Stopping Snake Oil With Smaller Healthcare Providers

Addressing Security With Actionable Plans and Maximum Value

Indiana University Health

Abstract

- Healthcare has been the most affected industry by ransomware, data breaches, and hacks. Every week there is news of yet another provider that has been hacked. In multiple cases, this has led to practices shutting down, and patients not even able to get their medical records. The guidance provided to many providers has not specifically addressed what organizations need to do to protect their patients and themselves. There has not been a specific list and toolset they can use to protect themselves.

Why are we here?

- There have been many snake oil companies out there that have only provided risk assessments, costing smaller providers tens of thousands of dollars, while not delivering anything of value
  - Or worse, taking money out of risk management plans – negative value!
- We want to change that and provide maximum value and immediate returns
- We want to help smaller organizations spend scarce resources more wisely
- We want to give orgs something they can use as a baseline

Why am I here?

- Because we're sick and tired of hearing about smaller providers getting ripped off by unscrupulous Information Security companies
- I've been in Healthcare Infosec since 1998
  - Started out by getting rid of one of those unscrupulous people for a client
  - Repeated this at two other organizations
  - Moved up the ranks to CISO
- This is 22 years of experience in a shortened format designed to give an understanding of our security challenges
  - And how we can do more to fight back

What assumptions are we making?

- Small medical office or critical access hospital
- The person in charge of the risk management plan will not know computers well. They don't have to
- Computers used to access a lot of onsite and offsite resources
- Numerous applications, all with different usernames and passwords
- No clue as to what is going on

What is our agenda today?

- Risk Assessments, how to do them, and why to do them internally first
  - Tool download: A quantitative risk assessment tool we developed in Excel
- Using that to develop the Risk Management Plan you need
- Policies and Procedures – how to develop them and what you really need
- Physical Security – Why this is important
- H-ISAC and HSCC – Who they are and what resources they have!

Agenda

- EMR Maintenance – what to do and why
- Password Managers
- PCI – Why keeping up here is important
- Firewalls/VPNs and how not to turn them into your worst enemy
- ZFS – why you need this for local file storage in healthcare
- Cloud-based backups and why you need them (esp. Ransomware)
- Samba 4.x – why this works for authentication
- EDR – why this instead of AV

Agenda

- Flash Drive Encryption and why keeping to open source solutions works
- Good encrypted email with a secure portal
- Good two-factor authentication is not expensive
- CTUpdate WSUS Offline Update – A friend to BYOD and data caps
- Vendor Management – what to do?
  - Again, free tool download
- Callback policy on cashback or wire transfers

Agenda

- Training that doesn’t suck
- Have someone to call, always
- Thanking you for your time and opportunity

Risk Assessments

- We always advocate doing these internally with some outside help instead of just having one done by an outside firm
- You need to know your business well and know where the holes are
- The most critical part we have found is to be honest about compliance status
  - This will also get you in trouble with OCR and your insurance company if you are not
- This is not a death sentence or an IRS audit. The goal is always to improve
  - Even OCR admits that

Risk Assessment

- Quantitative is the method we use because it helps prioritize how we address risks
- We put one together with an Excel spreadsheet you can download based on the CMS Systems Readiness Assessment tool that evals risks based on:
  - Likelihood
  - Impact
  - Velocity
  - Potential Income Loss
  - Reputational Impact
- The scores attached to each identified risk can help prioritize controls

Risk Management Plan

- In the supplied spreadsheet, there's a Pivot Table for identifying your top risks
- Concentrate on the 20%
  - You will address most of the remaining 80% residual risk as part of the plan
- Develop a set of methods and processes to address these risks as part of a plan
- Always include a communication plan
- Assign accountable parties
- Keep following up and document when you do – keep a spreadsheet

Policies and Procedures

- You need to have these – these are HIPAA requirements
- You should address these by identified risk and develop/release them in that order
  - If you try and release these all at once and not part of an overall plan no one will follow them
  - If you can't tie back to an ID'd risk, same effect
- We recommend the policy template provided by HHS at:
  - https://www.healthit.gov/resource/information-security-policy-template

Physical Security – why is this important?

- We have treated building management separate from the rest of the enterprise
  - They also live on much longer lifecycles
- This means that while we have done a great job with our desktops and EMRs – we have unpatched machines with network access running older Windows versions
  - The Amiga 2000 that was running the HVAC for a school district was more secure
- Anything with a network connection or that protects data is now in scope, not just the Electronic Medical Records system itself
- Include these in your risk assessments and protect adequately!

Healthcare ISAC and Health Sector Coordinating Council

- Two organizations that participate heavily in intelligence sharing and threat intelligence are the
  - Healthcare Information Sharing and Advisory Center (H-ISAC)
    - https://h-isac.org
  - Health Sector Coordinating Council (HSCC)
    - https://healthsectorcouncil.org/
- H-ISAC provides excellent content, mailing lists, and threat intelligence for healthcare organizations
- HSCC provides significant guidance, content, recommendations, and coordination between members

Electronic Medical Record Maintenance

- If you are hosting one on your own, stop
- They are now getting so complex that they are prohibitively expensive to maintain
  - Security is now very challenging for smaller organizations
  - In addition, you have regulatory requirements that require a team
  - A bigger health system can do this for you and do it better
  - Tools such as privacy and diversion monitoring that larger ones have can be leveraged for your organization

Password Managers

- No other industry I have worked in has an emphasis on having numerous incompatible logins
  - And never heard of federation or SSO to address them outside of the key clinical systems
- This means you need to get one of the good password managers on the market and make sure your team knows how to use it
  - Even Google Chrome is an improvement over what we have now
- And is now an absolute must for your team members

