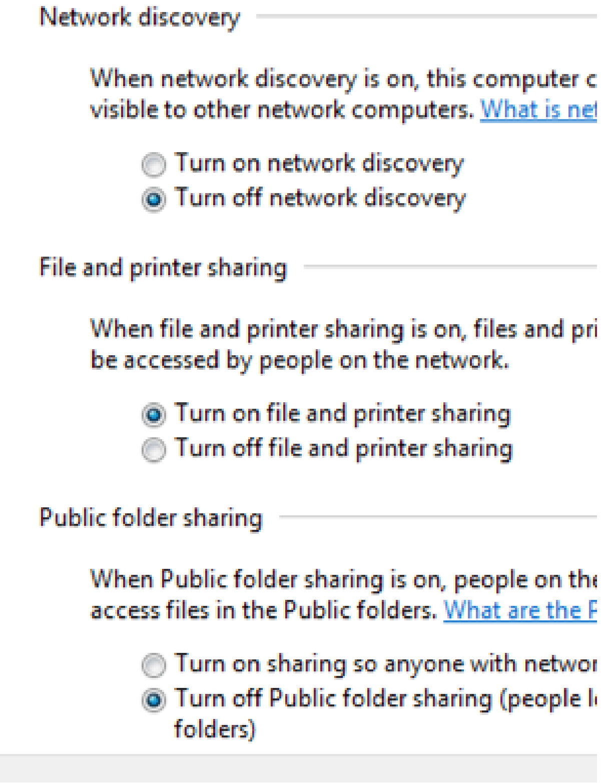
Again, the answer is updating - check with the OEM

- ASP is a Windows proprietary version of Java

Seriously, disable the front facing USB ports

- Stop people from bringing in Flash Drives that can be infected
- Stop people from plugging their smartphones (a linux computer) up to a medical device.
- Provide charging stations to techs / nurses
- Stop vendors from hooking up unknown devices to a system. Know what dongles are needed.
- Verify OEM vendors are doing the same. Tell them it is protecting machines from infections

How do OEMs use permissions on file shares?



Network discovery

When network discovery is on, this computer c
visible to other network computers. What is ne

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

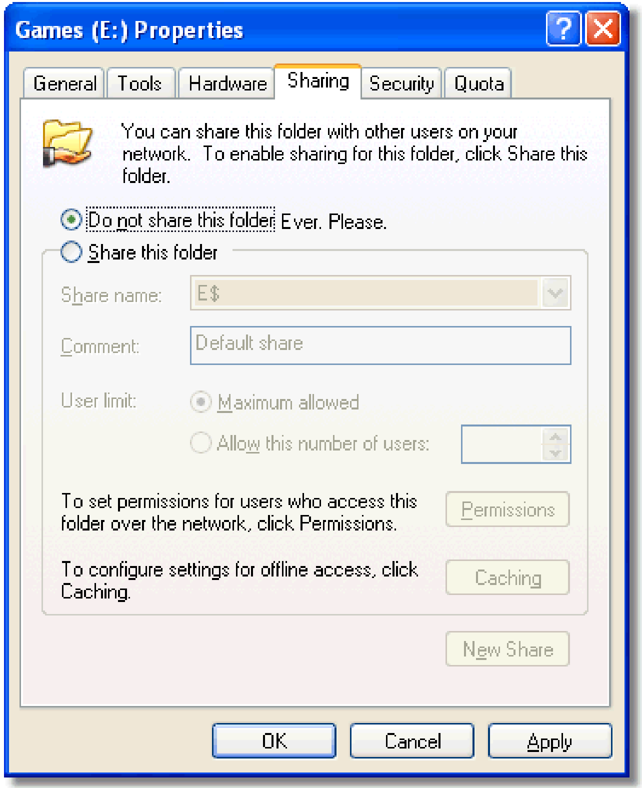
When file and printer sharing is on, files and pri
be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the
access files in the Public folders. What are the P

○ Turn on sharing so anyone with networ
● Turn off Public folder sharing (people l
folders)



Games (E:) Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

● Do not share this folder Ever. Please.
○ Share this folder

Share name: E$

Comment: Default share

User limit: ● Maximum allowed
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

You can set permissions to folders and control if users have read only access.

Do not just leave a folder as a public share with no permissions.

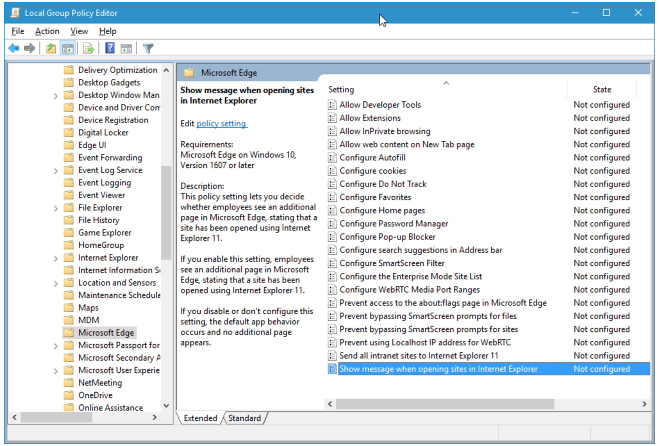
<u>Disable simple file sharing when applicable</u>

Use GPO (Group Policy Object)

GPO can be used to limit what a user (or admin) can do to a system. You can limit what they can or cannot run. Every function of windows can be individually controlled here. It is accessed in Windows through the gpedit.msc command

You can lock systems down to the most essential functions.

