Meaningful Use & IT Security Review

Presented by:
Jonathan Krasner
BEI
jonathan.krasner@beinetworks.com
703-731-8768
www.beihealthcare.com

Meaningful Use Update

- MU lasts 5 years for each provider
- MU is divided into 3 stages
- 2014 should be Stage 2 MU
- Switching between stages for physician offices is hard:
  - You need new EHR software
  - You will have to comply with new core & menu measures
  - Your staff will need additional training
  - Your office may need new workflows

Meaningful Use 2014

- Providers must demonstrate MU for 3 months
- Three months must be a calendar quarter
- You can be in Stage 1 or Stage 2
- These & other program changes were made back in 2012

EHR – Stage 2 Compliance

To be Stage 2 compliant an EHR must:

- Develop new software
- Pass Stage 2 certification testing
- Develop documentation and support for end users
- Release the software to clients for deployment

Houston, we have a problem

- As of March 2014, only a handful of physicians & hospitals had submitted for MU Stage 2
- Very few vendors had their software certified
- A testing lab left the program
- The outlook for successful Stage 2 attestation by more than a handful of providers was bleak

So, what is happening?

On May 20, to adjust for these problems, CMS/ONC announced a rule:

- If you do not have a certified stage 2 EHR, you can attest in Stage 1 for 90 days in 2014
- If you have a deployed stage 2 EHR, you can attest to stage 2 for 90 days in 2014
- If you have a stage 2 EHR, but cannot deploy, you can attest to stage 1 in 2014
- What happens in 2015 is not determined as of today, but stage 2 will happen some way in 2015
- The rule will be final at the end of the summer, after comments have been received
- The currently proposed rule may differ slightly from the final rule

What should you do?

Recommendation:

- Consult with your EHR vendor; where are they in the certification process?
- If you have a hosted EHR, you may be in Stage 2 and not know it – ask your vendor
- Determine if you will be Stage 1 or Stage 2 this year and develop a plan for attestation
- Plan for moving to Stage 2 for sure in 2015

IT Security & HIPAA

IT Security is like getting a physical

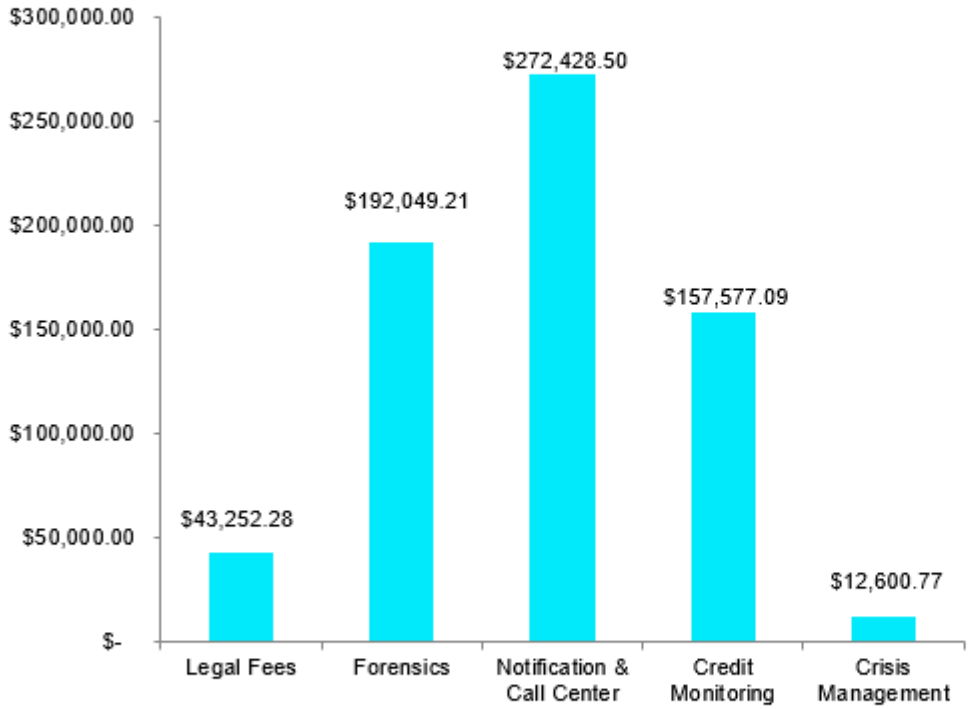
- No one wants to pay for it
- No one wants it
- Everyone needs it

