Hackers vs Your Organization
Prevent cyberattack from crippling your operations

January 27, 2017
Sathishkumar Gopalaswamy
Co-founder/Cyber Security Consultant, Zecuris
Two types of Companies

- One that is Hacked
- One that will be Hacked
“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

- Robert Mueller, FBI Director, 2012 RSA conference in San Francisco
Objective

- Overview of Cyber security Threats
- Present unique Security challenges
- Highlights from the Office for Civil Rights
- Security risks - Game changers in M&As
Why Cyber Awareness for Financial Executives

- Cyber-attacks are increasing every day
- Not only an IT problem
- High financial impacts that could shut down a business
Healthcare Cyber Security | Key Statistics

63% (YOY increase in Healthcare Breaches*)

89% (Healthcare org had one data breach#)

$6.2B (Estimated cost of breach#)

6% (Security spend % of IT spend in Healthcare~)

*Trapx report, #Ponemon 2016 report, ~ HIMSS

Healthcare industry more attacked than others. High cost impacts
Why Are Hackers After Patient Records?

- Patient Health Information (PHI) includes fundamental, unchanging facts about a patient
- In dark web,
  - Stolen cards $1-$3, SSN $15
  - Healthcare records $60 each
- Once compromised, one can own a person

Healthcare data most lucrative data of all
Why is Healthcare a Prime Target?

- Industry traditionally behind in technology
- Healthcare spends less on cybersecurity than other sectors
  - Unable to attract top talent
  - Not keeping pace with new technology

Barrier to entry. Low.
Patient Data is More Vulnerable Today

- More Mobile, More Accessible, More Connected
- Proliferation of new technology in healthcare, exploding
- Patient data is everywhere

Increasing entry points for Cyber threats
More Mobile, More Accessible
(More Entry Points)

Healthcare Industry
(Low Barriers to enter)

Patient Records
(Highly Lucrative)
What are the Impacts?

- Financial Impact
  - Penalties from OCR
  - Post-breach Costs
  - Lawsuits
  - Ransomware
- Operational Impact
- Reputational Impact
Recent HIPAA OCR Penalties and Enforcements

- Advocate Health, 4M Patients, $5.55M
- Univ. of Miss. Medical Center, 10K Patients, $2.75M
- Oregon Health & Science University, 7K Patients, $2.7M
- 12-Physician Pediatric & Adult Dermatology Practice, $150K
- 5-Physician Cardiology Group, $100K
Post Breach Costs

@ $200-400 / Hour

Forensics

$355 Per Record #

Breach Notification

Call Center

Credit Monitoring

Business Interruptions

@ 10$ / Record

Legal Guidance

@ $200-400 / Hour

#Ponemon 2016 report
Post Breach Costs - Do your Math

- Post breach cost for an organization with just 2000 records:
  - No of records: 2000
  - Cost per record: $355
  - Total breach costs: $710K

- Legal
- Forensics
- Breach notification
- Credit Monitoring
- Call Center
- Business Interruptions
Lawsuits

- 21st Century Oncology sued for $57M over data breach
- Majority of data breach class actions occur in Medical Industry

Ref: Bryan Cave - 2016 Data Breach Litigation Report
Ransomware

- More than 20 data loss incidents/day
- 4000 ransomware attacks/day in 2016
- 70% of victim businesses paid the ransom
- Hollywood Presbyterian Ransomware attack
  - All computers were inoperable; Patient handling went back to papers
- Video: https://zecuris.talentlms.com
What actions to take?

Top Five Actions for Financial Executives

- Get the basics of cyber hygiene
- Understand your current cyber risk status
- Identify potential cost impacts to your business
- Align Cybersecurity strategy with business strategy
- Get buy-in from management to invest in Cybersecurity

Be a Security Champion
Weak passwords are easily exploited

Use a passphrase.
For example, *VisitingLasVegas1985*

Each person needs own account
Phishing

▲ 88% of healthcare organizations had security incident involving phishing

- Risks
  - Patient data breach, ransomware
- Mitigations
  - User training, technical controls
Phishing – Email Wire Fraud Attacks

Request from CEO
Subject: Immediate Wire Transfer

To: Chief Financial Officer

⚠️ High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

Credit: FBI
Understand your Cyber Risk Profile
Customer Cyber Security Journey

Where do you see your organization in the cyber security maturity journey?

