A CISO Perspective. HIT Security, Ransomware, and Enterprise Risk Management

Information Security & Compliance

HEALTH Indiana University Health

Purpose of Presentation

- To show why tools are just part of the plan for success
- How to improve cyber security through monitoring the overall program.
- To give CEOs and CFOs the knowledge they need to effectively monitor and guide their cyber security programs

Why am I really doing this?

- Because CEOs and CFOs get told stories by people who want to look good in front of them - human nature
- This leads to metrics and measures that talk a lot and ultimately say nothing – and frustrated CEOs and CFOs
- This also leads to metrics and measures that don't help you truly understand the root causes of risks and how to fix them
- Ergo, you put band-aids on a festering problem without addressing real root causes
- We want to help you understand why these problems really exist and what you can do to help your organization

Why am I really doing this?

- Because you get conflicting answers as to what works and what doesn’t
- I want to give you a good path forward to quantitatively reduce risk and show progress
- The current situation involves multiple people pitching multiple ways to solve problems – it’s not working!
- We want to get you on the path to know what to ask for and get something working for you that actually reduces risks and focuses limited resources

How does Ransomware fit into this?

- Ransomware takes advantage of poorly run organizations
- If you are not able to build in basic defenses, it gets in and propagates
- If you cannot assess or address the effects, you shut down your business
- If you can’t recover easily or have good downtime procedures, you will shut down your business
- Ransomware works because it costs less than the expected business loss to recover
- It’s not something you can buy a magic tool to fix – there will always be one that gets by the best defenses – ask Merck

Agenda

- We will cover several key areas:
  - Model Systems – Why customizations put your organization at risk and what you can do about it
  - Legacy Systems – How relying on legacy systems can put you at risk
  - Enterprise Risk Management – why consistent scoring matters and why you need to do this
  - Business Impact Analysis – Knowing what's critical and being told what is critical are two different items
  - Processes – Where they work and don't work, and what you should focus on

How did we get here?

- I’ve been a CISO for 10 years at 2 health systems (Temple Health and IU Heath)
- A large part of my job has been spent in several areas
  - Figuring out the root causes of issues
  - Interfacing with lawyers, auditors, OCR, and outside agencies
  - Addressing why we had these issues in the first place
  - Developing the remediation plans to fix broken processes

How did we get here?

- I started my career pre-CISO in data conversion – not security!
  - Completely opposite the career path many of my peers took
  - Migrated a large number of bespoke systems to standard schemas and platforms
    - End Stage Renal Disease Management (CMS Contractor)
    - Several DOD projects
    - OTTR for Kidney, Liver, Heart, Lung Transplants and Dr. Criner's custom pulmonary databases (Temple)
    - Custom call center system to Healthline Echo Access (Temple)
    - Multiple bespoke systems to AmCom (Temple)
- Before I was a CISO, I was the consultant you called to fix these problems
  - TUHS IS and Call Center departments were my biggest customers

What were the most important things I learned?

- Customization is really expensive- software development is very hard to get right
  - Even DOD has moved away from it and they spend tens of billions on it
- Most customers go in with the best of intentions and end up regretting it
  - A number of my jobs at Temple were to rip out custom software and convert them to standard platforms (AmCom, OTTR, Echo Access)
- You will not be able to maintain an in-house system as well as Cerner, Epic, OTTR, or a company whose core competency is in those areas
- Anyone who tells you otherwise is not doing so with the best interest of your company at heart
  - Or never had to use TDS/Desktop 7000

Model Systems – where they started

- Back in the 1980's, companies such as SAP and Peoplesoft made a lot of money by taking the old AP/GL systems custom-developed on mainframes and moving them to a client/server platform
- This had the effect of standardizing companies on the big ERP platforms
- This allowed for better data interchange – if you chose not to customize
- However, since many of the solutions were still highly customized, upgrades took a long time as everything had to be rewritten
  - Peoplesoft at my previous employer took a long time because of the vast number of customizations
  - Customization of ERP made HR and Finance very difficult to manage or audit

Model Systems – a tale of two EMRs

- Moving over to Electronic Medical Records from electronic ordering and custom records, two camps emerged:
  - Epic
  - Cerner/Everyone Else
- Epic has an entire system focused on standardization, management, customer support, and ensuring physicians are able to derive benefit from the EMR
- Cerner was focused on developing around organizations' workflows and allowing them to drive using powerful technology

Model Systems – A Tale of Two EMRs

- During the Temple Epic Inpatient Implementation, I had the opportunity to work with Noah Dermer and Stirling Martin, the former and current CSOs of Epic, on cybersecurity management
  - Their approach of structuring releases and changes meant that it was very easy for them to roll up cybersecurity changes and fixes into their releases
  - Low variety meant that it was easier for them to package and test fixes with a high degree of confidence
  - Caveat #1: Making sure that the Tech Services teams actually patched and maintained the server and network infrastructure (hint: Many did not)
  - Caveat #2: Keeping all the systems that interface with Epic up to date and current is also difficult

Model Systems – A Tale of Two EMRs

- When I got to IU Health, I got the chance to work with Don Kleoppel, CSO of Cerner, and Mike Hill, who leads their Security and Compliance Practice
  - High degree of customization means that fixes for security issues more often have issues with certain customers because they break custom code
  - **Cerner has drastically improved security under Don's watch across the board – he is a true security leader with an excellent team**
  - Customizations break all of the "extensions" that people put in
  - Cerner has had to fix not only their customizations, but those for the Siemens products they bought – bringing everyone onto one codebase
  - They have made incredible improvements in a short time despite team losses

Why are customizations bad?

