Healing Healthcare Security

Barry Caplin, VP & CISO, Fairview Health Services
bc@bjb.org
bcaplin1@fairview.org
@bcaplin
https://securityandcoffee.blogspot.com/
Secure360 May 16, 2017
The frightening new frontier for hackers: Medical records

Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data

Growing phishing & ransomware success hits healthcare

Healthcare Data Security Incidents Second Highest in 2016
Symantec found that healthcare data security incidents in 2016 were the second highest in the services sector, with breaches increasing 22 percent.

3 cyberthreats make up 81% of healthcare breaches, Verizon finds

Teaching hospitals at higher risk for data breaches, study finds

Healthcare providers' cybersecurity tools may need an upgrade

Healthcare challenges: Ransomware and the Internet of Things are the tip of the iceberg

2016 a banner year for EHR security breaches

Healthcare providers ‘cannot be complacent over data security’
Healthcare Breach Stats

- **2009**: 18 breaches, 135K records
- **2010**: 198 breaches, 5.5M records
- **2011**: 196 breaches, 13.2M records
- **2012**: 209 breaches, 2.8M records
- **2013**: 274 breaches, 7M records
- **2014**: 307 breaches, 12.7M records
- **2015**: 270 breaches, 113.3M records
- **2016**: 329 breaches, 16.5M records

Total: 1801 breaches, 171M+ records

- **Anthem**: Second Largest Health Insurer in the United States: 80 Million Records Compromised
- **Premera Blue Cross**: Medical Insurance Company: Over 11 Million Records Compromised Via Hacker Breach
- **TRICARE**: 4.9 Million Patient Records Stolen from Employee’s Car

Tweet along: #Sec360
WTF!

• What’s the problem Healthcare?

• Is Healthcare fundamentally bad at security?

Tweet along: #Sec360
@bcaplin
http://about.me/barrycaplin
securityandcoffee.blogspot.com

Tweet along: #Sec360
Not-for-profit established in 1906
Academic Health System since 1997
partnership with University of Minnesota
>22K employees
>2500 aligned physicians
Employed, faculty, independent
7 hospitals/medical centers
(>2,500 licensed beds)
40-plus primary care clinics
55-plus specialty clinics
54 senior housing locations
30-plus retail pharmacies

2015 volumes
6.6M outpatient encounters
1.55M clinic visits
67,682 inpatient admissions
78,157 surgeries
9,060 births
290 blood and marrow transplants
45 organ transplants
>$4 billion total revenue
Who is Fairview?

- Fairview Ridges Hospital
- Fairview Range Health Services
- Fairview Southdale Hospital
- Fairview Northland Medical Center
- Fairview Lakes Medical Center

Tweet along: #Sec360
Healthcare Pressures

- Healthcare delivery is expensive
  - Reimbursements, therefore margins, are low

- Not-for-profit – nearly 2/3s of hospitals

- Healthcare workers need instantaneous, unfettered access…
  - And must spew data everywhere, now…
    - Or someone could die!

- Med Devices

- M & A
• HIPAA – Health Insurance Portability and Accountability Act
  • Focused on portability – mandated use of EHR
  • Privacy and Security were add-on’s
  • Security Rule finalized in 2003 (Privacy in 2002)
    • Focus on confidentiality of PHI (Protected Health Information)
    • Fines for data breaches, violations
• Fines were initially small
• HITECH Act changed that (2009)
  • Health Information Technology for Economic and Clinical Health
Regulatory

Small revenue margins + high fines
= not much extra for IT or security
= focus on PHI data breach only
User Population

• Clinicians – Nurses, Doctors, Specialists, “-ologists”, Researchers, Professors

• All are:
  • Very smart
  • Very busy
  • Will find a way

• We need them to use their brain-cycles to heal, not to work around security controls

• Must provide controls that complement workflows
  • “wasted” time could be a patient safety issue
The Value of Your Data

$50 > $1

Medical Record  Social Security Number

The street cost of a stolen medical record is $50 compared to $1 for a stolen Social Security number.

Stolen medical records available for sale from $0.03 per record

Black market medical record prices drop to under $10, criminals switch to ransomware

The black market value of stolen medical records dropped dramatically this year.

It’s a sellers’ market for personally identifiable data on the “dark web,” where stolen information is anonymously bought and sold. Like all savvy businesses, hackers go where the money is; right now the hottest selling commodity is medical record data – going for as much as $60 per record.[1]

To put that in context, in its heyday, a single set of credit or debit card data could fetch anywhere from $20 to $125. But the market for card data has taken a nosedive. You can pick up a set for as low as $1 each—or $.22 for data sold in bundles.

While a Social Security number can be purchased on the dark Web for around $15, medical records fetch at least $60 per record because of the additional information, such as addresses, phone numbers and employment history. That in turn allows criminals to file fake tax returns.

Tweet along: #Sec360
Adversaries

• Then and Now

• It’s about… speed to market, low cost/high return

• So Healthcare is the obvious target!
• Or is it?????
Financial/Retail Data

- PII – Personally Identifiable Information
  - Often includes SSN, mother’s maiden name
- 1-to-many
  - You have many credit cards
- Easy to monetize
- Asymmetric theft model
  - The victim often doesn’t bear the cost
  - (I’m not minimizing ID Fraud which is a very real and very bad thing. But the vast majority here are simple account hijacking.)
Healthcare Data

• “Rich”, complete information
• Basically 1-to-1
  • You have many credit cards
  • You have 1 healthcare record (yes, it might be fragmented)

• >112M records breached in 2015; >171M through 2016 (via OCR Wall of Shame)

• Over 171M healthcare records breached actually means…

  Healthcare data on over
  >171M Americans breached!

