Interdisciplinary Approach to Structuring Information Security

Mitchell Parker, MBA, CISSP

Executive Director, Information Security & Compliance, IU Health

Indiana University Health

Purpose of Presentation

- This session describes how to structure your Information Security program to include touchpoints and integrate with the rest of the enterprise

Two areas we are attempting to change

- Past/Current perceptions of security
- Having a realistic look at the contributing factors toward security issues

The big question we need to ask….

- Why do we still have so many security issues if we’re spending so much on it and getting the attention?

We need to focus on real ownership

- Not just on assigning it to someone
- Whole organization view on addressing it
- Significant dependencies on non-technical business processes

Focus on Communication

- Three major components of the business
  - InfoSec
  - Legal
  - Business Leadership
- In current practice, we're not communicating well and this leads to business issues that cause medical device or data breach issues

Focus on Communication

- FUD gets you nowhere
- You end up scaring people
- Scared people don't engage and report less issues

We need to focus on supporting the enterprise

- Emergency Management and Regulatory Affairs have specific IT requirements
- IT has been traditionally underrepresented in these areas
- With the rise of CMIOs and CNIOs in healthcare, we need to support the new clinical IS leaders
  - Now it’s about optimizing processes, not as much implementation

We need to focus on patient safety as a part of the job

- Medical Device Security is a patient safety issue and business issue
- Work with customers on augmenting their processes
- As medical devices increase in number and have a greater impact on outcomes, we need to make sure we reduce risk

HEALTH

We need to empower people

- Security is not just for IT anymore
- We need to get the message across to everyone
- Empowerment leads to better engagement
- Better engaged people are more likely to report security issues and not be afraid of repercussions

We need to engage people

- This is not just about having training
- Answer Their Questions!!!!
- Demonstrate improved patient safety and risk reduction
- Engage the workforce on their terms
- Demonstrate that we contribute to positive employee engagement scores
- Better engagement leads to better controls against insider threats

What does this really mean?

- This means we no longer can be aloof from the rest of the organization
- The days of being part of IT that hides are now over
- Information Security gets just as much exposure, if not more, than the CIO

The message is of empowerment, collaboration, and awareness

- Engage and Empower our organizations to work to fight the common goal
- Collaborate to share information
- Provide awareness at multiple levels to the workforce
- Not just the top leadership
  - While they help remove obstacles, they are not there every day

Grow out of just being in IT

- The risk is too great
- Cyber Security is a business problem
- Too many parallels with accreditation/regulatory
- Too many parallels with emergency management
- Too much of a risk with insider threats

Stop being trend chasers

- While there are very legitimate threats, if we keep chasing the latest threat of the moment, we won’t be truly addressing their root causes
- We will also build something that does not address the real issues
  - Device Management & Medical Device Security
  - Patient Safety
  - Emergency Management & Communication
  - Patient Engagement
  - Employee Engagement

Treat it like a business issue

- These issues have to do with business
- We need to Plan To Fail
- The entire business is affected due to cybersecurity issues
- The peripheral effect on us and our peers is very quick as opposed to isolated
  - Ransomware, Worms, and Business Email Compromise are prime examples

We are Information Risk Management

- We are more aligned with enterprise risk management, compliance, insurance, and privacy than IT
- We will go over how to structure this in the next slides

New Role of the CISO

- This encompasses the following five qualities:
  - Empower the workforce
  - Coordinate collaboration and Cloud
  - Educate on the organization’s terms
  - Outreach in coordination and in their words
  - Staff to Succeed

Why are we doing this?

- Regulatory - HIPAA, HITECH, OCR, Joint Commission, CAP, ACR, etc.
- Regulators want us to continually assess, plan, and address risks to a well-defined, yet constantly evolving set of standards
- So does FEMA and Emergency Management
- The major players, such as Joint Commission, at their root, want continual risk management as part of their processes
- We need to and are expected to Plan To Fail.
- Joint business/infosec/emergency preparedness approach to developing resiliency

What is Infosec Like Now?