Ask the OEM about GPO and what it can do for you. If they do not know, you may want to bring this up on capital equipment purchases.



Show message when opening sites in Internet Explorer

Edit policy setting

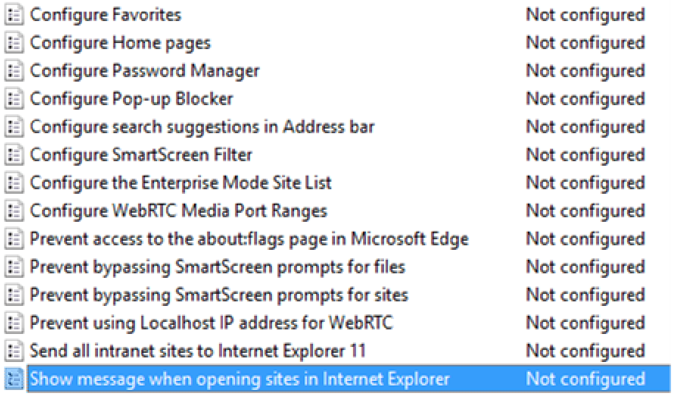
Requirements:
Microsoft Edge on Windows 10, Version 1607 or later

Description:
This policy setting lets you decide whether employees see an additional page in Microsoft Edge, stating that a site has been opened using Internet Explorer 11.

If you enable this setting, employees see an additional page in Microsoft Edge, stating that a site has been opened using Internet Explorer 11.

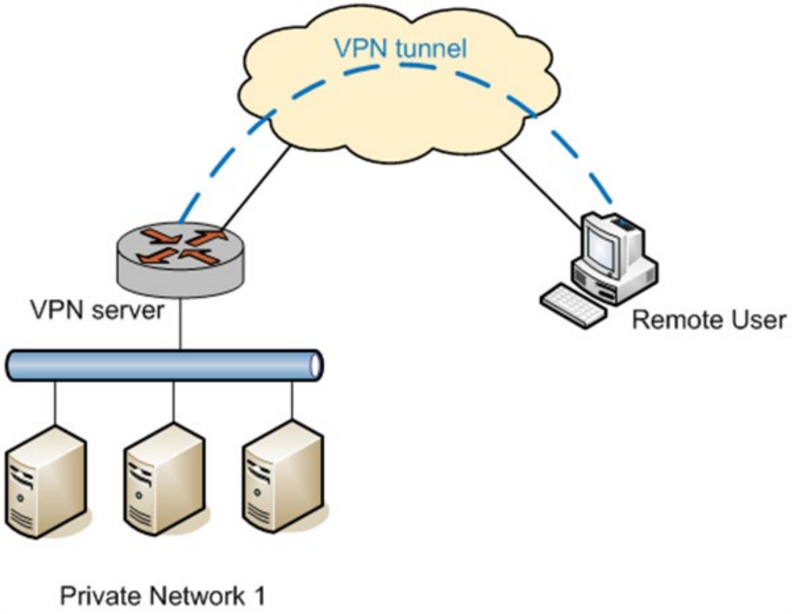
If you disable or don't configure this setting, the default app behavior occurs and no additional page appears.

Setting	State
Allow Developer Tools	Not configured
Allow Extensions	Not configured
Allow InPrivate browsing	Not configured
Allow web content on New Tab page	Not configured
Configure Autofill	Not configured
Configure cookies	Not configured
Configure Do Not Track	Not configured
Configure Favorites	Not configured
Configure Home pages	Not configured
Configure Password Manager	Not configured
Configure Pop-up Blocker	Not configured
Configure search suggestions in Address bar	Not configured
Configure SmartScreen Filter	Not configured
Configure the Enterprise Mode Site List	Not configured
Configure WebRTC Media Port Ranges	Not configured
Prevent access to the about:flags page in Microsoft Edge	Not configured
Prevent bypassing SmartScreen prompts for files	Not configured
Prevent bypassing SmartScreen prompts for sites	Not configured
Prevent using Localhost IP address for WebRTC	Not configured
Send all intranet sites to Internet Explorer 11	Not configured
Show message when opening sites in Internet Explorer	Not configured



Configure Favorites	Not configured
Configure Home pages	Not configured
Configure Password Manager	Not configured
Configure Pop-up Blocker	Not configured
Configure search suggestions in Address bar	Not configured
Configure SmartScreen Filter	Not configured
Configure the Enterprise Mode Site List	Not configured
Configure WebRTC Media Port Ranges	Not configured
Prevent access to the about:flags page in Microsoft Edge	Not configured
Prevent bypassing SmartScreen prompts for files	Not configured
Prevent bypassing SmartScreen prompts for sites	Not configured
Prevent using Localhost IP address for WebRTC	Not configured
Send all intranet sites to Internet Explorer 11	Not configured
Show message when opening sites in Internet Explorer	Not configured

Limit VPN access



This is not popular with the OEM or vendors.

