Healthcare Information Technology—A Risky Business?

Healthcare—Security Summit
12 March 2014
Disclaimers

» This presentation is for educational purposes only.
» This presentation does not constitute legal advice. Please consult your attorney or other professional advisor to discuss your specific situation and obtain the appropriate legal or other expert advice.
» Any products or services mentioned are merely examples and not an endorsement.
Introduction
Gerard Nussbaum, Director, Technology Services

gerard.nussbaum@kurtsalmon.com

Mr. Nussbaum has over 30 years of health care and industry experience dealing with information technology, finance and marketing functions. He has assisted clients with a wide range of information systems, telecommunication and networking planning; vendor selection; and implementation project management assignments; interim management; merger and consolidation; electronic health record system planning; facilities planning and design; and development of systems to model mergers and acquisitions. Gerard also has held leadership roles at a major hospital alliance and a major health care manufacturer/supplier.

Areas of Expertise

- Technology strategic planning, development and governance
- Senior information technology interim management
- Meaningful use, HIPAA privacy/security and related regulatory matters
- Health information exchange planning, development and governance
- Technology visioning for new facilities planning; infrastructure budgets and requirements as part of overall facilities assessment, design and planning
- Electronic health record planning, selection, contracting and deployment; community/physician health record initiatives
- Voice and data infrastructure assessment; network and telecommunications design review; and network tactical and strategic plan development, selection and implementation
- Evaluation, selection, contract negotiation and acquisition of software, hardware, and enterprise voice and data network systems (wired and wireless) infrastructure
- Project management of application, network and technology implementations
- Security and privacy assessment and remediation
- E-health strategy, development and implementation
- Central business office, physician practice and management services organization creation and start-up
- Outsourcing cloud computing/ASP analysis, negotiation and management
- Service level agreement development
- Implications of regulatory actions and requirements on information technology use and development

Professional Affiliations/Speaker/Author

Healthcare Information and Management Systems Society (HIMSS)
College of Healthcare Information Management Executives (CHIME)
Healthcare Financial Management Association
American Health Lawyers Association

Education

Juris Doctorate, Chicago-Kent College of Law
BS and MS in Accountancy from the University of Illinois, Urbana-Champaign
CPA, CMA, Registered Communications Distribution Designer (RCDD)
About Kurt Salmon

Extensive, relevant EXPERIENCE

» Academic, children’s, community and national health systems

Change LEADERS

» Highly pragmatic and focused

PROVEN team

» Careers spent supporting leading health systems and complex environments

Track record of SUCCESS

» Rich history dating to 1947
» Over 75% of ongoing work with repeat clients
About Kurt Salmon: Information Technology

- Strategic and Tactical Planning
- Physician-Hospital Alignment
- Connecting Communities
- Population Health and Care Coordination
- Technology Planning for New Facilities
- Business Intelligence and Analytics

- Vendor Selection and Contract Negotiation
- Pre-Implementation Planning
- Implementation Oversight

- Meaningful Use Achievement
- ICD-10 Preparation
- Security and Privacy Compliance

- IT Transformation
- Infrastructure Planning
- Right Sourcing
- Interim Leadership
Targeting Healthcare
Drawing a Target on Healthcare

The Target credit card theft should scare healthcare

Simple steps

» Steal credentials from a contractor
» Enter through the low-level system
» Find your way to the pot of gold
» Steal the gold

Questions

» Is there such a thing as a low-security system?
» How many third-party entry points are there?
» Do we have systems that are easy to exploit?

Danny Yadron and Paul Ziobro, Before Target, They Hacked the Heating Guy, Wall Street Journal, 5 February 2014
(http://blogs.wsj.com/digits/2014/02/05/before-target-they-hacked-the-heating-guy/tab/print/)
Potential Weak Points

Devices Emitting Malicious Traffic

Healthcare Providers Are Compromised

Healthcare versus Other Critical Infrastructure Sectors—ICS-CERT Responses

Implantable Medical Devices
Implantable Device Vulnerabilities

» Vulnerable to threats
  – Cardioverter defibrillator/pacemaker
  – Insulin pump
  – Other devices also potential targets

» Attack
  – Wireless controls used to program and report data from device
  – Intercepting and altering wireless signals
  – Malware payload on firmware updates
    • Reprogram
    • Mask alerts/generate false readings
  – Denial-of-service attack on device or controller/programmer
    • Overwhelm device
    • Cause battery drain
  – High-power electromagnetic interference

» No identified actual adverse events

Radio Frequency Wireless Technology in Medical Devices—Guidance for Industry and Food and Drug Administration Staff, Food & Drug Administration, 13 August 2013 (http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077210.htm)
Implantable Device Vulnerabilities

» FDA premarket approval (PMA) process does not fully address security risks

» FDA’s adverse event reporting geared to clinical, not information security, risks

» Newer devices may offer improvements (e.g., encryption)

» Many earlier devices still in use

» Constant catch-up cycle on current threat-reduction approaches

» Augmenting security could impair device functionality
  – Encryption could interfere with emergency treatment
  – Limits on device size and battery capacity limit adding complexity
  – More complex devices may be a challenge for clinicians and patients

Radio Frequency Wireless Technology in Medical Devices—Guidance for Industry and Food and Drug Administration Staff, Food & Drug Administration, 13 August 2013 (http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077210.htm)
Embedded Off-the-Shelf Software
Windows XP—Doom Approaching?