IT security is a big deal -- even for you

- It is in the news every day
- You have heard about Target, NY Times, Heartbleed, etc
- You don't hear about what happens to small business -- but we see it

COSTS RELATED TO CYBER INCIDENTS

Average Cost of First Party Expenses



* ACE Data, Reflects Average Incurred Costs Across Paid Claims

Every Breach Response is Unique

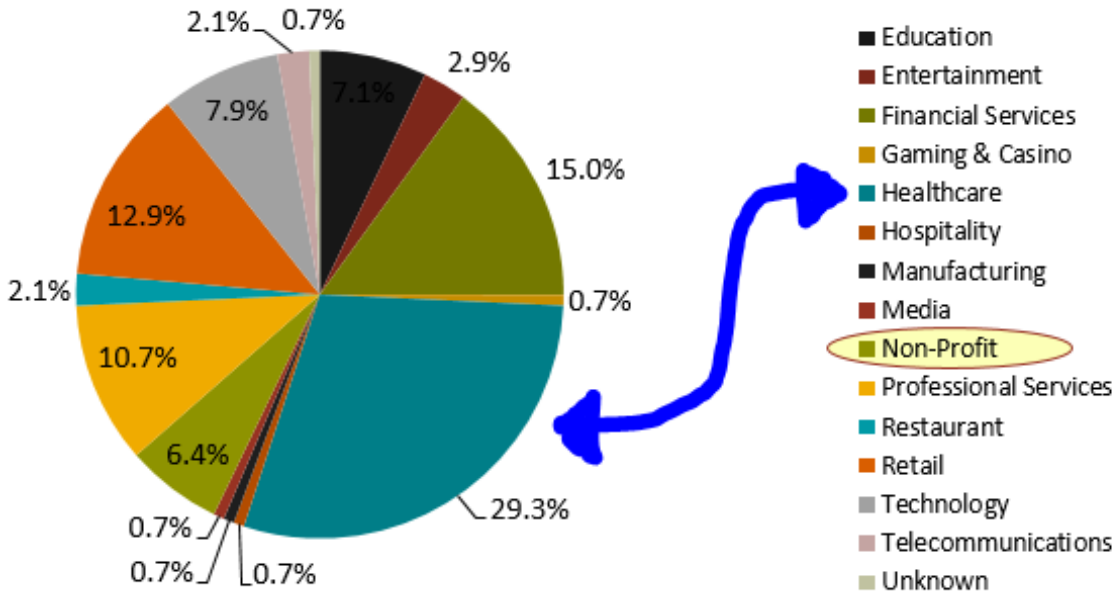
Cost Range of Each Service

- Legal Fees:
  Under $5,000 up to about $250,000
- Forensics:
  About $10,000 to Seven Figures
- Notification & Call Center:
  Approximately $3 per Record
- Credit Monitoring:
  Payment per Enrollee or Restoration Service
- Minimal Crisis Management Costs

