Actionable Cybersecurity Insights

Fernando Martinez PhD CISSP CISA CISM
Texas Hospital Association Chief Digital Officer
President/CEO Texas Hospital Association Foundation
Learning Objectives

- gain an understanding of the anatomy of a cyber exploit
- explain administrative concepts including risk analysis, controls and closed-loop processes in the context of managing cyber threats and
- define and explain how to implement administrative countermeasures for cyber threats
Healthcare is a target
<table>
<thead>
<tr>
<th>Company Name</th>
<th>State</th>
<th>Type</th>
<th>NPI</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port City Operating Company doing business as St. Joseph's Medical Center</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>4984</td>
<td>08/31/2016</td>
</tr>
<tr>
<td>Carpenters Benefit Funds of Philadelphia</td>
<td>PA</td>
<td>Health Plan</td>
<td>20015</td>
<td>08/31/2016</td>
</tr>
<tr>
<td>Hopebridge</td>
<td>IN</td>
<td>Healthcare Provider</td>
<td>1411</td>
<td>08/31/2016</td>
</tr>
<tr>
<td>United Methodist Homes</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>843</td>
<td>08/31/2016</td>
</tr>
<tr>
<td>David G. Simon, DMD, PA, dba Simon Orthodontics</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>15129</td>
<td>08/31/2016</td>
</tr>
<tr>
<td>Greig H. Hirata M.D. Inc, dba Fetal Diagnostic Institute of the Pacific</td>
<td>HI</td>
<td>Healthcare Provider</td>
<td>40800</td>
<td>08/30/2016</td>
</tr>
<tr>
<td>South Alamo Medical Group PA</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>2180</td>
<td>08/30/2016</td>
</tr>
<tr>
<td>First coast pediatric surgery and wound</td>
<td>FL</td>
<td>Business Associate</td>
<td>500</td>
<td>08/27/2016</td>
</tr>
<tr>
<td>Family Medical Group Northeast PC</td>
<td>OR</td>
<td>Healthcare Provider</td>
<td>2077</td>
<td>08/22/2016</td>
</tr>
<tr>
<td>Legacy Health</td>
<td>OR</td>
<td>Healthcare Provider</td>
<td>38000</td>
<td>08/20/2016</td>
</tr>
<tr>
<td>Acadiana Computer Systems, Inc.</td>
<td>LA</td>
<td>Business Associate</td>
<td>31151</td>
<td>08/17/2016</td>
</tr>
<tr>
<td>Chapman &amp; Chapman, Inc.</td>
<td>OH</td>
<td>Business Associate</td>
<td>2032</td>
<td>08/17/2016</td>
</tr>
<tr>
<td>Monroe Operations, LLC dba Newport Academy and Center for Families</td>
<td>TN</td>
<td>Healthcare Provider</td>
<td>1165</td>
<td>08/17/2016</td>
</tr>
<tr>
<td>Authentic Recovery Center, LLC</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1790</td>
<td>08/17/2016</td>
</tr>
<tr>
<td>Wardell Orthopaedics, P.C.</td>
<td>VA</td>
<td>Healthcare Provider</td>
<td>552</td>
<td>08/16/2016</td>
</tr>
<tr>
<td>University Medical Center Physicians</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>18500</td>
<td>08/16/2016</td>
</tr>
<tr>
<td>AU Medical Center, INC.</td>
<td>GA</td>
<td>Healthcare Provider</td>
<td>417000</td>
<td>08/16/2016</td>
</tr>
<tr>
<td>Gordon Schlaniztn New Vision Institute</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1130</td>
<td>08/10/2016</td>
</tr>
<tr>
<td>Wels Pharmacy Network</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>10000</td>
<td>08/10/2016</td>
</tr>
<tr>
<td>Anne Arundel Dermatology, P.A.</td>
<td>MD</td>
<td>Healthcare Provider</td>
<td>1210</td>
<td>08/09/2016</td>
</tr>
<tr>
<td>InterAct of Michigan, Inc.</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>1290</td>
<td>08/07/2016</td>
</tr>
<tr>
<td>CoreLink Administrative Solutions, LLC</td>
<td>ND</td>
<td>Business Associate</td>
<td>1813</td>
<td>08/06/2016</td>
</tr>
<tr>
<td>Central Colorado Dermatology, PC</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>4065</td>
<td>08/03/2016</td>
</tr>
<tr>
<td>CoreSource, Inc.</td>
<td>IL</td>
<td>Business Associate</td>
<td>769</td>
<td>08/03/2016</td>
</tr>
<tr>
<td>Don White, RNI, DC, PC dba Canyon Rd Chiropractic and Massage</td>
<td>OR</td>
<td>Healthcare Provider</td>
<td>2800</td>
<td>08/03/2016</td>
</tr>
<tr>
<td>Kaiser Foundation Health Plan of Colorado</td>
<td>CO</td>
<td>Health Plan</td>
<td>960</td>
<td>08/03/2016</td>
</tr>
</tbody>
</table>

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
How are Cyber Threats Carried Out?
How are Cyber Threats Carried Out?

- **INTRUSION** (failed control)
  
  Equifax breach

- **DECEPTION** (social engineering)
  
  USERS are the target

- phishing, spear-phishing, compromised credentials
Why Are Organizations Vulnerable?
(and what can be done to prepare?)
Making sense of the ENVIRONMENT

• Know your landscape
  • Security and data sprawl is a challenge
  • Too many vendors to manage
  • Complex security and data architecture models

• Security architecture and approach
  • Are you susceptible to an outside attack
  • Are effective controls in place
  • Can any internal systems be breached (are they already?)
Making sense of TERMINOLOGY

- Ineffective CONTROLS
  - Single-factor authentication
    - Versus two
    - Vulnerability scanning and a patch management program not a closed-loop process
- Deficient risk awareness
5 Crucial Questions

- How are we stopping phishing attempts?
- How are privileged accounts handled?
  - Doctrine of least privilege
- How are software patches applied?
- Are our third-party vendors secure?
- How do we control access?
  - Dual or multi-factor authentication

https://www.healthcareitnews.com/news/hows-your-cybersecurity-posture-answer-these-5-crucial-security-questions
Related and Misunderstood

RISK ANALYSIS

Over the past 10 years 88% of the 42 organizations that have entered into monetary settlements or civil money penalties related to ePHI failed to conduct a sufficient risk analysis.

Jon Moore, Chief Risk Officer, Clearwater Compliance
What is Risk Analysis?

In April of this year OCR issues guidance entitled:

“Risk Analyses vs. Gap Analyses – What is the difference?”

OCR explains that Risk Analysis IS NOT

- Technical testing or
- Compliance gap assessment

The three E’s

- Evaluate
  - Appropriate risk analysis
- Educate
  - Total workforce/user base
- Exercise
  - Table top exercises – simulated cyber incidents allow for exploring the difficult questions under controlled conditions
Risk Analysis documentation must include an inventory of all information assets used to create, maintain, retrieve, or transmit ePHI and the threats, vulnerabilities, likelihood, impacts and controls associated with each.
Controls

- Address barriers to adopting two-factor authentication
- Demand closed-loop, effective program for vulnerability and patch management
- Leverage purchased services versus “best effort”
Training

- Ongoing workforce education. Build a culture of awareness.
- Implement an effective simulated phishing email training program which includes evaluating workforce reaction (incident response) to identified phishing emails
- Table-top exercises, built around simulated cyber incidents where your leaders and team can run through the difficult questions under controlled conditions.
Questions or Comments?

Fernando Martinez PhD CISSP CISA CISM
fmartinez@tha.org

THANK YOU