The Importance of Cybersecurity in a Complex Threat Environment

Presented by:

Mac McMillan

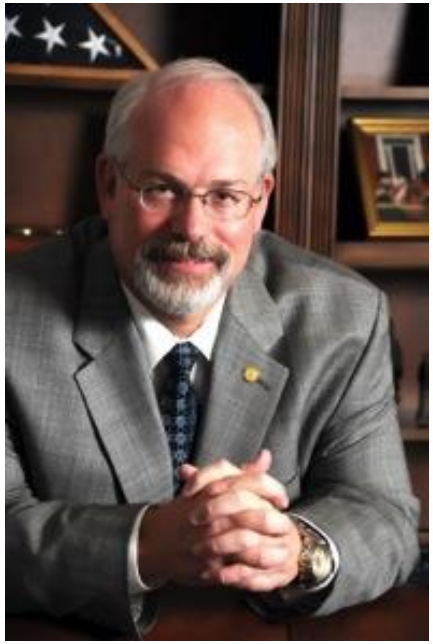
Chair, HIMSS P&S Policy Task Force

& CEO, CynergisTek

HIMSS
transforming health through IT

Today's Presenter

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

HIMSS
transforming health through IT

Sun Tzu & Cybercrime

"If you know yourself but not the enemy,
for every victory gained you will suffer a defeat."

HIMSS
transforming health through IT

The Face of Cybercriminals in Healthcare

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

HIMSS
transforming health through IT

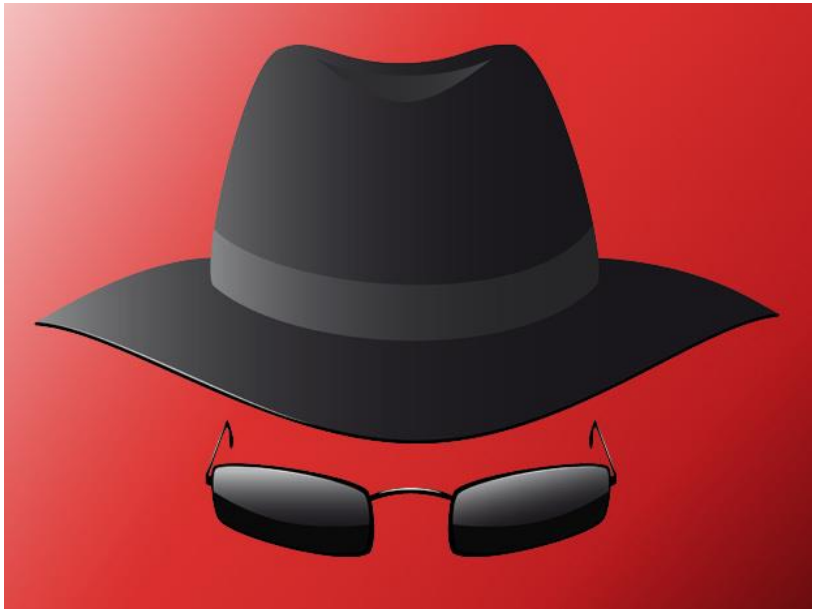
Cyber Incidents: Accidents, Mistakes & Deliberate Acts

- 4M medical records maintained on **four workstations stolen**
- 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
- 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
- 400 hospitals billings delayed as clearinghouse hit with **ransomware**
- **Failure to apply fix** to router results in compromise and loss of 4.5M records
- Mistake during **software upgrade test** results in 8000 letters mailed
- Physician held up at gunpoint, threatened with harm unless he **turned over passwords** for computer and phone
- And, on and on it goes…

