Understanding Cybersecurity Risks in Healthcare

Presented by:
Marti Arvin
VP Audit Strategy | CynergisTek, Inc.

Today’s Presenter

• Vice President of Audit Strategies, CynergisTek, Inc.

• Subject matter expert on healthcare compliance programs with a focus on the HIPAA Privacy, Security and Breach Notification Rules

• Experienced in developing, implementing and evaluating compliance programs for large and small organizations

• Holds the CHC-F, CCEP-F, CHPC and CHRC certifications

Marti Arvin
CynergisTek, Inc.
The Threat Changes

The Cyber Threat Spectrum

- Hacktivism
- Crime
- Insiders
- Espionage
- Terrorism
- Warfare
Evolving Healthcare Threat Landscape

From lost/stolen devices to hacking

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Incident</th>
<th>Value</th>
<th>Year</th>
<th>Company</th>
<th>Incident</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-11</td>
<td>BCBS Tennessee</td>
<td>1.02M Stolen Hard Drives</td>
<td></td>
<td>2012</td>
<td>TRICARE</td>
<td>4.9M Lost Backups</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NYC Health &amp; Hospitals</td>
<td>1.7M Stolen Backup Tapes</td>
<td></td>
<td></td>
<td>Advocate Medical</td>
<td>4.03M Computer Theft</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Utah Dept. of Health</td>
<td>780K Hacking</td>
<td></td>
<td>2014</td>
<td>Community Health</td>
<td>4.5M Hacking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Boston Children</td>
<td>Hacktivism</td>
<td></td>
<td></td>
<td></td>
<td>Anonymous</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>Premera BCBS</td>
<td>11M Hacking</td>
<td></td>
<td>2015</td>
<td>CareFirst</td>
<td>1.1M Hacking</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AvMed</td>
<td>1.2M Stolen Laptops</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Health Net</td>
<td>1.9M Lost Hard Drives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Nemours</td>
<td>1.6M Lost Backups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Boston Children H</td>
<td>Hacktivism</td>
<td></td>
<td></td>
<td></td>
<td>Anonymous</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Premera BCBS</td>
<td>11M Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anthem BCBS</td>
<td>80M Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Montana Public</td>
<td>Health</td>
<td>1.3M Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UCLA</td>
<td>4.5M Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Westchester Health</td>
<td>Hacked</td>
<td></td>
<td></td>
<td></td>
<td>Pro ISIS Group</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Multiple Sources

Cybercrime as a Business

- Cybercrime is expected to generate $600B in revenues in 2016
- Trends in cybercrime all make cyber-criminals more effective
  - Cybercrime-as-a-service model gives less technically-savvy criminals access
  - Dark web marketplaces make “monetizing” stolen data as easy as buying on Amazon
  - Cybercriminals are adopting tactics previously only used by nation-state attackers
Dark Web Marketplace

A Bitcoin wallet, PGP for encrypted communication, and a TOR browser and you are in business...

Our Adversary is Committed

655,000 health records for sale on the dark web (June 28, 2016)

“Next time an ADVERSARY comes to you and offers you an opportunity to cover this up and make it go away for a small fee to prevent the leak, take the offer. There is a lot more to come.”

9 million plus more health records online (June 30, 2016)

Healthcare HL7 Interoperability Software Source Code, Signing Keys & Licensing Database for sale (July 12, 2016)

“There will likely be two buyers for this, someone with nefarious intentions or someone from a small country wanting to use it for business.”
The Stakes are Higher

- Cyber extortion
- Cyber espionage
- Hacktivism
- Targeted attacks
- Cyber terrorism
- APTs & malware

*Motivated, Persistent & Disruptive*

Cyber Espionage: Intelligence

Cyber espionage is being carried out by nation-state actors for political purposes

- Large breaches such as Anthem, Premera, Community Health Systems, UCLA are suspected cases of espionage
- A case example is the OPM intrusion presumed by a Chinese group that captured security clearance documents
- But...they are also targeting industrial control systems that control and manage critical infrastructure
Hacktivism: Causes

Attacking for a cause

- U.S. government databases were breached in 2013 by Edward Snowden who released hundreds of classified documents in an “act of conscience”
- GhostShell attacked several U.S. universities in 2015 leaking sensitive information
- Anonymous hacked Boston Children’s and Hurley Medical Center for ideological reasons
- Pro ISIS group hacks hospital website

Targeted Attacks (APT): Information

Typically nation-state attack groups

- “APTs are known for being highly sophisticated, using multiple vectors to attack a target network, and having unrelenting tenacity”
- Many attacks go undetected for considerable periods of time, estimated 280 days on average
- Phishing, zero day attacks, ransomware increased dramatically in 2016

“There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don’t know it.”

