Your Privacy & Information Security Program: Preventative Care or Open Heart Surgery

Presented by:
Marti Arvin
Vice President Audit Strategy, CynergisTek

Agenda

- Preventative Medicine is good for you
- What you need to be prepared for and why
- Creating convincing arguments for more privacy and information security resources
- Questions

Preventative Medicine is Good for You
Life lessons applied to privacy and security programs

• How many of you have heard the following quotes or sayings?
  – An ounce of prevention is worth a pound of cure  
    Ben Franklin
  – An apple a day keeps the doctor away
  – Penny wise, pound foolish
  – Failing to plan is planning to fail  
    Alan Lakein
  – Treatment without prevention is simply unsustainable  
    Bill Gates

We all know this but . . .

• It is still difficult at convince your governing body a good preventative strategy is important
• What can you do to help them put the risk in context?
• What are the resources that can help you, they are not just in health care.

Helpful tools to convince your leadership

1. Use the recent Ponemon study
2. Benchmark with colleagues
3. Find out what the OCR is focusing on
Ponemon study

- Average cost per record of a data breach is $221
- Average cost per record in healthcare is $402
- Total average cost for breach paid by organizations increased from $6.53 million in 2015 to $7.01 million in 2016
- About 2/3 of the cost is in indirect costs

Responding to data breach takes you away from operations

- What is the impact on your program’s daily operations?
- What are you spending on responding that would have been better spent on prevention?

What you need to prepare for and why
Preventative care prescriptions

- Know your business associates
- Be prepared for the inevitable breach incident
- Be prepared for an OCR audit or investigation

Preventative prescription #1

- Know who your business associates are
- Know whether you have agreements with them
- Know if your agreements have been updated
- Know something about their processes

Preventative prescription #2

Take the pulse of your business associate, how healthy are they?

- Did you ask about their risk assessment process before initiating an agreement with them?
  - Do you do this on an ongoing basis?
Preventative prescription # 3

Be prepared for the inevitable breach incident

The average cost for mitigating a data breach is over $400 per record

Ponemon 2016 Cost of Data Breach Study: United States

OCR website - 25% of the complaints from Hawaii are investigated

Preventative prescription # 3

- Are you looking at your system to see if there is inappropriate activity
  - Two recent OCR resolutions agreements related to failure to assess user accesses

Preventative prescription # 3

- How do you prepare to respond when you find something
- Have you identified
  - Who will be involved?
  - Who will decide if notification is necessary?
Preventative prescription # 3

- Do you have agreements in place for potentially needed vendors?
  - Breach response services
  - Forensic services
- What would a significant settlement mean to the health of your organization?

Preventative prescription # 3 cont.

OCR is well in to Phase II of its audit program

While you might not have been selected for a desk audit you could be selected for a more extensive onsite audit

Is selected for an audit are you prepared?

- OCR has set specific timelines
  - Covered entities will not get “credit” for documents produced after the deadline
- Lack of comprehensive risk assessments and ongoing risk management has been a key findings
  - Phase I of the audits
  - A number of the resolution agreements
Creating convincing arguments for more privacy and information security resources

Convincing senior leaders

- Everything I have already said
- Because of breach notification requirements you must tell on yourself.
  - You cannot hide anymore
- The argument that your organization did not have sufficient resources to fix an issue is not good enough

Convincing senior leaders

- The fines and penalties will likely be in seven figures
- If not seven figures, still an amount impactful to the organization’s bottom line
**Convincing senior leaders**

- What the organization will send on
  - Legal fees
  - Consultants
  - Other outside assistance
  - Internal resources pulled away from their normal job duties
    - Other business processes might suffer.
- None of the above expenditures go to providing patient care or fixing the problem

**And if that does not convince them**

- Here is what OCR will be doing!!!

**And if that still does not convince them**

- Here is what the attorneys and consultants will be doing
And if that still does not convince them

- Here is what they will feel like.

Questions

Marti Arvin
Marti.arvin@cynergistek.com
512.405.8550 x7051