Top 10 Security Challenges for Healthcare
HCCA Mid-Central Regional Conference

Presented by:
Mac McMillan
FHIMSS/CISM
CEO, CynergisTek

Today’s Presenter

• Co-founder & CEO CynergisTek, Inc.
• Chair, HIMSS P&S Policy Task Force
• CHIME, AEHIS Advisory Board
• Healthcare Most Wired Advisory Board
• 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

Mac McMillan
FHIMSS/CISM
CEO CynergisTek, Inc.
Sun Tzu & Cybercrime

• “If you know the enemy, and know yourself, then you may not fear the results of a hundred battles. If you know yourself but not the enemy, for every victory gained you will suffer a defeat.”  Sun Tzu

• He went on to say, “If you know neither the enemy or yourself you will suffer a hundred defeats.”

• A hundred of anything in a Chinese Proverb is very good or very bad...

Cybercriminals Today

• 12 y/o learning computers in middle school
• 14 y/o home schooled girl tired of social events
• 15 y/o in New Zealand just joined a defacement group
• 16 y/o in Tokyo learning programming in high school
• 19 y/o in college putting course work to work
• 20 y/o fast food employee that is bored
• 22 y/o in Mali working in a carding ring
• 24 y/o black hat trying to hack whoever he can
• 25 y/o soldier in East European country
• 26 y/o contractor deployed over seas
• 28 y/o in Oregon who believes in hacktivism
• 30 y/o white hat who has a black hat background
• 32 y/o researcher who finds vulnerabilities in systems
• 35 y/o employee who sees a target of opportunity
• 37 y/o rouge intelligence officer
• 39 y/o disgruntled admin passed over
• 41 y/o private investigator
• 44 y/o malware author paid per compromised host
• 49 y/o pharmacist in midlife crisis
• 55 y/o nurse with a drug problem
2014 Cyber Incidents

- 4M medical records maintained on four workstations
- Physician loses laptop with psychiatric patients records
- Neurologic institute accidentally emails 10,000 patient records to 200 patients
- Phishing/hacking nets nearly $3M from six healthcare entities
- University reports laptop with patient information stolen out of a student’s car
- Vendor sells hospital's X-rays (films) to third party
- Resident loses track of USB with over 500 orthopedic patients information
- Portable electronic device with patient data stolen from hospital
- Physician has laptop stolen from vacation home
- 2200 physicians victims of ID theft/tax fraud
- Stolen laptop from nurse's home with patient data
- Printers returned to leasing company compromise thousands of patient records
- Health System reports third stolen laptop with 13,000 patient records
- 400 hospitals billings delayed as clearinghouse hit with ransomware

The Emergent Threat

Black Hat 2014

- Snatching passwords w/ Google Glass
- Screen scraping VDI anonymously
- Compromising AD through Kerberos
- Remote attacks against cars
- Memory scraping for credit cards
- Compromising USB controller chips
- Cellular compromise through control code
- Free cloud botnets for malware
- Mobile device compromise through MDM flaws
- Cryptographic flaws and a Rosetta Stone
**Black Market Driven**

- Darknets will be more active, participants will be vetted, cryptocurrencies will be used, greater anonymity in malware, more encryption in communications and transactions
- Black markets will help attackers outpace defenders
- Hyperconnectivity will create greater opportunity for incidents
- Exploitation of social networks and mobile devices will grow
- More hacking for hire, as-a-service, and brokering

*Rand National Security Research Division*

---

**Increased Reliance**

Today’s CISO has to understand the needs of the business as well as have the security expertise to match its demands of both the threat and the business. Simply understanding HIPAA is not enough in today’s modern health IT environment. It’s about compliance, it’s about assurance.
Trust, But Verify

- 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 is needed.

Resilient Supply Chains

- Greater due diligence in vetting vendors
- Security requirements in contracting should be SLA based
- Particular attention to cloud, SaaS, infrastructure support, critical service providers
- Life cycle approach to data protection
- Detailed breach and termination provisions
Trusted Medical Devices

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.

FDA has published guidance to both consumers and device manufacturers.

FDA, the NHISAC and NIST are collaborating on revised rules for medical devices.

Administrative Discipline

- 3.4 million BotNets identified
- 20-40% of recipients in phishing exercises fall for scam
- 26% of malware delivered via HTML, one in less than 300 emails infected
- Malware analyzed was found undetectable by nearly 50% of all anti-virus engines tested
- As of April 2014 Microsoft no longer provides patches for WN XP, WN 2003 and WN 2000, NT, etc.
- EOL systems still prevalent in healthcare networks
- Hardening, patching, configuration, change management...all critical
- Objective testing and assessment

Various: Symantec, IBM, Solutionary
Annual Threat Reports

"FBI alert warns healthcare not prepared"
Embrace Mobility of Data

- Medical staff are turning to their mobile devices to communicate because it's easier, faster, more efficient...but it is not 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
- Priority placed on the data first and the device second
- Restrict physical access where possible, encrypt the rest

“Clinical staff have on average six plus mobile devices”

Prioritize Efforts to Fight ID Theft & Fraud

- ID theft and fraud costs billions each year, affecting everyone
- US CERT estimates 47% of cybercrime aimed at healthcare
- Healthcare directed attacks have increased more than 20% a year for the last three years running
- 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
Lose Assets, Not Data

- 1 in 4 houses is burglarized, a B&E happens every 9 minutes, more than 20,000 laptops left in airports
- First rule of security: no one is immune
- 138%: the % increase in records exposed in 2013
  - 83%: the % of large breaches involving theft
- 6 – 10%: the average shrinkage rate for mobile devices
- Typical assets inventories are off by 60%

“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

Lower Your Risk Profile

- Defenses are not keeping pace
- Three most common attacks: spear phishing, Trojans & Malvertising
- APTs, phishing, water cooler attacks, fraud, etc. (HeartBleed, ShellShock, Poodle)
- 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.
- Conduct independent risk assessments regularly

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

- 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 FTC remains committed to enforcement of privacy and security
- Business associates will present new risks for covered entities
- States continue to create new laws

Single law in EU 2014
Two Laws seeking to unify requirements in US

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

Manage The Cost of Security

Discovery, Notification & Response
Business Disruption
ID Theft Monitoring
Investigation/Review

Civil Penalties
Federal CAP/RA
State Actions
Law Suit Defense

Criminal Penalties
Insurance
Degradation of Brand/Image
Distraction of Staff

VBP Payments Impacts
Federal CAP/RA
Insurance
Degradation of Brand/Image
Distraction of Staff

HCAPPS Score Impacts
Patient Confidence/Equity
Physician Alignment/Nurses and Staff Agreement
Making The Right Investment

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

• In a 2014 study HC CISOs gave themselves an average maturity rating of 4.35 on a scale of 1-7
• Many report missing critical technologies to fight today's threats
• More than half of healthcare entities spend less than 3% of their IT budget on data protection
• Less than half have a full time CISO or information security manager
• Many healthcare security managers are first timers

What We Need Now

• Enlightened leadership
• Skilled personnel
• Intelligence
• Smarter rules
• A better road map
• Vigilance
Questions

Got a Question

Contact Us

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