PCI-DSS

- Very few people pay cash in doctor's practices anymore
- However, many credit card machines have not kept up with the times
- People think PCI Compliance is one and done
  - Hint: It isn't and that PCI 2.0 compliant device doesn't take chip cards
  - Customers demand the chip cards work like Walmart and CVS
- Work with your bank and app vendors, and get the latest P2PE (Point to Point Encryption) devices
  - They will literally give them away to you
  - You will need to update quarterly and plan for it

PCI-DSS

- Partner with a Revenue Cycle vendor to handle your payments and provide a patient portal
  - You do not want to assume the risk of running this yourself
  - Or trying to make a small network PCI Compliant
  - Or writing down credit card numbers
  - Or recording them on voicemails
- This is a risk you should pay someone to assume, not a risk assessment
  - In this case risk transference is a wise move

But we have a firewall!!!

- And you opened port 3389 on it and you didn't patch it
- One of the most important lessons from COVID-19 is that remote access is a large target
- That same appliance that worked 5 years ago is not effective against modern threats
- Remote Desktop is not effective – you will get owned
- Remote Desktop Services gateways or OpenVPN on pfSense on a Core 2 Duo will do a better job than many of the appliances out there
- Even Google Remote Desktop protects you better
- If you run RDP or old VPN, say hello to ransomware

ZFS – why not just a RAID array or file shares?

- Under the HIPAA Security Rule, we have to maintain the confidentiality, integrity, and availability of data
- We focus a lot on confidentiality and availability – not integrity
- We have a lot of patients who will need 30-40 years of medical records
  - Esp. pediatric craniofacial surgery patients
- The probability of data becoming corrupt over the years is very high
  - We need to guard against file corruption and protect file integrity
- Many of the common file systems on low-cost servers and NAS devices do not do this (yet)
- Right now a number of ZFS-based appliances available that can protect files

Cloud-based Backups and why you need them

- We spoke with Hancock Regional about why they paid
- It came down to recovery time and getting systems back
- If and when you get attacked, you need to protect your backups
- Major insurance companies are now asking if you store backups separately under a different set of credentials
  - They also ask if you test them
  - This is because ransomware actors know where to go to find them and encrypt them first
- Your average cloud provider will have better security than you

Samba 4.x for Domains

- Many of the applications we still run require Active Directory authentication on Windows
  - This is a fact of life
- This can run on a small Linux VM or appliance not requiring much care and feeding
- Easy to integrate with small NAS appliances and Windows
- Better than licensing a Domain Controller and MS licenses

Secure Email

- We need to be able to securely send email to patients
  - We cannot assume they will read it on anything remotely secure
  - Secure Portal apps do not support patient satisfaction
    - I wanted to throw my computer at a wall after dealing with one for my kids
  - Providers don't read multiple inboxes
- The current vertical solutions out there for it can be prohibitively expensive
- Stick with good secure providers like Protonmail that provide the encryption, mobile access, and a simple secure portal

EDR

- Antivirus in healthcare is DOA
- Too much interference with applications
- Too many exceptions that allow malware to execute due to getting apps to run
- EDR integrates better with SIEMs and log management technology
- Integrate with tools like osQuery to provide analytics
- Less time spent figuring out why your apps don't work and making exceptions that open holes for malware

Flash Drive Encryption

- One of the major challenges of flash drives has been proprietary drives
- For example: I have one that I used for transporting pictures that no longer works on MacOS due to being 32-bit
- Significant churn in the encryption vendor market means that data you have now may not be decryptable 10 years later due to OS constraints
- Stick to the Open Source solutions for your encryption – at least you will have a better chance of reading your data

Two-factor authentication

- If there is one factor that has stopped the majority of hack attempts, it's a good two-factor authentication solution like Duo, Authy, or Yubikeys
- This is esp. true for healthcare, where numerous phishing attacks use compromised accounts
  - They gain access to send via secured email systems
  - This bypasses most anti-spam protection
  - They also provide access to internal networks for further analysis/recon/etc.

WSUS Offline Update

- We have used this tool extensively
- All Microsoft and Office patches on one flash drive that doesn't kill bandwidth
- Lets you quickly get a machine up and patched

Vendor Management

- You need to perform risk analysis of your vendors
- However, you need to start with a good baseline and requirements
- Use ours: https://iuhealth.org/about-our-system/vendor-relations
- Most vendors are not going to answer questionnaires
- More are getting certified and it makes our job easier if they do

Callback Policy

- At this point, you should not allow wire transfers without:
  - Having an established vendor relationship
  - Speaking with them on the phone
  - Having someone confirm, even if internal, with the supposed executive asking
  - Confirming any changes with someone trusted
- The BEC attacks we have seen all rely upon impersonation of trusted executives to coerce people into sending money without checks or phone calls
  - They always seem to be busy or in meetings!

Training That Does Not Suck

- Most Security Training Sucks
- Unless it directly ties into their job or affects them they will not care
- Keep it short, sweet, and relevant
- Discuss what people need to do
- If you make it longer than 3-5 minutes you lose people
- Policies come with training plans. Always.

Always Be Available

- You need to make sure you or trusted team members are available
- When a computer security incident happens, it's a very bad day for the victims
  - Do not play the condescending edgelord – you will upset people, and yourself out of a job
- Always respond to customer requests
- Always say Please and Thank You
  - Your elementary school teachers were right

And with that, THANK YOU!

- Follow me on Twitter @mitchparkerciso
- Special thanks to:
  - Chetrice Romero, Program Director, Indiana Executive Committee on Cybersecurity
  - John Riggi, Senior Director, Cybersecurity, American Hospital Association