New England HFMA Compliance Conference
Doubletree Hotel, Westborough, MA
December 11, 2015

Cybersecurity in Healthcare

Panelists:
Heather Fowles, CISA, CISSP, ISO
& Director of Information Security,
Mass Eye & Ear Infirmary

John D. Halamka, MD, CIO,
BIDMC System

Cedric J. Priebe III, M.D. SVP and CIO,
Lifespan

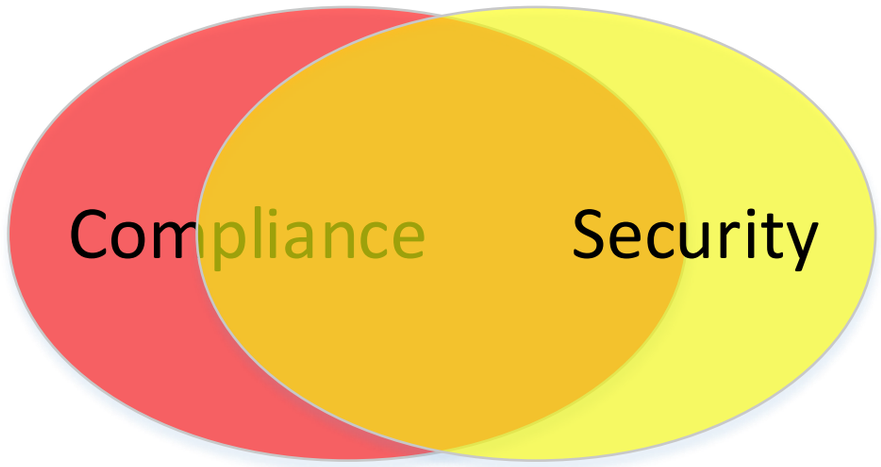
Moderator:
Chris Baldwin - Owner & Principal,
CSB IT Solutions, LLC

Security Management & Risk Management

Strategy: We need to have a consistent approach to risk assessment, risk mitigation, and security incident response with a well defined set of processes, tools, and command structures. Some services may be insourced and some outsourced….”John Halamka”

1. How should the information security program be governed?
2. What should be outsourced?
3. What should be insourced?

Compliance vs. Security



Compliance

- Office of Civil Rights
- Attorney General actions
- OIG Audits
- HITECH/HIPAA Omnibus Rule
- Cyber-liability
- Payment Card Information (PCI 3.0)
- State Laws (CMR17)

Security

- Physical, Technical, Administrative safeguards
- Storage and Transmission (encryption)
- Intrusion Detection
- Vulnerability Management
- Network Monitoring
- Workforce as a Threat

Threats & Vulnerabilities

Some Examples from the Field:

- The Lost Laptop
- The Compromised Radiology Workstation
- The Anonymous Attack
- The Phishing Experience
- The Boston Marathon Issues

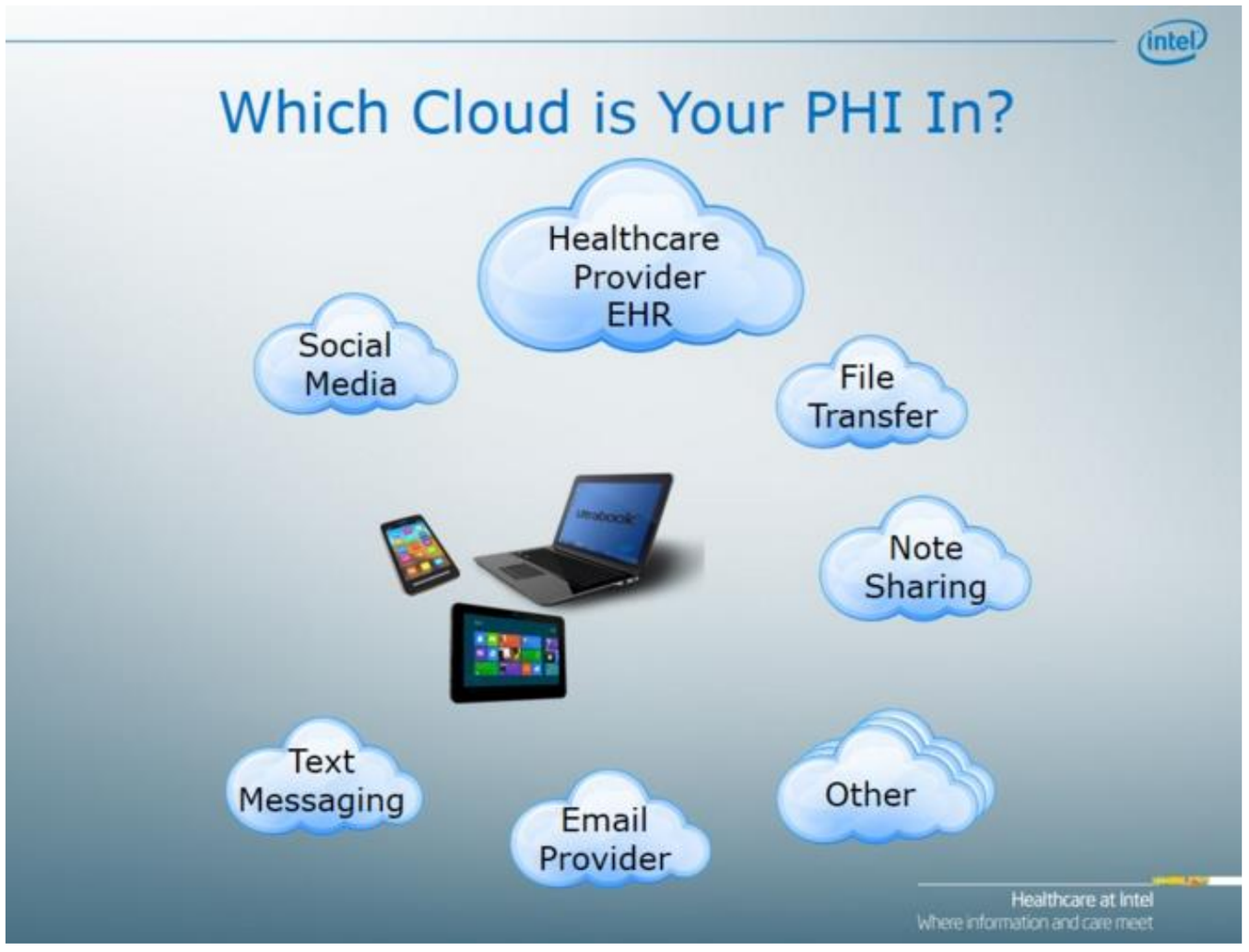
Most Nightmarish Experience…..

- HIPAA Breach
- OCR Settlement
- The Anonymous Attack
- The Phishing Experience
- The Boston Marathon

CEO…CIO…CISO

- Roles and conversations
- Division of responsibility
- Making the case for resources
- “Fox Guarding the Chicken Coop”

The Cloud & Business Associates



Top Ten Security Initiatives ?

- Encryption
- Workforce Education
- Intrusion Detection
- Next Generation Firewall
- Mobile Device Management
- Policies & Procedures
- Data Loss Prevention