- InfoSec is a lot like Joint Commission, CAP, or ACR requirements when run to address information risk
- Information Security is one component of many under the same constraints
- We need to realize that we have a lot more in common than we think
- We can use this to our advantage and work together
- Working together has advantages for all parties in modern healthcare

How do we empower the workforce?

- ANSWER EVERY QUESTION
- Be empathetic
- Always follow up
- Service with a Smile
- Make sure people know your cell phone # and email

How do we empower the workforce?

- Get out there and make your face known
- Assess risk continually - does not need to be formal
- Continually find gaps
- Circle back with customers and discuss resolving open risks together
- Frame of collaborating together to resolve issues

Empowering (continued)

- Based on your findings, develop 15-20 minute presentations about the program
- Provide basic explanations of security and why we do what we do
- Connect to Purpose for your organization
- Explain key initiatives and how they fit the organization's strategy!

Empowering (continued)

- Develop a monthly communication plan for your organization that addresses practical tips the whole team can follow
- Be timely - Christmas, Tax Time, and Black Friday esp.
- Put it on the Intranet
- Put it in email!

Empowering (continued)

- When you issue guidance, make sure that there are three levels to it:
  - Team Member
  - Service Desk
  - Management
- Provide words and actions they can use
- Make friends with Nursing and clinical staff so you can have someone non-IT review it

How do we coordinate collaboration and cloud?

- Get to know finance and supply chain
- Get to know Legal
  - Make sure your contracts and Business Associate Agreements cover the HIPAA Security Rule, HITECH, and specific implementation details
- Enculturate yourself with the business area leaders
- Cloud now comes in through multiple entry points
- Starting to see it as an "add-in" to other services
  - Many of which are legacy and do not undergo full review

HEALTH

Collaboration and Cloud

- Educate on how cloud security can be more secure than on-premises
- However, it needs care and feeding
- Going to the cloud does not obviate their need to maintain the application
- It also requires us to follow up a lot more and demonstrate their compliance
- Set firm risk assessments and baselines
- Always follow up and schedule to do so!

Educate on the Organization’s Terms

- Use their learning management system
- Use their format and scoring
- Use their governance
- Most important….customize what you have for them
- Don't give them third party content that you haven't customized or isn't relevant

Assess Risk on the Organization’s Terms

- Use their format and scoring
- Use their risk management plan
    - Use their management tools to address
- Don't use third party frameworks they do not understand
- You have limited time with people who need to quickly understand what you are doing – MAXIMIZE IT

Outreach in Coordination with Organization

- Build positive engagement by answering questions
- Always be available
- Find groups to present to
- Always constantly adapt
- Meet with as many top leaders as possible
- Take their advice and meet with whoever they say
- Continually tailor message

Structuring for Success

- You will not own all of the resources for security
- You will have a distributed team
- Focus on empowering the organization
- Focus on team members with good communication and analytics skills
- Don't focus on tool knowledge - you can teach tools, you can't teach instinct

Staffing Plans

- Rule #1 of Staffing plans - written by the Rolling Stones - you can’t always get what you want
  - Healthcare has very low margins
- Rule #2 of Staffing plans - You have to make the most of what you have
  - Leverage other organizations and teams to work together to most efficiently spend less money
  - Define and work toward shared common goals and tasks
- Rule #3 of staffing plans - You won’t get what you need (sorry Mick and Keith)
  - Experienced infosec people cost a lot. We have to train
  - We need to develop pipelines to keep the staff coming in

Staffing Plans

- Staffing is a function of:
  - Your risk assessments
  - Business impact analysis
  - Enterprise risk management
  - 96 hour survivability tool
  - Joint Commission responses and resources
  - Asset management and maintenance programs
- It is not something you can easily benchmark due to high varieties in healthcare delivery and EMRs, and is definitely something you cannot.

Conclusions

- You can structure for success
- It is achievable
- We are part of the business, now more than ever
- We need to be at the same table because of this
- The program needs to be structured around the organization, not the other way around

Thank you!

- Questions?
- Email: mitchell.parker@iuhealth.org
- Cell: 317 719 5531
- Desk: 317 963 5577

HEALTH