- Sometimes vendors need remote access and they ask for it from the Hospital IT Security team.
- IT gives access after verifying the servicer or OEM
- Several redundant accounts can be created - creating vulnerabilities
- VPN logins should be purged regularly. What is your policy? Do you have one?
- Know who is getting into your network

Track sensitive hardware and operating systems

- Tablets and Laptops can have VPN access.
- Lost and stolen hardware accounts for up to 15% of breaches. Bring awareness to this.
- What vulnerabilities do your OEM servicers, doctors or nurses take home with them?
- Put these things in your CMMS system and track them! Track Vulnerabilities.

Look at Zero Trust policies.

Get active on purchasing of capital equipment

Check for the security breaches from a device before buying it. Ask about Embedded security vs Bolt-on security.

- Ask about the OEM support for updates and patches
- Ask about further testing for cyber attacks from the OEM
- Ask about cloning drives, software recovery, patient file protection, password complexity, network segmentation

Embedded Security - Part of the concept

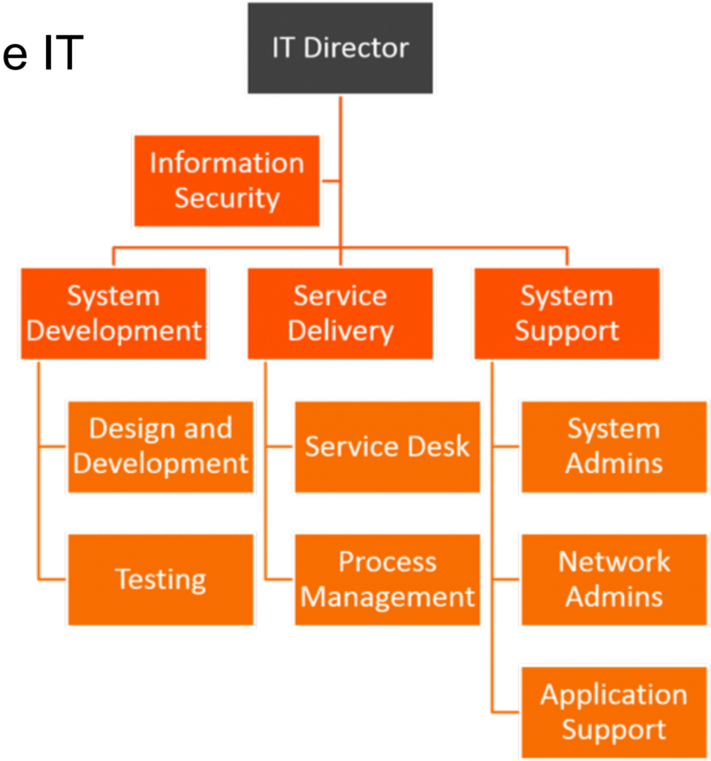
Bolt on Security - an afterthought or option

We are not only to use the OEM, but also IT

Do you know the sub departments in your in house IT team? IT is compartmentalized by design.

- IT Desktop Support team
  - Support Technicians
  - Help Desk Technicians
  - Trainers
- IT Network Support and Server Support
- Web / App development and support team
- IT Information Security and Compliance
- IT Management Team and CIO

See any HTM tasks? (We are merging)



IT Director

Information Security

System Development

Design and Development

Testing

Service Delivery

Service Desk

Process Management

System Support

System Admins

Network Admins

Application Support

Things HTM & IT can do about network security

- Work on **policies** and follow them. Establish Vendor / tech access logs
  - Vendors can reset things - Do you know when it happens?
- Identify **operating systems**, their version, and their locations
- **Logins** - Do you use active directory - Set strong passwords
- Limit **VPN access**. Ask the “Hard questions” about remote access
- Network Design - We need to think security by design. (IT already doing it)
  - **VLAN** - How do the isolate devices and control traffic flow?
  - **ACL** - How do they control LAN access to other devices and internet?
  - **Intrusion Detection / Prevention systems** -Do they monitor access?
  - **Cisco ISE** - How do they handle control in emergency situations?
- IoMT consultants - Ask for help - **Check them out at the show today!!!**

Know the devices to understand vulnerabilities

A device like this can be on weird things, like beds or blanket warmers

If you were told that there was a problem with Windows 10 version 1909:

- What machines would that effect? Do you have a list? Where are they? What departments are affected?
- When is the last time they were updated? Can they be patched? What OEM support can you get?
- How do they connect? Who do they need to connect to? How are they restricted? How are they monitored?

IoMT means we will have computers in odd places

- Raspberry Pi - Mint Linux
- Android devices / iOS devices = Linux / UNIX

Control Logins - Do not use generic logins

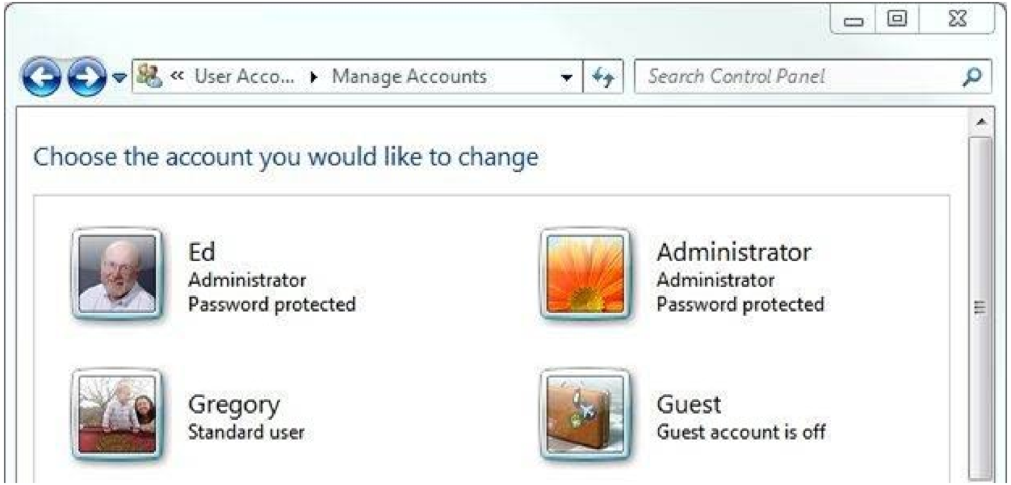
Authentication - Login control. Limit who can access the system