– Gartner Inc., 2012

Cyber Extortion: Money

- First appeared around 2005
- Two forms: Crypto ransomware (data) and Locker ransomware (system)
- Sophisticated attacks use:
  - New asymmetric keys for each infection
  - Industrial strength & private/public key encryption
  - Privacy enabling services like TOR and bitcoins for payments
- Indifferent to target, everyone is a target (home/business)
- Malvertising, spam email, downloaders/botnets & social engineering

The United States is the largest target worldwide by a huge margin.
SOCs worldwide report as much as a 10X increase in ransomware attacks from December to January with no abatement.

Healthcare as a Critical Infrastructure

“Looking specifically at healthcare breaches, the targeting of organizations relating to population welfare may be part of an intelligence-collection effort intended to support the aims of China’s 12th FYP, which launched in 2011.”

Source: CrowdStrike 2015 Global Threat Report.
Ubiquitous is the New Paradigm

- Smart phones
- IOT
- Social media
- POS systems
- Medical devices
- Removable media (USBs)
- SPAM & email
- Applications
- Smart TVs
- CCTV cameras
- Environmental systems
- Downloads
- Attachments
- Browsers
- Wearables
- Telehealth

Threats are introduced from all directions, simple compliance strategies will not suffice, an integrated set of controls is needed.

What are Vendors Doing with PHI?

“There you are, I was tracking you.”

- The taxi-hailing commuter platform Uber had two breaches in 2014 that weren’t reported until 2015, gaining the ire of the New York SAG.
- What they did:
  - First they allowed internal users access to riders’ PII and displayed it through a tracking system called “God View”.
  - Second they had a breach of their riders’ database that permitted a third party access to 50,000 riders’ PII on GitHub.
- The settlement requires Uber to employ encryption, better access controls and multi-factor authentication.
- Health Systems are partnering with Uber to help patients not miss appointments.
The Insider Threat

- 93% feel vulnerable to insider threats
- 59% worry about privileged users most
- Contractors/service providers next biggest concern
- 2010-2015 20% increase in ID/Med ID theft
- 37% feel user awareness training is failing
- Traditional audit methods are failing right and left

Short Term Demand Outpaces Supply

- Nearly half of all entities do not have a full-time CISO or information security manager
- Current estimates place shortage of CISOs at 1.5M
- Education & Training vehicles increasing, but time still a factor
- Short term reliance on external support is critical
Compliance is Not the Answer

- HHS Security & Privacy guidance does not fully address the important controls outlined in federal guidance.
- HHS guidance does not fully align with the NIST cybersecurity framework.

What We Can Do
Security Challenges

- Configuration Management
- Securing End Points
- Encryption of Data
- Prevention of Leakage
- Log Management
- Establishing Identity
- Monitoring System Activity
- Accounting for Access
- Ensuring Minimal Necessary
- Technical Testing
- Data Search/Control
- Asset Management

Solutions with Intelligence

- Technology that provides proactive heuristic protection
- Technology that incorporates artificial intelligence and machine learning
- Technology that protects while not inhibiting enterprise features and services
- Technology that takes a holistic approach
- Technology that creates a knowledge based picture
- Technology with healthcare intelligence
- Technology that requires limited administration to manage
- Technology that provides multiple options for implementation
Challenges Will Continue

- Shortfalls in application and system security
- Lack of an integrated plan for security
- Inexperience in security technology
- Inadequate security planning
- 2/3 budgeting less than 3% of the IT budget security
- Internal audit organizations lack IT audit training or tools
- Inadequate security expertise

Solutions That Strengthen Defenses

- **Improve the perimeter**: remote access connections, firewalls/UTM, IPS, web apps, sandboxing, SaaS & public/private clouds
- **Focus on malware detection**: secure email gateways and secure web gateways
- **Reinforce endpoint detection**: admin privileges, regular testing, anti-virus, anti-malware, host based IPS, include IoT devices
- **Automate audit/monitoring**: dedicated SOC, enhanced SIEM, behavioral analysis
- **Step up IR capabilities**: define process, train members, establish contacts, track & learn, share intelligence
- **Threat deception**: use technologies that deceive/divert, endpoints, applications, data, identity and infrastructure

With motivation, the right equipment, the right training and timely execution can help stop the threat.
Wrap Up

- The challenges are just getting more complex
- Manual processes are not adequate to even be minimally compliant
- Technologies should be chosen that offer the greatest impact with the least amount of administration
- Technological choices should fit within a strategic plan/security framework
- Organizations can expect to spend 6-10% of their IT budgets to meet minimal standards

Questions

Questions?

Marti Arvin
Marti.arvin@cynergistek.com
615-540-8071
@arvin_marti