• US population is >300M
  • So can we be done now???

Tweet along: #Sec360
Effects of a Healthcare data breach

• Your healthcare data is breached and
• You have surgery scheduled tomorrow… What happens?
• You have your surgery
• OTOH, if the hospital is hit by major ransomware?
  • What if you’re actually on the OR table???
Effects of a Healthcare data breach

• But... very hard to monetize
• Data can be used to commit financial crime
  • But it’s easier to just steal credit card numbers
• Medical Service fraud
  • Yes, but you have to show up
  • This can be a very nasty problem – the fraudster pollutes the victim’s medical record
  • And no one needs to steal your medical data to do this
• Drugs!
  • Real, but you have to show up
  • Data theft is too complex for most of the drug-seekers; volume is too low for the big players
  • And no one needs to steal your medical data to do this
Let’s Review

• Healthcare data is the most valuable data
• Healthcare has limited funds for security
• Focus on PHI data breach

• Professional thieves
• It’s about… speed to market, low cost/high return

• So Healthcare is the obvious target!
• Or is it?????
What’s Worse?

- Credit card theft is annoying
  - It’s like retail “shrinkage”
  - Yes, it does cost us all
- Real ID Fraud is very bad for the victim but rates are low
- Medical ID Fraud can be committed without theft of your medical record
- Remember the OPM breach???
  - Is this the most significant breach of PII ever?
- Intellectual Property
  - IP theft may have even greater negative impact to our economy
  - And what about theft of military secrets?
Reality

• If healthcare data is the most valuable, and...
• Healthcare orgs have weak security, and...
• Financial orgs have great security, then...

• Why did the bad people hit the financial/retail industry first?
  • Footprint? Opportunity?
  • Ease of Monetization?
  • Volume?
Reality

- Why are they hitting healthcare now?
  - Financial/Retail hardened their defenses?
  - Financial/Retail no longer interesting?
  - Monetization? – still hard
  - Volume? – fewer total records to get

Tweet along: #Sec360
Sidebar Rant – The Real Problem

• Is the problem that PII gets breached?
• Or…
• That it’s too easy to commit ID fraud or other crimes with the data?

• Can we make it harder to:
  • Get services
  • Open accounts
  • Masquerade

… with other’s information???

Tweet along: #Sec360
Did HIPAA Help?

• Initially… Yes!
• Woke healthcare up
  • But the focus on Confidentiality is the problem
  • (yes, I know there’s more to it, but look at the CMS Wall of Shame)
• The fines are material, but healthcare still has no excess funds!
  • Kick ‘em when they’re down?
• So, no, HIPAA doesn’t help
Gimme a “C”

- Do Regulations help?
  - Initially… Yes! – but they must keep up with the times
- Security can’t be
  - A point solution
  - About one data type – PHI, CC data, FTI, etc.
  - Just about Confidentiality
- Winter is coming!
  - Well, really it’s spring!
  - We’re already thinking about Availability
    - Can you spell DDoS?
    - Can you spell Brickerbot?

Beyond HIPAA

While meeting HIPAA compliance requirements doesn’t necessarily equal the kind of robust security efforts needed to effectively safeguard data - including data that goes beyond patients' protected health information - OCR's recent enforcement ramp-up likely will help nudge security laggards out of their complacency.

But it's also important to remember that the OCR enforcement actions we're seeing have been in the works for years. Looking ahead, will OCR be spending less time investigating major breaches that get reported now? Let's hope not.

What about data Integrity?

• What if rather than decrypting our data for some bitcoin…
  • It was fix our slightly altered data for a “small consulting fee”?
  • Now that’s scary!

Tweet along: #Sec360
Solution #1

• Play in the same sandbox
• The alphabet soup of regulations has got to go
• We need a single security framework and standard that will work across all areas of critical infrastructure?
  • Sound familiar…?

• NIST CSF – CyberSecurity Framework
  • History
  • Yes, I realize that this is very US-centric
  • Think globally, act locally – I can’t be responsible for all the world’s problems!
Solution #1 – NIST CSF

- It maps to everything
- Already directed at every critical infrastructure industry vertical
- Can easily apply a maturity model
- 800-53 provides the detailed standard
Solution #2

• Many organizations still need an “incentive”

• Are fines useful?
  • Potentially

• How about rather than fine organizations, force them instead to put an equivalent amount of funding into an enterprise security program!

• Perhaps some fine members of the vendor community can offer holistic security services?
  • Maybe not
Regulations

• Are they necessary?

• Why can’t we solve these things ourselves?
What about 3rd party solutions and med devices?

- Can’t live with ‘em, can’t live without ‘em.
- The same principles stand for these providers
  - They must be held to the same high standard
  - Vulnerabilities or other issues that can weaken their customers’ security posture must be fixed
  - All software must be patchable
    - Even better – use solid, secure software engineering principles!
The Bottom Line

Point solutions and regulatory compliance will never replace a holistic enterprise security program based upon a solid framework

Tweet along: #Sec360
Barry Caplin
Fairview Health Services
bcaplin1@fairview.org
bc@bjb.org
@bcaplin
securityandcoffee.blogspot.com