- Instead of having people learn a time-tested and working system, building workarounds or interfaces means that you have a system that cannot be maintained
  - Not by the vendor or you
- Minor patches and fixes turn into major events with potential downtimes
- What you do to satisfy one doctor ends up upsetting them all when your performance is very slow or you have a data breach
  - You will have these issues, intentional or not
  - Don’t let one user hold you hostage
  - More important – don’t let your staff think they can break the rules to satisfy one important person – this happens more than you think!

Why are customizations bad?

- You will not be able to interchange data using standard formats with other health systems and realize collaboration benefits
  - FHIR, etc.
- You will not be able to use new technologies such as AI/ML that require standardized data sets and workflows
- You will have a system that every time a new vulnerability is discovered that you cannot patch
  - Your risk of infection goes up significantly
  - Your ability to recover due to customization goes down even more!

How can you fix this?

- Drive from the top down that customizations don’t happen – people need to learn how to use the system the way it was intended
- Emphasize that just because you can doesn’t mean that you should
- There are ways to interface with the EMR to accomplish functionality should you truly need it, like FHIR
- To realize the benefits and improvements in EMRs, you need to focus your business around it and make it key to strategy execution
- Emphasize that no one person is above process
  - We use Help Desk tickets filed by the C-suite to show this
  - If they can file a ticket, so can you

How can you fix this?

- Most important: Good Governance!
  - Have a standardized intake process
  - Avoid the temptation of “no IT involvement”
  - Vendors will always be pushy and offer good last-minute deals - that is no excuse to avoid process
    - You will spend money on something without due diligence that will cost you more money to fix on the back end
    - I have been on multiple teams to fix broken systems and processes caused by “good deals” - I had a consulting practice based on this
    - These “deals” overload the IT department and lead to disengagement when they have to fix yet another broken system

How can you fix this?

- Standardized Management
  - Standard policies defining expected work
  - Keeping to the strategy
  - Governance committees empowered to set and enforce standards
  - A C-suite that manages expectations accordingly
  - A CHIO/CMIO empowered to make decisions and stop overreach

Legacy Systems

- Much like customized systems, these present major risks
- Often this comes from the very high cost of replacement
- There comes a time when the benefit ends and it becomes onerous to continue its use
- Either one of several outcomes occurs:
  - People try to keep the system to justify positions or standing
  - The organization just cannot afford to replace it
  - It gets overlooked in isolation
  - It is so valuable that there is no viable option (often industrial or bespoke)

Legacy Systems

- Employee Engagement and Retention is another casualty
- Who wants to work on systems no one uses?
- Who wants to work with technologies that have no application outside their job and lead to no future?
- It's not millennials just being picky or stereotypical!
- It's people seeing a lack of innovation or forward thinking, and seeing that they will be stuck for years, perhaps permanently, and moving on because of it
- We are no longer in a place where people take a job and stay there for 30 years. Give them a reason to stay, a way to advance, and they will!
  - You are shooting yourself in the foot with your future!

Legacy Systems

- When it come to disaster recovery, this is a major, major risk
- Oftentimes you will not be able to find hardware, software, or resources to even bring a system back up in case of a cyber attack
  - **If you do, be prepared to pay IBM tens of thousands of dollars**
- This is especially true for Ransomware – there are many old systems out there that are so old that you cannot secure them against it
- The older a system is, the harder it is to find parts or expertise to replace it
  - eBay does great business selling old hardware for this reason
  - Many people still run XP for that one device that doesn't work – new machines can't

Justify Positions or Standing

- This is especially salient with Cloud Computing
- This means that people manage or justify headcount with assets even though a more efficient solution is available
- This also has the side effect of keeping technology around that is hard to use and not able to interface with modern technologies
    - Web Content Management systems and web applications are often the ones used ironically
    - I have seen old web CMS kill revenue and marketing campaigns
- It also leads to technology you cannot secure
- You can solve this case by analyzing applications for alternatives

Not Able to Replace

- In the case of Clinical Engineering hardware and applications, this is very common
  - You will not spend money to replace medical devices just because their operating system is out of date – does not make sense
- However, there are options that vendors do provide and will work with you on that do not involves large cash outlays or partnerships
  - Those work for larger health systems, not smaller ones or smaller hospitals
- Solution: Lock down networks as much as possible and monitor – don’t use specialized med device security solutions – spend on asset mgmt.