Authorization - What can you do? Not all logins are the same

- **Administrators** - can install programs and make changes to the system
- **Users** - can use the system - can't make system changes or install programs without an admin password.

Watch out for generic Administrator and Guest accounts.

All accounts should have a password.



Choose the account you would like to change

Ed
Administrator
Password protected

Administrator
Administrator
Password protected

Gregory
Standard user

Guest
Guest account is off

Use Stronger security measures

Have a policy for passwords using upper and lowercase characters, symbols, and numbers: Us3C@mm3lC@s3 = Use Camel Case

Have a policy to change passwords periodically

Keep in mind that up to 35% of breeches are email in nature.

Get ready for newer login techniques: Security is something you have, something you are, something you know.

- You have a FOB or Key card
- You know a password and login
- You have a biometric scanner (Cell phones are the future)

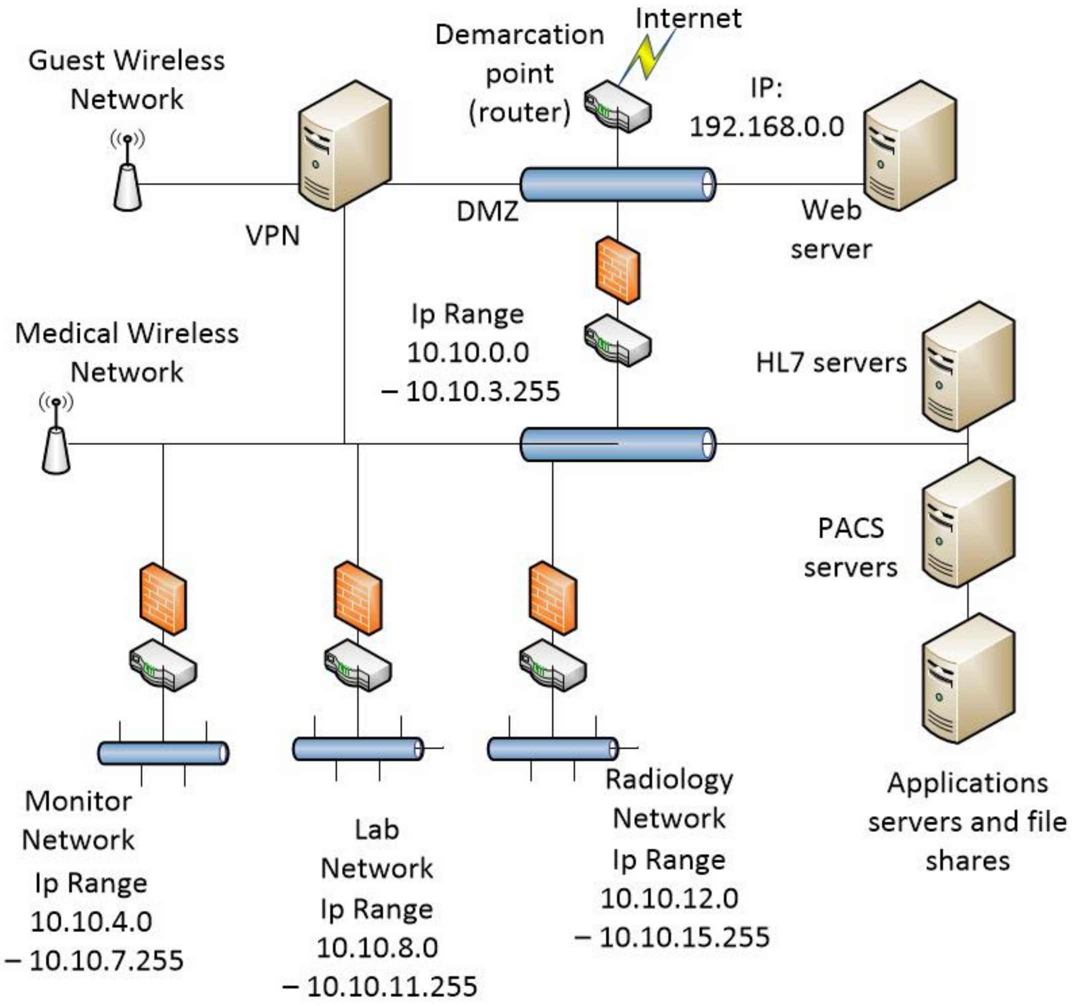
Sandbox Updates

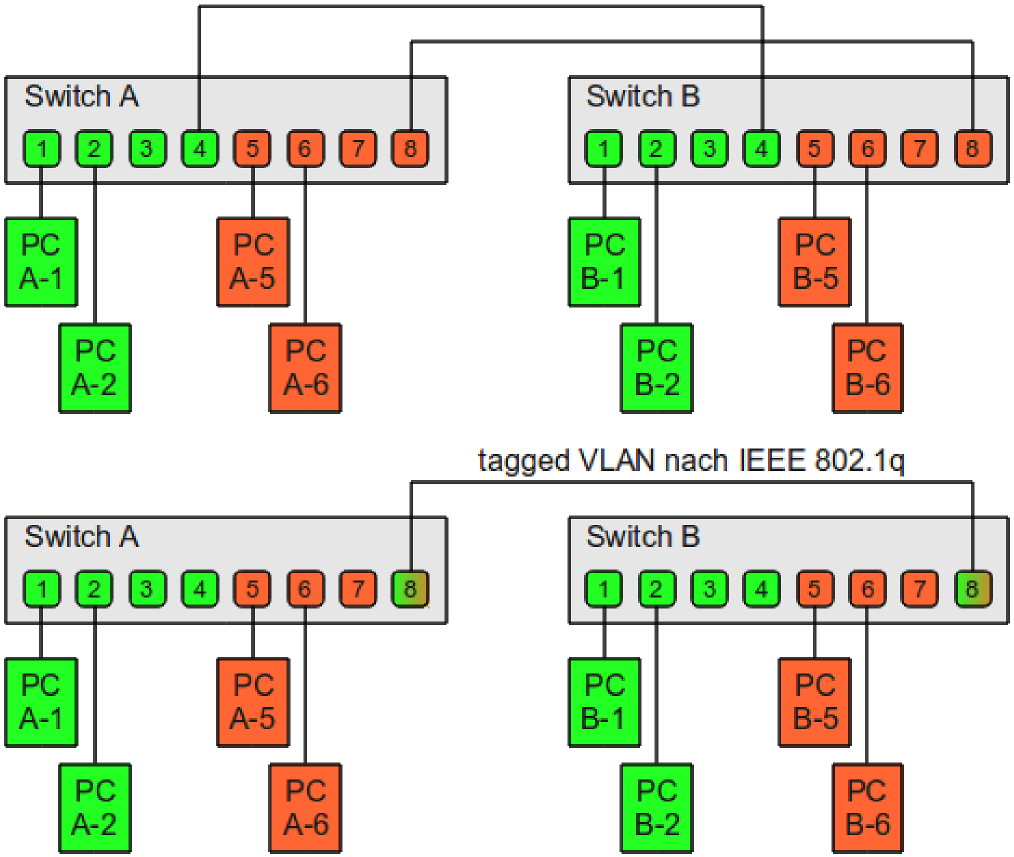
- Test upgrades and updates on a test system off of the network.