HIMSS
transforming health through IT

Every new Threat Demonstrated Touched Some Aspect of Health IT

- **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



HIMSS
transforming health through IT

Black Market Driven – Cybercriminals Have Financial Backing & Support

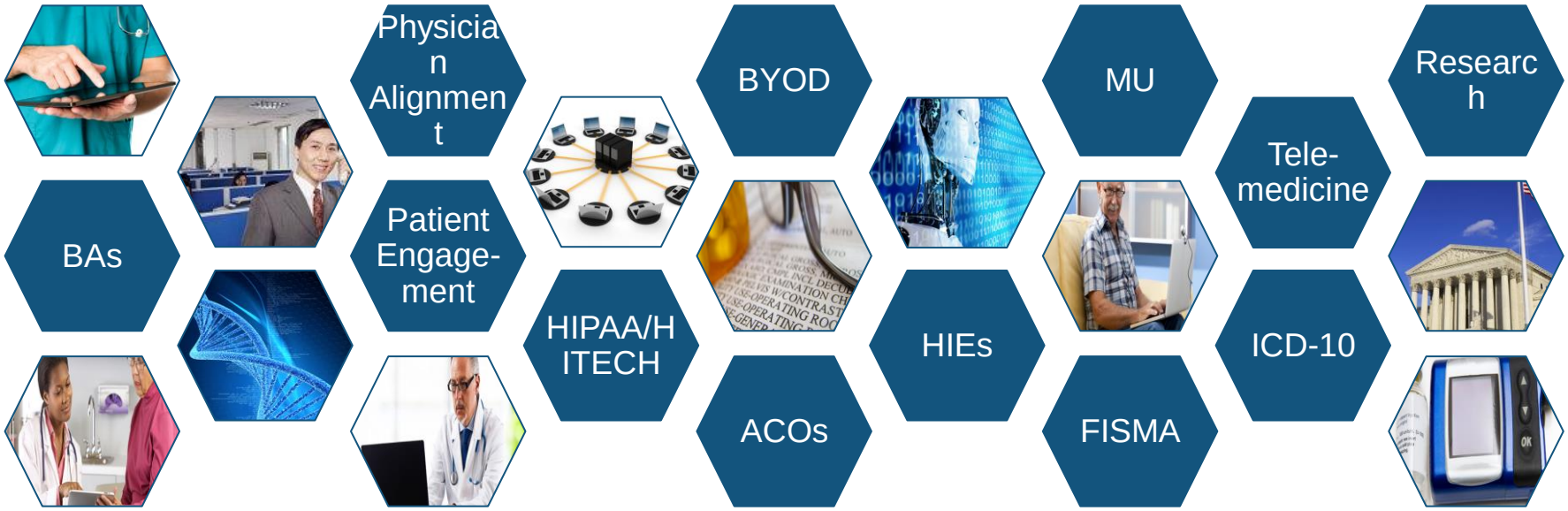
- Darknets will be more active, participants will be vetted, cryptocurrencies will be used, greater anonymity in malware, more encryption in communications and transactions
- Black markets will help attackers outpace defenders
- Hyperconnectivity will create greater opportunity for incidents
- Exploitation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

RAND Corporation, 2014

HIMSS
transforming health through IT

Increased Reliance

More than 98% of all processes are automated, more than 98% of all devices are networkable, more than 95% of all patient information is digitized, accountable care/patient engagement rely on it. The enterprise is critical to delivering healthcare. Any outage, corruption of data, loss of information risks patient safety and care.



HIMSS
transforming health through IT

Insider Abuse: Trust, but Verify

- It is estimated that more than half of all security incidents involve internal 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.
- 51% of respondents in a SANS study believe the negligent insider is the chief threat.
- 37% believe the security awareness training is ineffective.
- Traditional audit methods & manual auditing is completely inadequate.
- Behavior modeling, pattern analysis and anomaly detection is what is needed.

HIMSS
transforming health through IT

Questionable Supply Chains

- Venders still account for nearly 30% of our breaches
- Need 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

HIMSS
transforming health through IT

Devices Threaten Safety & Information

- In June 2013 the DHS tested 300 devices from 40 vendors. ALL failed.
- In 2014 the FDA issued guidance for manufacturers and consumers addressing design, implementation and radio frequency considerations.
- In 2015 we're no closer to a solution

"Yes, Terrorists could have hacked Dick Cheney's heart."

– The Washington Post
October 21, 2013

HIMSS
transforming health through IT

Malware & Advance Persistent Threats

- 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

"FBI alert warns healthcare not prepared"

Various: Symantec, IBM, Solutionary Annual Threat Reports

HIMSS
transforming health through IT

Embrace Mobility of Data

- Medical staff are turning to their mobile devices to communicate because its easier, faster, more efficient…but it is not secure
- Sharing lab results, locating another physician for a consult, sharing radiology images, updating staff on patient condition, getting direction for treatment, transmitting trauma information 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 6.1 mobile devices"

