2014 Outlook: Top 10 Security Concerns For Healthcare
Montana HIMSS Educational Conference & Tradeshow

Presented by:
Mac McMillan
FHIMSS, CISM
CEO, CynergisTek
Today’s Presenter

Mac McMillan
FHIMSS/CISM
CEO CynergisTek, Inc.

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- Chair, HIMSS P&S Steering Committee
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- Health Tech Industry Advisory Board
- Disruption Forum Advisory Board
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired
Insider Threats

• It is estimated that more than half of all security incidents involve staff.
• More than 70% of identity theft and fraud were committed by knowledgeable insiders – physicians, nurses, pharmacy techs, admissions, billing, etc.
• 2013 witnessed a 20% increase in medical identity theft.
• Traditional audit methods & manual auditing is completely inadequate.
• Behavior modeling, pattern analysis and anomaly detection is what works.
The headline read: 
“Yes, Terrorists could have hacked Dick Cheney’s heart.”

The Washington Post
October 21, 2013

In June 2013 the DHS tested 300 devices from 40 vendors, ALL failed. In response the FDA issued guidance for manufacturers and consumers addressing design, implementation and radio frequency considerations.
Better vendor management is required:

- Pre-contract due diligence
- Risk category
- Contract requirements
- Maintenance/Monitoring
- Breach notification
- Contract termination

Business Associates have been involved in more than 20% of breaches since 2009
Rising Malware Threat: A Maintenance & Administration Nightmare

- If you did not think malware was a threat, think again...
- 3.4 million BotNets identified
- Slightly less than half of all malware hosted in the United States
- 26% of malware delivered via HTML, one in less than 300 emails infected
- Malware analyzed last year was undetectable in 40% of all anti-virus engines tested
- As of April 2014 Microsoft no longer provides patches for WN XP and 2003 and WN 2000, NT, etc. are already EOL

Various: Symantec, IBM, Solutionary Annual Threat Reports
Mobile Device Security

Almost half of the global workforce uses smartphones and we’ll see 905M tablets by 2017. – Forrester, Feb. 2013

• Medical staff are turning to their mobile devices to communicate because it’s easier, faster, more efficient...but is it secure?
  – Sharing lab or test results
  – Locating another physician for a consult
  – Sharing images of wounds and radiology images
  – Updating attending staff on patient condition
  – Getting direction for treatment
  – Locating a specialist and collaborating with them
  – Transmitting trauma information or images to EDs
  – Prescribing or placing orders
Identity theft incidents are rising and becoming more costly.

- Insiders selling information to others
- Hackers exploiting systems
- Malware with directed payloads
- Phishing for the “big” ones

“Everyone in this room is a target”
Theft of Assets

15 devices stolen involving more than 500 records in Q1 of 2014

• First rule of security: No one is immune
  – Three desk tops, 4M patient records
  – Stolen laptop puts 4.24M patients at risk
  – Stolen laptops result in $2M in fines

“That’s a big number because its meant to drive home the point that unencrypted laptops and mobile devices pose significant risk to the security of patient information.”
Sue McAndrew, OCR

138% - the increase in records exposed in 2013
Theft accounted for 83% of large breaches
6-10% - the average shrinkage rate
Typical clinical asset inventories are off by 60%
Targeted Attacks

- Three most common attacks: spear phishing, Trojans & Malvertising.
- Most organizations can’t detect or address these threats effectively.
- An advanced incident response capability is required.
- Results in losses of time, dollars, downtime, reputation, breaches, litigation, etc.

“Targeted Attacks

No increase in budget for defenses
Sophistication of attack hardest...
Organizations suffering a targeted...

“‘Our study confirms that organizations are facing a growing flood of increasingly malicious data breaches, and they don’t have the tools, staff or resources to discover and resolve them.’”

Larry Ponemon

“I feel like I am a targeted class, and I want to know what this institution is doing about it!”
Anonymous Doctor, FAHC
Inadequate Resources

- The average maturity rating reported was a 4.35 on a scale of 1-7.
- Missing critical technologies to fight today’s threats.
- More than half spend less than 3% of their IT budget on protecting data.
- Almost half have a full time CISO or information security manager.

OCR's investigation found that Concentra had recognized in its risk assessments that the lack of encryption created risks. They taken steps to begin encryption, but efforts were incomplete and inadequate over time leaving assets vulnerable.

The shift is happening, but will it be soon enough?
Regulations

- OCRs permanent audit program will resume in FY 2015 with new capabilities.
- Improvements and automation in reporting and handling complaints.
- Meaningful Use audits are evolving in scope and impact.
- The FTCs enforcement has been upheld by the courts.
- Business will present new risks for covered entities.

Covered entities and business associates must understand that security is their obligation.
Sue McAndrew, OCR

When organizations tell consumers they will protect their personal information, the FTC can and will take law enforcement action to ensure they live up these promises.

When asked how the 2015 audits would differ from the pilot, Leon Rodriguez responded, “one focus in the audits will be on risk analysis.”
Enforcement in 2014

HHS                  Office
                  for Civil Rights

HHS                  Office
                  of the Inspector
                  General

Federal Trade
Commission

States Attorney
General

Covered
Entities
& Business
Associates

Civil Law Suits

HHS                  Center for
                  Medicaid/Medicare
                  Services
Breaches & Incidents

The real cost of privacy and security incidents is lost productivity, fewer dollars for positive initiatives and negative reputational impacts.
Wrap Up
Thank You

Questions

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555
www.cynergistek.com