- See if it is stable before implementing to all other devices
- Watch out for versions of Operating Software.
- Remember to run backups of drives if possible - Clonezilla and spare drives. Copy a running systems HDD

Learn TCP/IP Network Segmentation

Separate networks into smaller segments that operate independently of each other.

This protects the systems and controls the data flow on a small scale.


Internet
Demarcation point (router)
Guest Wireless Network
IP: 192.168.0.0
VPN
DMZ
Web server
Ip Range 10.10.0.0 – 10.10.3.255
Medical Wireless Network
HL7 servers
PACS servers
Monitor Network Ip Range 10.10.4.0 – 10.10.7.255
Lab Network Ip Range 10.10.8.0 – 10.10.11.255
Radiology Network Ip Range 10.10.12.0 – 10.10.15.255
Applications servers and file shares



VLAN - Virtual LAN

Used to control data flow on a larger scale.

- Set at the switch
- Separates a big switch into multiple smaller switches
- Communication does not leave the VLAN
- Use a Trunk (Tagged) data link to the next switch
- Use Routers to bridge VLANs

ACL access is now set by some HTMs

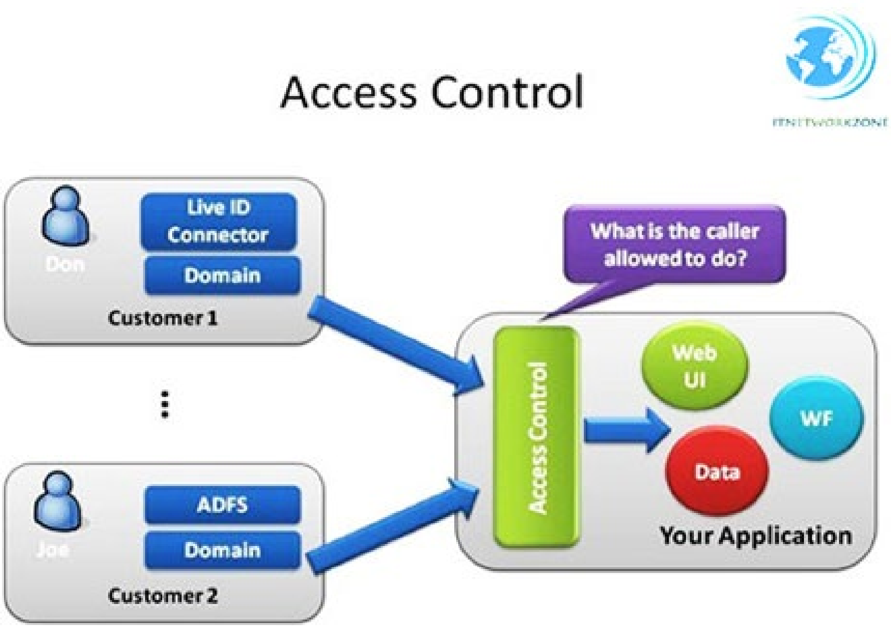
Access Control Lists what MAC addresses or IP’s have access to which machines

