Hackers vs Your Organization
Prevent cyberattack from crippling your operations

February 24, 2017
Sathishkumar Gopalaswamy
Co-founder/Cyber Security Consultant, Zecuris

Adam Laughton
Attorney, Seyfarth Shaw LLP
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
Healthcare Data | Perfect target for Cyber hackers

More Mobile, More Accessible
(More Entry Points)

Healthcare Industry
(Low Barriers to enter)

Patient Records
(Highly Lucrative)
Privacy Reminder

- Reminder: Perfect security may still leave organizations vulnerable under the other side of HIPAA: privacy

- Security is focused on the technical aspect of protecting PHI; privacy focuses on operational aspects (policies, procedures, training)

- Our focus today will be on security, but a security plan alone is a half measure
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
Recent HIPAA OCR Penalties and Enforcements

- Hacking is not the only vulnerability or potential source of liability
- Office of Civil Rights is currently conducting audits of both privacy and security
- Audit Protocols are available online
- Audits have numerous potential consequences
Post Breach Costs

- Legal Guidance: $400-600 / Hour
- Forensics: $200-400 / Hour
- Breach Notification: $355 Per Record #
- Call Center: $10 / Record
- Credit Monitoring: $10 / Record
- Business Interruptions: $10 / Record

#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
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
Passwords

- Weak passwords are easily exploited
- Use a passphrase.
  For example, *VisitingLasVegas1985*
- Each person needs own account

63% of confirmed data breaches involved leveraging weak, default or stolen passwords
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?

<table>
<thead>
<tr>
<th>Security Maturity Level</th>
<th>L1 Ad-hoc</th>
<th>L2 Repeatable</th>
<th>L3 Defined</th>
<th>L4 Measured</th>
<th>L5 Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symptoms</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple Passwords</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No HIPAA Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of / insufficient Network Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Business Associate (BA) Agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Security Gaps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breaches</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational impacts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Interruptions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Breaches</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Interruptions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Confidence loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Potential Data Loss</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational impacts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduced Penalties</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>24/7 Security Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Security Campaigns</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Incident Response Program</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Threat Protection</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phishing Campaign</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Laptop/IoT Encryption</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BA Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HIPAA Compliant</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Avoid Penalties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Minimum interruptions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Peace of Mind</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Elevated Patient Experience</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Continuous Operations</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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. **Limited Access Controls**
   - High exposure of patient records
   - Security functions not configured
   - 85% risk of data breach

   **Example:** $3.3M penalty, 2014, New York Presby.

4. **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

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

   **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
  - \( \text{ROSI} = (\text{Monetary loss reduction} - \text{Cost of Investment}) / \text{Cost of Investment} \)
  - Monetary Loss Reduction = Monetary loss per Risk \* Probability of Occurrence

- Step #2 – Level to which risk would decrease, after mitigation
  - \( \text{ROSI} = (\text{Monetary loss reduction} \times \text{mitigation ratio}) - \text{Cost of Investment} / \text{Cost of Investment} \)
### 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
  - $6.25M\times60\%

- **Risk Mitigation ratio**
  - 70%

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

- **ROSI**
  - 163%
  - \[
  \frac{(3.75M\times70\%) \quad – \quad 1M}{1M}\]
How to Achieve HIPAA Compliance

- First step is always a gap or risk assessment
  - This is a compliance requirement in and of itself
- Appropriate policies and procedures
  - Tailored for the organization based on the gap/risk assessment
- Training
- Periodic checkups and updates
  - A stale gap or risk assessment is a false risk assessment
Cyber Insurance – Do you have it?

- Does your current CGL or other liability policy cover cyber risks?
  - SPOILER: Many don’t

- Cyber insurance relatively new product in the marketplace

- Insurers and underwriters want to see your risk assessment and existing compliance plan
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

Perform Cyber Due Diligence
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

Link Security to Business Strategy
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