L1 Ad-hoc
- Simple Passwords
- No HIPAA Training
- Lack of / insufficient Network Security
- No Business Associate (BA) Agreement

Risks
- Data Breaches
- Reputational impacts
- Business Interruptions
- Penalties

Symptoms
- Shared user ids
- No awareness of Ransomware
- Critical Security Gaps

L2 Repeatable
- Anyone can access
- Security and Privacy Policies in place
- Some Monitoring

Risks
- Data Breaches
- Business Interruptions
- Patient Confidence loss
- Penalties

Symptoms
- Advanced Threat Protection
- Phishing Campaign
- Laptop/IoT Encryption
- BA Monitoring

L3 Defined
- 24/7 Security Monitoring
- Cyber Security Campaigns
- Incident Response Program

Risks
- Potential Data Loss
- Reputational impacts
- Reduced Penalties

Symptoms
- HIPAA Compliant
- Avoid Penalties
- Minimum interruptions

L4 Measured
- Peace of Mind
- Elevated Patient Experience
- Continuous Operations

Risks
- HIPAA Compliant
- Avoid Penalties
- Minimum interruptions

Symptoms
- Peace of Mind
- Elevated Patient Experience
- Continuous Operations

L5 Optimized
- Peace of Mind
- Elevated Patient Experience
- Continuous Operations

Risks
- HIPAA Compliant
- Avoid Penalties
- Minimum interruptions

Symptoms
- Peace of Mind
- Elevated Patient Experience
- Continuous Operations
Top 5 Risks

1. **Vulnerable Network Systems**
   - No monitoring to prevent threats
   - Laptops not secure, no encryption
   - Personally Identifiable Information to 17 sites w/o encryption
   - 100% risk of data breach

   **Potential Penalty:** $750K – 1.5M
   Examples: $1.5M, 2014 Columbia Presby. – Insecure Server.
   $750k, 2015 Cancer Care group, Stolen Laptop unencrypted

2. **Lack of Security Awareness**
   - Freeware and shareware accessed with embedded adware & malware
   - 90% risk of data breach
   - Potential Penalty: $700K
   Example: $750K penalty, 2015, University of Washington Medicine Phishing incident & lack of security training

3. **No prior Risk Assessments**
   - No previous risk assessments
   - 96% risk of data breach

4. **Limited Access Controls**
   - High exposure of patient records
   - Security functions not configured
   - 85% risk of data breach

5. **Gaps in Policies**
   - No continuity plans in place
   - Insufficient BAA language
   - 93% risk of data breach
   Example: $1.55 M penalty, 2016, North Memorial MN

Example: $2.7M penalty, 2016, Oregon Health & Science Univ.
Estimating Potential Cost Impacts

ROSI (Return on Security Investments)

- **Step #1** – All relevant costs of an incident & their probability
  - ROSI = (Monetary loss reduction – Cost of Investment) / Cost of Investment
  - Monetary Loss Reduction = Monetary loss per Risk * Probability of Occurrence

- **Step #2** – Level to which risk would decrease, after mitigation
  - ROSI = (Monetary loss reduction * mitigation ratio) – Cost of Investment / Cost of Investment
Estimating Potential Cost Impacts

Example ROSI calculation of a Breach of 10K Patients, $2.75M OCR Penalty:

- **Monetary Loss Per Risk:**
  - Penalties: $2.75M
  - Post Breach costs: $3.55M
  - Total: $6.25M

- **Probability of Occurrence:** 60%

- **Monetary Loss Reduction:** $3.75M

- **Risk Mitigation ratio:** 70%

- **Cost of Investment:** $1M

- **ROSI:** 163%

Due to Security investments
Presenting to Executive Management

- Break down the Cyber Risk to Board
  - Align Cyber security strategy with business strategy
  - Make it real - Take popular breaches and relate to it
Cyber Security – An M&A Hurdle

- Increase in Cyber attacks during an M&A process
  - To reduce the value of Acquired company
  - To gain access to Acquiring company

- Perform Cyber Due Diligence prior to M&A

- Risk and compliance obligations start immediately
Key Takeaways

- No one is immune. Cyber attacks are imminent
- Know your security posture, Crown jewels of data
- Align Cybersecurity strategy with Business strategy
- Increase Security investments
- Leverage MSSPs to address security gaps
- Be a security champion of your organization
Q & A