Has ingress and egress rules

Can be as simple as “Machine with IP ________ can talk to IP _________ on port ______”

Used to watch behavior as ports are software specific- **Understand Ports**

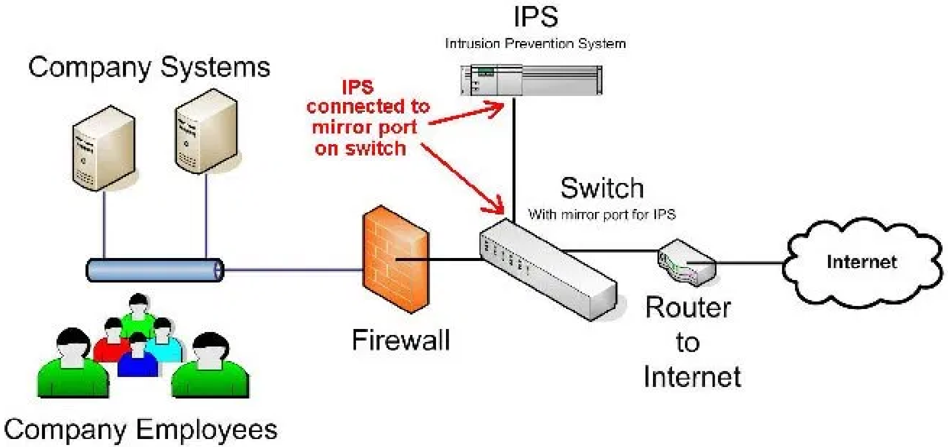
Stored at any device with firewall (switches and routers)



Intrusion Prevention (or Detection)

Software or server that monitors and logs what it sees on the network

- Addition of new devices
- ACL / Firewall issues
- Network scans - active probing
- Clone IP / MAC addresses



Can work with Cisco ISE

- Makes VLANs to isolate suspicious devices

Norton by Symantec

McAfee

TREND MICRO

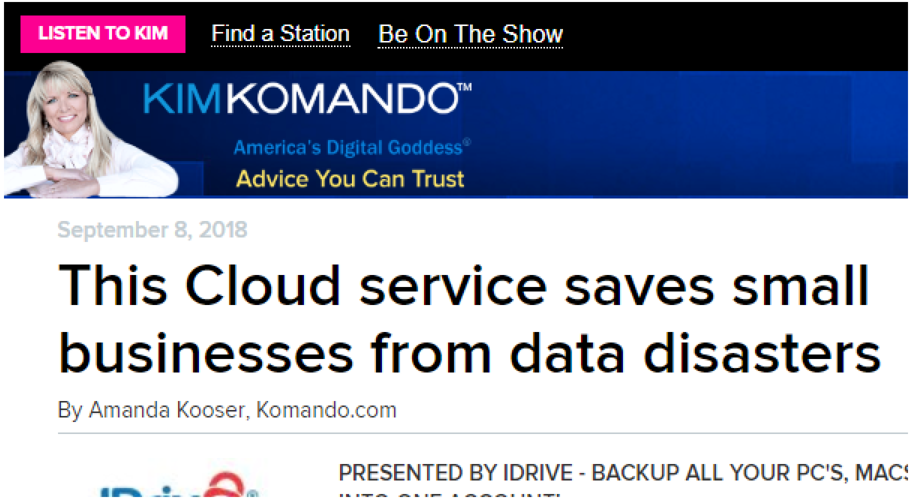
CISCO

Ask IT about Cloud apps and data storage

Newer technologies such as cloud applications allow hospitals to pool resources and ensure security with a 3rd party storage option, such as Iron Mountain.

Use Epic, AGFA, Carestream or other cloud system to push data to secure locations quickly. Encrypt traffic.

Look for things like “Hosted on Amazon EC2 (AWS)”



September 8, 2018

This Cloud service saves small businesses from data disasters

By Amanda Kooser, Komando.com

PRESENTED BY IDRIVE - BACKUP ALL YOUR PC'S, MAC
INTO ONE ACCOUNT!

*Problem with cloud… who owns it? Remember: HIPAA keeps us honest

Look at some of the people in the show today!

