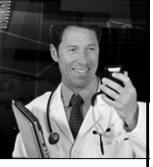
Culture of Privacy & Security, What Does That Mean?

Iowa HIMSS



Presented by Mac McMillan
FHIMSS, CISM
CEO, CynergisTek, Inc.

CYNERGISTEK

www.cynergistek.com

Today's Presenter

- 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
- HealthTech Industry Advisory Board
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
FHIMSS/CISM
CEO CynergisTek, Inc.

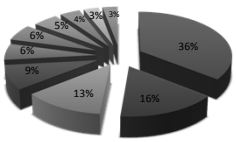
Agenda

- Analyzing the Numbers
- Challenges to Privacy & Security
- A Look Ahead
- Questions/Discussion

Analyzing the Numbers

Threat Outlook

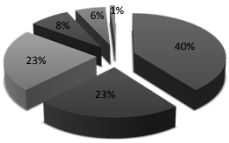
Data Breaches by Sector



- Healthcare 36%
- Education 16%
- Government 13%
- Accounting 9%
- Computer Software 6%
- Financial 6%
- Information Technology 5%
- Telecom 4$
- Computer Hardware 3%
- Community & Non-Profit 3%

2012: The Numbers

Top Causes of Breaches



- Hackers 40%
- Accidents 23%
- Theft/Loss 23%
- Insider Theft 8%
- Unknown 6%
- Fraud 1%

Risks Are Increasing

- For the fifth straight year insider abuse and misuse of data and access to systems continues to be biggest threat to patient information and identity
- Emerging trends in managing and delivering IT services; cloud services, BYOD, mobile apps, social media, texting…are increasing the risks to patient information
- In 2011/2012 we witnessed public hacking of medical devices demonstrating their vulnerability, in 2013 a national threat advisory released called them a critical threat
- Threats that continue to lead in the stats include: third party service providers/business associates, hackers using new/old threats, loss and theft of data

2012: The Numbers

- 42% increase in number of **targeted att**acks
- **5,291 new vulnerabilities** discovered in 2012, roughly 100 per week
- Average number of identities exposed during breach **604,826**
- **415 mobile device vulnerabilities**, an increase of 25%, 80% of healthcare still using unprotected mobile devices
- % spam with dating/sexual content 55%, average opens during tests **at healthcare entities +20%**
- Overall email virus rate, **1 in 291**
- Overall email phishing rate, **1 in 414**
- Bot zombies detected, **3.4 million**, making indiscriminant attacks a forgone conclusion

Symantec Report, 2013

The Numbers Continued

- Web attacks blocked per day - 247,350, **25% increase**
- Increase in mobile malware families – **58%**, percentage healthcare securing mobile devices – **less than 20%**
- Unsecured medical devices (pace makers/imaging systems/insulin pumps) present patient safety issues, **69%** do not secure these devices
- **62%** are using cloud services, **70%** are not confident or only somewhat confident of security
- **28%** are members of an HIE, **17%** will join in 2013, **66%** are not confident or only somewhat confident in security

Ponemon Institute & Symantec 2013

Complexity Creates Challenges

- Healthcare has significant challenges ahead from HIE, ACO, Patient Engagement, Physician Alignment, Telemedicine, etc.
- Greater connectivity and data sharing, creating the ubiquitous health record
- New approaches to information management and service – cloud, mobile devices, mobile apps, social networks…some say the demise of the network as we know it
- Clashing social norms and privacy and security regulations

Resources Create Challenges

- Spending on security (people, technology, services) continues to lag far behind other regulated industries
- The average spend on IT security is between 6 – 12% of the IT budget while Healthcare comes in below 3% except for those who have suffered a major breach
- Adoption of security technologies has been slow
- Healthcare organizations reported for the fourth straight year the same story,
  - Nearly 70% reported allocating less than 3% of their IT budget on security related support

Regulations Create Challenges

- HITECH introduced multiple changes to HIPAA Privacy and Security (Omnibus Rule, Breach Notification, Accounting for Disclosures)
- Evolving Meaningful Use requirements
- Anticipated changes to other rules such as SAMHSA, CLIA the Common Rule, etc.
- Continued evolution of State Laws with greater specificity
- ***New*** Federal proposed laws such as Security America's Health Information Act of 2012 in response to incidents
- 2012 Cybersecurity Executive Order for protection of critical infrastructure

Enforcement Creates Challenges

- HIPAA Privacy & Security enforcement are the responsibility of HHS/OCR:
  - Resolution of complaints: 10,000/yr.
  - Investigation of breaches: ~10/mo.
  - Random audit program: 115 1st yr.
- Meaningful Use attestation enforcement is the responsibility of HHS/CMS:
  - Audits/investigation by OIG
- Regional HHS OIG Offices conducting random audits of covered entities for compliance
- Omnibus provides greater flexibility to penalize

The costs associated with incidents are increasing.