“PCs running Windows XP after April 8, 2014, should not be considered to be truly protected” – Microsoft

» Microsoft Security Essentials updates to existing users until mid-2015
» More vulnerable to malware and other attacks
» “anti-malware products have limited effectiveness on PCs that do not have the latest security updates, your PC will still be at risk for infection” – Microsoft
» No security updates for the Windows XP operating system

Is healthcare in good company?

» 95% of ATMs running on XP
» Utilities—widespread use of XP in control systems

Have you performed a risk analysis?

» Cost of buying new medical devices
» Risk of vulnerability
» Cost of adverse event(s)
  – Patient harm
  – Medical malpractice
  – Publicity
  – HIPAA

Dealing with Windows XP

In many cases, you will not have a choice about continuing to use Windows XP

» Download Microsoft Security Essentials
» Air gap or isolate to separate from other networks
» Whitelist of allowed connections, applications, files
» Locking unneeded ports
» Install final XP update
» Use a browser that retains support
» Update other apps—e.g., Office—or remove any non-critical apps; old software is vulnerable
» Tighten down security settings
» Train users for extra vigilance
» Increase monitoring of unpatched equipment
» Disable plug-ins
» Check for Flash and Java and remove unless essential
» Anti-virus and firewall

Vendor contracts, medical device manufacturers and other constraints may limit what you can do
Who Is Responsible for OTS Software in Medical Devices?

FDA guidance on off-the-shelf (OTS) software has been consistent for over a decade.

» Manufacturers must
  – Keep their devices safe and effective
  – Examine sources of quality data and correct or prevent quality problems
  – Have a plan for how to update OTS software and follow it
  – Design in appropriate security

» Healthcare organizations
  – Lack technical resources/information to independently maintain medical device software
  – Should not patch medical devices
  – Work with medical device vendors
  – Plan for cyber security events

» FDA
  – Sets device approval requirements
  – FDA review of most software patches not required

Addressing Medical Devices and Related Risks

While the healthcare provider is not primarily responsible under FDA regulations ...

» Are medical devices included in your
  – Security risk assessment
  – Incident response

» Who is responsible for
  – Tracking medical devices
  – Monitoring security controls
  – Network architecture and security
  – Assuring adequate technical security knowledge
  – Inclusion in incident response teams and drills

» Is a security review part of acquiring medical devices

» Contractual issues
  – Commitments from medical device vendors on security and patching
  – Gag clauses that limit adverse incident reporting

» Insurance coverage of medical devices related to adverse security events under
  – Cyber liability insurance
  – Medical malpractice

» Voluntary reporting of adverse security events
Reporting Security-Related Device Issues

In the event that a security incident causes significant injury

» Reporting medical device adverse incidents (facilities)
  – Death to both the FDA and the manufacturer
  – Serious injury to the manufacturer or to the FDA if the medical device manufacturer is unknown

» Voluntary reporting to FDA
  – Malfunctions (Facilities)
  – Significant adverse events or product problems with medical products (individual clinicians and consumers)

» Challenges of identifying a security breach causing an adverse event

Medical Device Reporting (MDR), U.S. Food and Drug Administration, (http://www.fda.gov/medicaldevices/safety/reportaproblem/default.htm#howtoreport)
Patient Safety Event Reporting

Patient Safety and Quality Improvement Act of 2005 (PSQIA)

» Voluntary reporting system
» Create datastore to assess and resolve patient safety and health care quality issues
» Federal privilege and confidentiality protections for patient safety information
» Patient Safety Organizations collect and review patient safety information

- Patient safety event reporting
  - Serious errors or system failures harming a patient
  - Near misses in which an error or system failure occurred without patient harm
  - Unsafe conditions with potential to cause harm

- May include health information technology events

Mobile and Consumer Devices
Leveraging Connectivity to Engage Patients

Continuous Capture/Embedded Analytics

Display/Monitoring/Control/Feedback

Core Clinical and Analytic Systems

Connectedness adds benefits to data collection

Health Systems-based Monitoring

Source: Scanadu.com, Sen.se, Soterawireless.com, Kurt Salmon
Growing Nodes Outside of the Four Walls

» The number of connected devices will continue to grow rapidly
  – Ingestible monitoring devices
  – Pill bottles
  – Home patient monitoring
    • Medical
    • Activities of daily living
  – Wearable sensors/monitors
» Connected to central healthcare systems
» 26 billion devices by 2020 (all Internet)

Mobile Platforms Bring Access and Vulnerabilities

Use of mobile computing devices is growing rapidly in healthcare

Source: Threat Report H2 2013, F-Secure
Response Tactics
Response Tactics

» Technical tools and processes
  – Data loss prevention
  – Penetration and vulnerability tools
  – Identity management and end-user provisioning
  – End-point authentication
  – Mobile device management
  – Forensic tools
  – Auditing tools, stepped-up audits
  – Application layer scanning
  – Encryption
  – Incident response
Response Tactics

» Reevaluate scope of security risk assessment—does it cover all of the vulnerabilities?

» Raise emphasis on secure application design
  – Selection criteria
  – What is your application security design architecture?

» Revamp security governance

» Educating management—in business terms

» Workforce education and involvement

» Security event reporting—more than internally
  – Patient safety organizations
  – Vendors
  – FDA
Wrap-Up
QUESTIONS

Gerard Nussbaum
Director, Technology Services
Kurt Salmon
212-508-8371
Gerard.Nussbaum@kurtsalmon.com