HIMSS
transforming health through IT

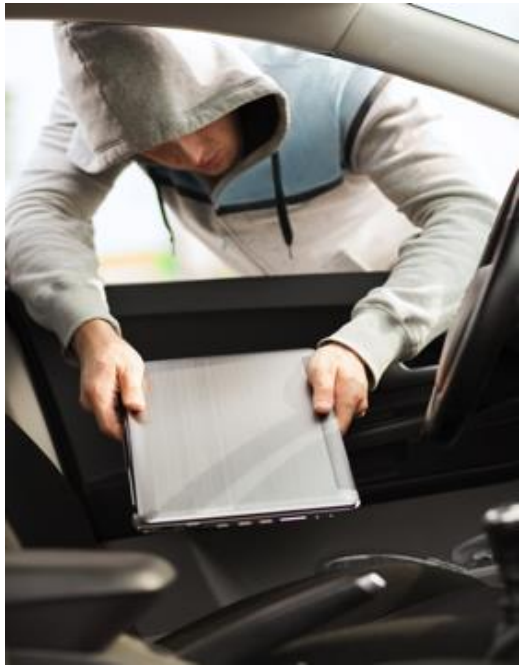
ID Theft & Fraud

- ID theft and fraud costs billions each year, affecting everyone
- 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

Thefts & Losses Thriving

- 68% of healthcare data breaches due to loss or theft of devices
- 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%

HIMSS
transforming health through IT



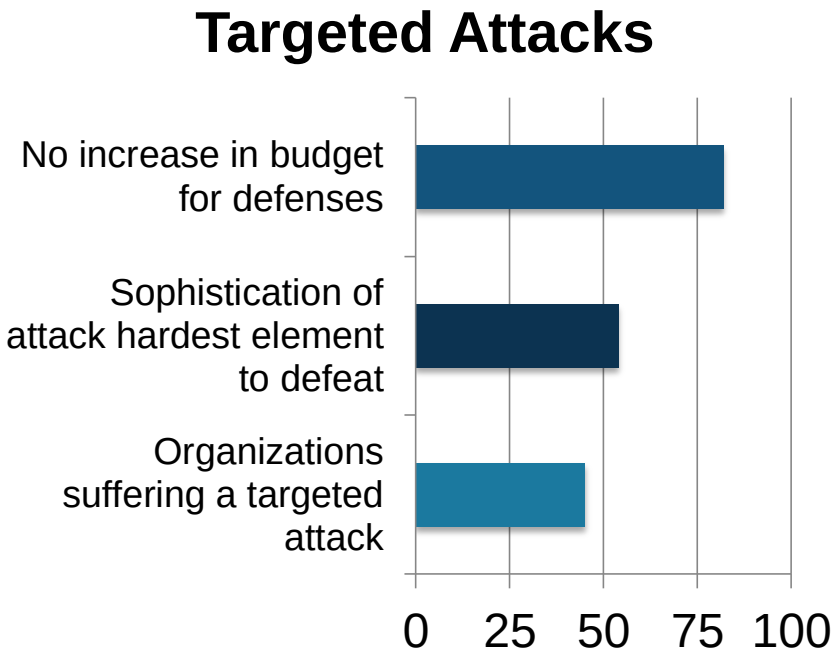
"That's a big number because it's meant to drive home the point that unencrypted laptops and mobile devices pose significant risk to the security of patient information."

– Sue McAndrew, OCR

Healthcare's Growing Risk of Targeted Attacks

- Defenses are not keeping pace
- Three most common attacks: spear phishing, Trojans & Malvertising
- Individual employees remain easy victims of social engineering
- Most organizations can't detect or address these threats effectively
- Top three areas of vulnerability – endpoints, third parties & mobile devices
- Need to focus on exploitation and exfiltration
- Results in losses of time, dollars, downtime, reputation, breaches, litigation, etc.

HIMSS
transforming health through IT



"I feel like I am a targeted class, and I want to know what this institution is doing about it!"

– Anonymous Doctor, UVMC

More Compliance

- OCR's permanent audit program is set to begin in 2015, with both desk top and comprehensive audits.
- Improvements and automation in reporting and handling complaints.
- Meaningful Use audits are evolving in scope and impact.
- New OIG audits for technical integrity of EHRs.
- The FTCs enforcement of privacy and security will continue.
- States continue to create new laws

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

Covered Entities and Business Associates must understand that security is their obligation.
– Sue McAndrew, OCR

HIMSS
transforming health through IT

The Growing Cost of Security

Discovery, Notification & Response	Civil Penalties	Criminal Penalties	VBP Payments Impacts
Business Disruption	Federal CAP/RA	Insurance	HCAPPS Score Impacts
ID Theft Monitoring	State Actions	Degradation of Brand/Image	Patient Confidence/Loyalty
Investigation/Review	Law Suit Defense	Distraction of Staff	Physician Alignment/Nurses and Staff Agreement

Questions

Questions?

Mac McMillan

mac.mcmillan@cynergistek.com

512.405.8555

@mmcmillan07

HIMSS
transforming health through IT