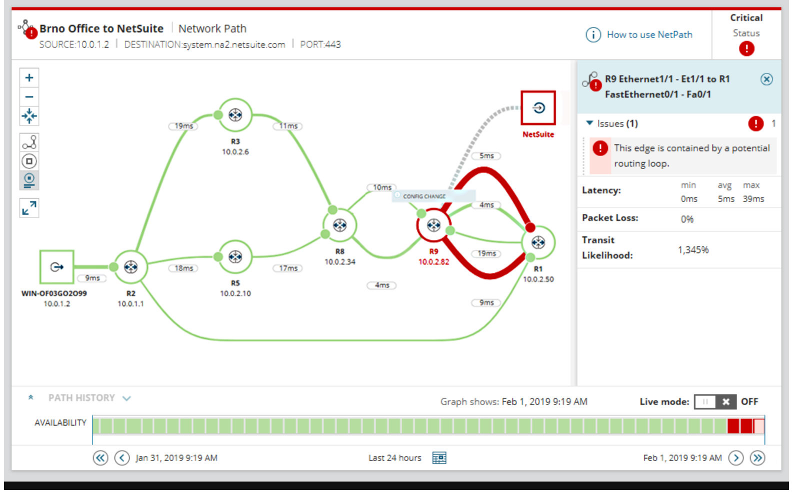
- There are companies that help find vulnerabilities,
- Ask about Cisco ISE
- They do passive scans for about 2 weeks and report the machines and all meta data they find.

MEDIGATE

Cynerio

SUPERIOR analytics®

ordr



Brno Office to NetSuite | Network Path

SOURCE:10.0.1.2 | DESTINATION:system.na2.netsuite.com | PORT:443

How to use NetPath

Critical
Status

R9 Ethernet1/1 - Et1/1 to R1 FastEthernet0/1 - Fa0/1

Issues **(1)** 1

This edge is contained by a potential routing loop.

Latency: min 0ms, avg 5ms, max 39ms

Packet Loss: 0%

Transit Likelihood: 1,345%

PATH HISTORY

Graph shows: Feb 1, 2019 9:19 AM

Live mode: OFF

AVAILABILITY

Jan 31, 2019 9:19 AM — Last 24 hours — Feb 1, 2019 9:19 AM

Checklist of IoMT Cybersecurity - Preparation

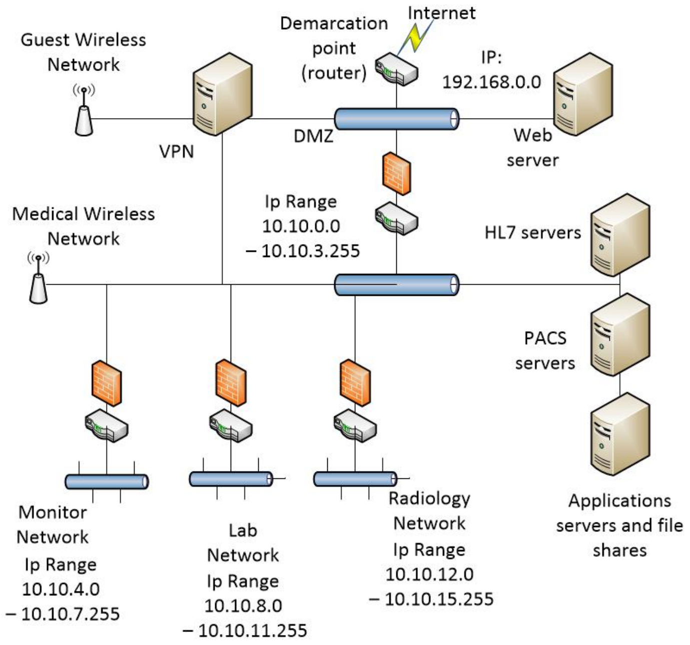
- Actually use a BET **Risk Assessment** to tell vulnerabilities
  - Tell what equipment / operating system is the most vulnerable
  - Tell how your network is put together, VLAN and segments
  - Use ACL, Strong Passwords, Intrusion Prevention
  - Tell where to go to defend against an attack or what machines to isolate first. Where are the vulnerabilities? Know your IoMT.
- Keep logs of **Operating Systems** for each machine
  - Patch revisions and Software Revisions and machine location
  - Security Packs / Windows Updates - Antivirus Updates (FDA is OK)
  - Sandbox when updating - Copy the HDD
  - ACL, ISE, Intrusion Prevention used when possible
- Use this data when selecting **New Purchases**, get active.
  - Embedded security vs bolt on security and long term support
  - Remind people: We reduce loss, prevent breaches and fines
  - Ask the hard questions to the OEM but remember to get them onboard

What to do when Hacked?

During Hack - Damage Control -

Do not assign blame - Evaluate the damage

- ○ Isolate systems using VLANs. -IPS
- ○ Disable outgoing traffic immediately
- ○ Go to paper redundants
- ○ Call in the problem stakeholders
  - ■ (IT, Risk Management, OEMs, EPIC, ect.)
- ○ Average 180 day lag on detection


Internet
Demarcation point (router)
Guest Wireless Network
IP: 192.168.0.0
DMZ
VPN
Web server
Medical Wireless Network
Ip Range 10.10.0.0 – 10.10.3.255
HL7 servers
PACS servers
Monitor Network Ip Range 10.10.4.0 – 10.10.7.255
Lab Network Ip Range 10.10.8.0 – 10.10.11.255
Radiology Network Ip Range 10.10.12.0 – 10.10.15.255
Applications servers and file shares

What to do when Hacked?

After Attack - Transparency, not misinformation is key.