Objective: Limit Third Party Exposure

COSTS RELATED TO CYBER INCIDENTS

Claims by Business Sector

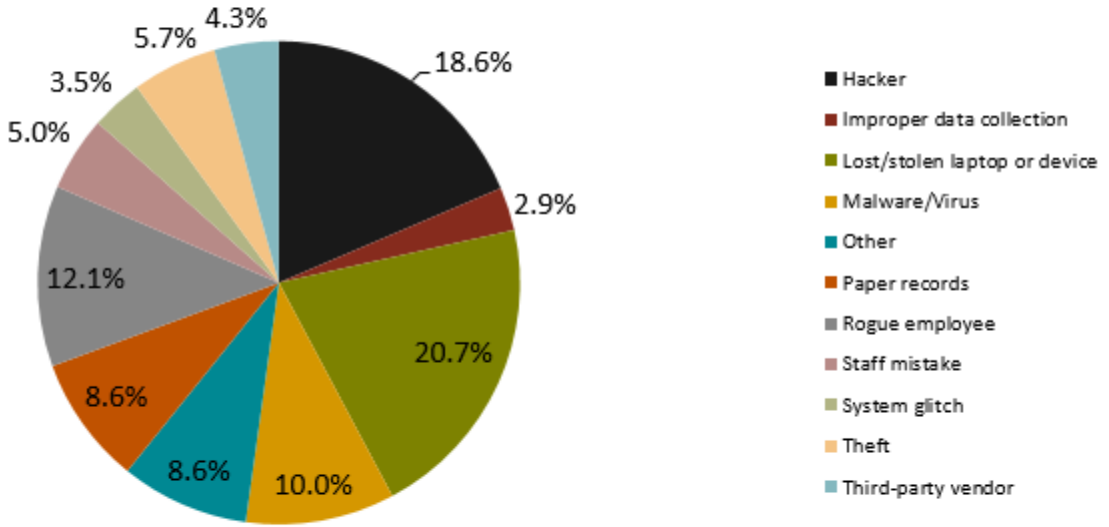


NetDiligence 2013 Cyber Claims Study

BARNES & THORNBURG LLP

COSTS RELATED TO CYBER INCIDENTS

Claims by Cause of Loss



NetDiligence 2013 Cyber Claims Study

BARNES & THORNBURG LLP

SPEAR PHISHING

"The vast majority of targeted computer attacks now start with a malicious e-mail sent to a company employee."

Nicole Perlroth, Critical Infrastructure Systems Seen As Vulnerable To Attack, New York Times, (Jan. 17, 2013)
http://bits.blogs.nytimes.com/2013/01/17/critical-infrastructure-systems-seen-as-vulnerable-to-attack/

BARNES & THORNBURG LLP

How is this related to HIPAA?

- HIPAA, in part, provides health care specific guidelines for IT security
- You must have a policies & procedures manual
- You must do a yearly risk assessment
- The vulnerabilities discussed on the previous slides are things you will try to avoid through your HIPAA policies and procedures

Given all this, what should you do?

- As mentioned previously, you need good security
- As mentioned previously, you want to minimize time, expense and disruption to employees

→ **You must focus on low cost, high value products & services**

BEI's list of IT security "things to do"

- Employee training
  - Information security training -- HIPAA specific
  - Fake phishing emails
  - Train doctors not to use insecure email or text to transmit PHI (use docbook from MCMS)
  - Instill a culture of security in the organization -- this culture comes from you!
- Develop an acceptable use policy
- Install privacy screens on monitors in common areas
- Encrypt your laptops
- Make sure antivirus is up to date
- Make sure firewall is up to date
- Use HIPAA compliant VPN

BEI's list of IT security "things to do" (2)

- Make sure you have Business Associates Agreements in place with all necessary vendors
- Make sure your IT vendor (if you use one) is HIPAA compliant
- Make sure operating systems are constantly updated
- Make sure wireless is WPA2 encrypted
- Install guest wireless
- Make sure strong passwords are required
- Make sure no one uses the same ID/passwords
- Change passwords at least semi-annually
- Don't allow post-it notes with passwords to be in plain view

BEI's list of IT security "things to do" (3)

- This list is relatively easy to implement
- These items need to be reviewed periodically for compliance
- Make sure to formalize these into HIPAA policies

Make sure this does not happen to you!