Mobile Device Risk Management: Security in Motion

20TH NATIONAL HIPAA SUMMIT

BY J. DAVID KIRBY,

PRESIDENT, KIRBY INFORMATION MANAGEMENT CONSULTING, LLC

DAVE@KIRBYIMC.COM

Overview

- Definitions/scope
- Key security threats and issues in mobile environments
- Mitigation strategies

Definitions/Scope

- Mobility of data, ePHI access devices, and ePHI collection devices involved in health and healthcare.
- Mobility within a care facility (a facility with some physical protections) by providers, insurers, other healthcare related entities and business associates.
- Mobility outside of a facility (with generally fewer physical protections) by providers, patients, others (e.g. insurers, debt collectors, business associates)and the public generally.
- Security: Confidentiality, Integrity, Availability

Key Security Issues in Mobile Devices/Media

- Scale of problem:
  - 39% of privacy breach incidents reported on HHS' "wall of shame" occurred on laptop or other portable device. (vs 25% on desktop or server) – despite desktops+servers with ePHI access likely being much more numerous than mobile devices
  - Plus mobile media (backup tapes, USB devices) account for a large number of the exposed records (in a few large events); (88% of all exposed records are in only 20 events in last two years).

COVERED ENTITY	STATE	B/A	DATE	# OF PATIEN	TYPE	DEVICE/LOCATION
TRICARE	CA	SAIC	9/13/2011	4,901,432	Loss	Backup Tapes
Health Net	CA	IBM	1/21/2011	1,900,000	Unknown	Server drives
NYC - HHC	NY	GRM	12/23/2010	1,700,000	Theft	Backup tapes (in van)
AvMed	FL		12/10/2009	1,220,000	Theft	Laptop
Nemours Foundatic	FL		8/10/2011	1,055,489	Loss	Backup Tapes
Top 5 breaches - 9/2010-11/2011						

Key Security Issues in Mobile Devices/Media

- Scale of problem:
  - Strong maliciousness component: 60% of breaches involve malicious intent. Organized crime is much more active in seeking ePHI now than in the past (for medical identity theft mostly).
  - Serious impact: 29% of respondents to Ponemon Institute Study said that that breaches led directly to instances of medical identity theft.
  - BAs are involved in 59% of reported breaches overall.

Key Security Issues in Mobile Devices/Media

- Scale of problem:
  - Personal physical security (of the phone/tablet/laptop user):
    - The smartphone is now the most expensive item carried that is of value to street thieves.
    - Such thefts exceed hard currency thefts in NYC in 2011.
    - 50% of all thefts in NYC (16,000 thefts total) over first 10 months of 2011 involved thefts of smartphone/tablets.
    - Iphones are most prized (70% of cell phones stolen on NYC subway are Iphones).
    - City of San Francisco reported 40 cell phone theft muggings in November 2011.

Key Security Issues in Mobile Devices/Media

- As compared with fixed media/devices:
- Loss of mobile device
  - Greater than fixed device
  - ~4% per year of handheld devices lost (i.e. misplaced)
- Immaturity of technical protections… though improving – more later
- Low usage of existing protections (e.g. signons)

Key Security Issues in Mobile Devices/Media

- BYOD – Bring Your Own Device – growing expectation that employees can use their own devices for work-related uses. Mixes personal and corporate data and apps.
- Aberdeen Group study in 2009: 40% of employees use their own phones for business.
- 48% of IT managers forbid BYOD (2012 Cisco survey of 1500 IT Managers)
- Many major IT firms allow BYOD in 2012(Cisco, Intel, Nvidia)
- Needs to protect company data, sort out "ownership" and legal discovery questions.
- But only 43% surveyed corporate execs (PWC survey) have security procedure for BYOD usage.
- In short: a new area of security concern for most organizations and individuals.
- Many healthcare settings are likely to be early adopters of policies for BYOD (e.g. hospitals with medical staff who access hospital systems but aren't usually employed by the hospital)

Key Security Issues in Mobile Devices/Media

- It is not all only about confidentiality losses.
- Each loss of device introduces an availability issue (at minimum to the device's authorized user and maybe to others who now won't get data cached on the device).
- When a device that collects ePHI is lost before it can upload ePHI into a server, a data integrity problem (loss of only copy of ePHI) is introduced.
- Medical identify theft (a routine consequence of losing a copy of ePHI) may result in a single medical record with mixed data on two people. (data integrity problem).

Mitigations: Administrative, Technical , Physical

- Do adequate risk assessments. The large breaches especially were clearly foreseeable and preventable.
- Use encryption – on devices, media, and during transmission with appropriate key protections. Most of the historical losses would have been prevented if encryption had been in use.
- For smartphone, networked mobile devices – use remote wiping and location software.
- Use device entry authentication (e.g. PINs or connect-the-dots patterns) with timeout locks.

Mitigations: Administrative, Technical , Physical

- At enterprise level: do purchasing controls for non-BYOD devices to assure that devices have technical security facilities needed.
- Do training updates to assure users know how to use a mobile device securely and are reminded of the importance of secure use.
- Do real-time or near-real time backup of device-based ePHI onto servers.
- Use secure thin-client/web apps to avoid storing ePHI on the device.
- Monitor/qualify mobile device connections to internal network.

Personal Mitigations for BYOD users.

- Android:
  - 1) research publisher of the app
  - 2) read online reviews
  - 3) check for reasonable permissions (android)
  - 4) avoid direct install of APKs (Android application package file)
  - 5) use malware scanner.
- Iphone
  - 1 Enable Passcode Protection
  - 2 Enable SIM PIN Protection
  - 3 Enable Auto-Lock
  - 4 Re-map Your Home Button
  - 5 Use a Password Storing App
  - http://howto.wired.com/wiki/Secure_Your_iPhone

Mitigation: Emerging Enterprise Technical Protections

- Mobile Device Management tools (that include security functions) along with:
  - Software distribution/patching, policy management, inventory management (which also have security impacts)
- MDM Common Security Features:
  - Enforced password usage
  - Device wipe (remote)
  - Remote lock
  - Audit trail/logging
  - "Jailbreak" detection – when user has defeated the vendor-built constraints on phone/data/app usage.
  - External memory blocking

Mitigation: BYOD Problem

- "Sandbox" software
  - is emerging that allows enterprises to secure facilities on a personal (employee's) phone that allow for enterprise data/activities to be separated from personal data/activities.
  - Examples: Sybase iAnywhere Mobile Office, Zenprise, Fixmo, Good for Enterprise
- Use of thin-client apps on mobile devices:
  - With good authentication, timeout, and encryption reduces the vulnerable surface of a mobile device.

Q&A

- Thanks
- Dave Kirby – Dave@KirbyIMC.com, 919-272-1157