It gets overlooked in isolation

- Many times an application works for one group and just sits there doing its job until it stops working or gets infected
  - Example: Pitney Bowes stamp machine running Windows 2000 and Call Center Apps
- With the Cloud, it becomes even easier for someone with a credit card to expense a small application and store PHI on it
- The issue is that under the HIPAA Security Rule, it's required to know your assets and data flows
- What you need to do is implement solutions to know what you have inside, and also examine your traffic to see who is using cloud apps you do not know about
  - You will find many applications you never thought existed

It’s valuable with no other option

- Often you will get this with customized robotics, industrial devices, or Supervisory Control and Data Acquisition (SCADA) systems for assembly lines
- These are one-off systems that most likely existed before networking or IT – they will cost millions to replace
- They may have had networking functionality built in to monitor and gather metrics
  - And were networked to facilitate central monitoring and consolidation
- Just like medical devices, you need to isolate, monitor, and protect them

Summary of Legacy Systems

- You will never keep everything up to date
- It is financially disadvantageous to do so
- However, it’s also disadvantageous to keep something around because of non-objective reasons
- You need to plan to manage device communications to be absolutely minimum
- You also should plan to replace them when possible - we don’t want you killing net income or bond covenants when there is a way to protect and extend lifecycles!

Enterprise Risk Management

- You need to assess risk across your enterprise
- One scoring system that covers:
  - Risks
  - Likelihood
  - Impact (Income, Brand, Retention/Engagement)
  - Will the impact affect other organizations?
- Everyone needs to use it
- Enforced by C-suite

Enterprise Risk Management

- Everyone needs to identify their top risks and score them
- Does not need to be complicated
  - Really, don't overthink this – you're not going to see benefit
  - If you get too tied up with this you won't have time to address risks or plan
- Does, however, need to be combined and weighted for the whole organization
- The output will be representative of your organization's perceived risks

Enterprise Risk Management

- You also want to do a security risk assessment using the same scoring system
- Many of the risk assessments done by the Big 4 don’t match up with ERM scoring
  - This leads to a disconnect because you have your security risks ranked differently than business risks
  - They need to be the same so you can present the same picture to the stakeholders like the Board
- If you outsource this it needs to use the same scoring system and format

Enterprise Risk Management

- We use the HIPAA Security Rule and ERM Scoring
- One consistent system that matches Enterprise Risk to Security Risk
- Easy to explain risks to Chief Risk Officer
- Easy to use numbers from our assessments in leadership presentations
- Consistency in communication and scoring enables us to communicate what our risks are and why

Business Impact Analysis

- According to the Department of Homeland Security:
- A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios which should be considered.
- Identifying and evaluating the impact of disasters on business provides the basis for investment in recovery strategies as well as investment in prevention and mitigation strategies.

Why do you do one of these for each department?

- You need to identify what resources are needed to support them during an interruption of service
- You also need to prioritize the order of events and systems for service restoration
  - Ones with greatest operational and financial impact should be restored first!
  - You need to do this after the risk assessment so that you know what the greatest risks are
  - However, you also need to look at alternative modes of operation
  - Also need to budget in Recovery Time for all processes, not just IS

HEALTH

What are the other benefits?

- The applications that you think they use are different than what they consider critical – this will show which ones
- This will also show what cloud-based and “Shadow IT” applications they use
- Use this to make sure that you prioritize backups and recoveries!
- You will also see the difference between what the business thinks it will take to restore service vs. what IS says – you need to manage expectations and the difference!

Processes

- This leads us to the processes we need to focus on
- Focus on scored greatest organizational risk
  - Do not get tied down with point solutions
  - Point solutions aren't going to mitigate risk – they are going to make someone's account fatter
- Look for ways to mitigate using resources you already have
  - Do not get focused on shiny things or people offering point solutions
    - Most of those companies get acquired or go out of business
    - Focus on the basics identified by the assessments – broadest solution set

Processes

- Use and train internal resources whenever possible
- Build out a team capable of executing enterprise risk assessments, security risk assessments, security planning, and following up
- Consultants will cost you a lot of money to do this work and you will not get consistent work out of them, even the Big 4
- You need consistency to execute this work
- Most important, you need ownership and an engaged staff to do it
  - Giving people an opportunity to help improve the organization and have a say improves engagement

This all fits together

- Give people a reason to learn, grow, and opportunities to improve and stay engaged
- Build a culture of setting and following standards and using model systems, and not just putting things in place just to satisfy a small group
- Good governance and consistency will help you here
- Have your team do quantitative Enterprise Risk Assessments, Security Risk Assessments, Business Impact Analysis, and Risk Management Plans
    - Make sure they own it and give them every opportunity to be engaged
    - Build from that information and use that to improve the organization

What happens if I don’t do that?

- You’re setting yourself up for failure at multiple levels
- Security isn’t just a tech issue, it’s a cultural one too
- You will have an environment which will lend itself to failure, finger-pointing, lack of accountability, and data breaches
- You will not be able to prove to the OCR, Joint Commission, or your state health departments that you accurately reduce risk or protect information
- You will have serious reputational risk damage

Thank you!

- Questions?
- Contact Info:
  - Mitch Parker
  - Mitchell.parker@iuhealth.org
  - 317 963 5577 (o)
  - 215 519 1053 (c)