A Look Ahead

Healthcare IT Trends

- **Mobile Health** – more than 2/3 of physicians are using tablets for clinical purposes, more than 90% report texting is part of their workflow
- **Personal Health Records** – patient engagement will continue to be a big focus area with patient portals being the primary interface for data
- **Telemedicine** – an increasingly large elderly and mobile patient demographic along with the needs of rural America will increase the need for telemedicine
- **EHRs** – adoption of EHRs has momentum, while still slower among smaller physician practices, this plus HIE, ACO and other exchange initiatives will make interoperability an imperative
- **Clinical Analytics** – the desire for better analytics will push for greater sharing and initiatives like "big data"

Information Week, 2013

The Threat Landscape

- **Cybersecurity** – primarily espionage and terrorism directed malware threats, will include infrastructure, telecommunications and Internet Outages.
- **Supply Chain Security** – organizations will experience increased threats from disrupted supplies from key partners.
- **Big Data** – related to supply chain, big data creates large repositories of sensitive data as lucrative targets
- **Cloud** – also related to supply chain, like big data creates massive interdependencies on partners
- **BYOD** – increased consumerization of the workplace and poor implementations leads to sensitive data on unprotected devices and boundary issues

Infosecurity & Fire Eye, 2013

Threat Projections

- **Sophistication** – Hackers will gain access to more sophisticated attacks used for cyber warfare and espionage over time increasing the risk
- **Websites** – Sites on the Internet will become more dangerous with time as hackers use malvertising attacks and water cooler scams
- **Social Media** – The combination of OS, communications and advertising will make this an attractive target, the use of smart phones will increase this risk exponentially
- **Malware** – Will continue to increase in sophistication and ability to thwart defenses. Smartphone and tablet penetration will make this variant of malware lucrative
- **Phishing** – Identities will remain valuable and phishing is an easy way to steal them, more sophisticated sites and variants are expected

Symantec, 2013

Shrinkage Happens

- Lost or stolen media and devices will continue to occur

- Number one source of lost or compromised patient information
- Evaluate data management rules and protective measures
- Encrypt any media and mobile devices with protected health information

Just Do It

- Encrypt….

- Many statutes require development of an enterprise encryption strategy for data at rest and in motion
- Decisions regarding encryption must now be documented
- Meaningful Use, Breach Notification, Accounting for Disclosures

Its About the Program

- Enforcement activity is expected to increase as will penalties and fines

- Evaluate readiness posture and address gaps
- Build a sound program around an established data security framework
- Invest in resources; people, technology and external support
- Train, monitor and test

People Aren't Infallible

- Privacy breaches will continue as workforce members violate rules

- Change the culture of the organization from the top down
- Reorient training for workforce members to more effective methods
- Evaluate privacy monitoring practices
- Tie privacy and security to performance evaluations and ensure accountability

Detection & Reaction

- Network, technical, criminal, service risks will all increase

- Conduct thorough risk analysis of the enterprise regularly
- Adopt a standards based security architecture
- Enhance network and system monitoring capabilities
- Develop big data, cloud, third party and incident detection security strategies

The Last Word

- Expect more: more legislation, more rules, more requirements

- Congress expected to pick back up on Cybersecurity legislation
- More rules to come; Accounting for Disclosures, Meaningful Use Stage 3, etc.
- States are adopting more stringent laws
- Base programs on industry standards

Change the Discussion

- Incidents will cost healthcare valuable dollars

- Prevention always costs less than reaction
- Stop focusing on the fines, refocus on ROI
- Security incidents waste valuable dollars, costly in top line revenue to replace
- Technology, resources and expertise will be in demand

CYNERGISTEK

Wrap Up & Questions

Today's Reality

- An evolving and more directed threat will become increasingly more dangerous and present **real risk to both confidentiality and patient safety**
- Digitization of data, automation of processes and services and the consumerization of the network will continue to increase the requirement for **more sophisticated protections**
- To create an enterprise capable of meeting tomorrow's protection requirements and ensure reliable information services will **require greater commitment of resources**

CYNERGISTEK

Thank You

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

CYNERGISTEK