- Do an after action report
- Hire a consultant / do penetration testing

Contact the following within 60 days after discovery

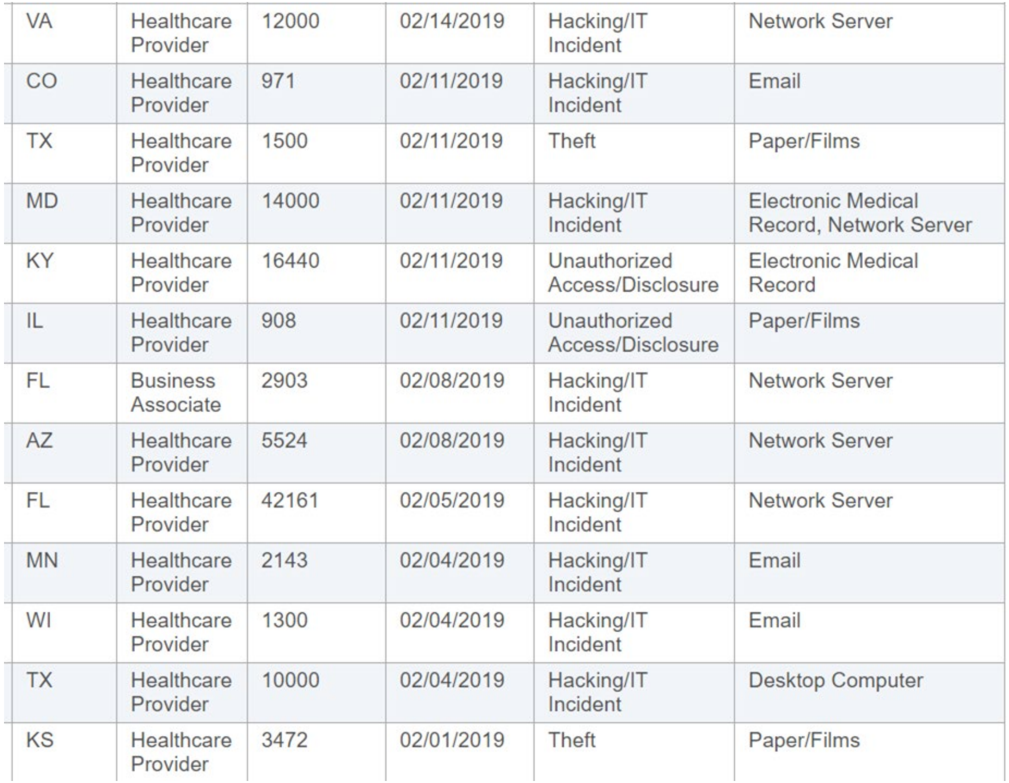
- Let Risk Management handle press.
- Contact US Department of Health and Human Services - Office of Civil Rights (OCR) - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Contact state-level health services in all states where patients are involved
  - It's better to over report than under report
  - Local police need to be involved - Let them assist or call in assistance
- Alert patients whose records are involved by mail

What happens if I do not do these things?

CHS settles patient data breach for $5M (for 6 million records)

“The CHS associate, named CHSPSC, agreed to pay the Office for Civil Rights $2.3 million to settle the HIPAA breach, according to a Sept. 24 news release. OCR's investigation found that the company failed to conduct a risk analysis and implement access controls”. - Source: Becker Hospital Review 10/8/2020

Past attack trend data



VA	Healthcare Provider	12000	02/14/2019	Hacking/IT Incident	Network Server
CO	Healthcare Provider	971	02/11/2019	Hacking/IT Incident	Email
TX	Healthcare Provider	1500	02/11/2019	Theft	Paper/Films
MD	Healthcare Provider	14000	02/11/2019	Hacking/IT Incident	Electronic Medical Record, Network Server
KY	Healthcare Provider	16440	02/11/2019	Unauthorized Access/Disclosure	Electronic Medical Record
IL	Healthcare Provider	908	02/11/2019	Unauthorized Access/Disclosure	Paper/Films
FL	Business Associate	2903	02/08/2019	Hacking/IT Incident	Network Server
AZ	Healthcare Provider	5524	02/08/2019	Hacking/IT Incident	Network Server
FL	Healthcare Provider	42161	02/05/2019	Hacking/IT Incident	Network Server
MN	Healthcare Provider	2143	02/04/2019	Hacking/IT Incident	Email
WI	Healthcare Provider	1300	02/04/2019	Hacking/IT Incident	Email
TX	Healthcare Provider	10000	02/04/2019	Hacking/IT Incident	Desktop Computer
KS	Healthcare Provider	3472	02/01/2019	Theft	Paper/Films

These are HIPAA Breaches from Feb 2019 (42 in Feb 2020)

- **29 breaches** reported in **Feb 2019**
- **25** of the 29 were coded "Unauthorised Access" or "**Hacking**"(36 of 42 in Feb 20)
- **4** were "**Theft**" or loss of an item (2)
- 14 direct system or server hacks (29)
  - **8** were **email** related hacks (24)
- Hacks **up 50%** from May 2017 (**+44%** from Feb 19 to Feb 20)
- Involved over **2 million Patient records** - 25 times increase from May 2017 (**1.6** Million in Feb 20)

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Is the sky falling? … No

- We are not at the front line of this defense.
- We are being asked to do more, IoMT is a real factor. There is support. Use it!!
- Thankfully, we do have a hospital IT security team to help
- We have OEM development teams who are talking about this stuff.
- We are on the peripheral edge of the war on cybercrime. This is changing.
- This is about minimizing risk, we are good at that. We Do, Document, and Follow up

Questions