Implementing Mobile Device Encryption: A Case Study

Bridget Aman, CISSP, CISA, CPA
John Blackley, CISSP
Introductions
Agenda

• Management Support
• Proof Of Concept (POC) Process
• Important Questions to Ask Vendors
• Project Management
• Testing
• Implementation
• User Impact
• Communications and Training
Drivers for encryption?

Hurdles?
Children’s Scope

- Laptops
- USB
- CD/DVD (write-restriction)
- Blackberries
- iDevices
Management Support

- Pre-requisite
- Alignment helps

- ROI:
  - Reputation
  - Trust
  - Brand/image
  - Research studies on costs of losing devices with unencrypted sensitive data

- Shamelessly leverage breaches
POC Process

- Most important step of project
- Critical Lesson Learned: “SHOW ME”
- Spent 3 months total
- Narrow down field
  - Gartner Magic Quadrant
  - Industry standards
  - Peer benchmarking
• Narrowed down to final two

• White boarding exercise listing pros/cons helped flush some things out

• Lesson Learned: Reference calls!!!

• Best practice: Technical rep and policy maker are both in the same room during POC
Technical Scenarios to Demo

- How does the patching process work with pre-boot authentication?

- What is process for moving data from one encrypted laptop to another?

- What is data recovery process when an encryption key gets lost/corrupted or user forgets key?

- How will data forensics be impacted?
Technical Scenarios to Demo

- What does USB encryption look like at work and at home? (including initial use)

- What does CD encryption look like at work and at home? (including initial use)

- How does USB/CD encryption work in multi-user/single-workstation scenario?

- File based encryption: how do I ensure everything that should be encrypted actually got encrypted?
Project Management

- Multi-disciplinary
  - Project Manager
  - Desktop Support
  - Testing Lead
  - Training
  - Technical Lead
  - Help Desk
  - Information Security
  - Communications

- Requires strong leader to keep all in lock step

- Weekly meetings throughout

- Steering Committee = Involved
  - Implementation dates
  - Go-live issues
Testing
Laptop Encryption

• WOW, we did a lot of testing – 6-8 weeks!

• Unit testing covered everything we could think of to break the system

• Tested every make/model of device in our environment

• Tested with 75 applications

• Three pilot groups
  • 2 Information Technology groups with a focus on remote access methods
  • 1 Clinical group of 15 people
Implementation - Blackberry

- Big bang ~ 350
- Four character PIN
- Data wipe after 10 failed attempts
- Enterprise AND personally-owned

Lesson Learned:
- Train on how to make/accept calls without entering PIN
Implementation - Laptops

- Staged approach
- 1,100 over 4 weeks
- Automatically pushed the agent
- Scripted the following:
  - Checked for minimum memory
  - Installed .net 2.0
  - Performed defrag
  - Installed encryption agent
  - Chk dsk
  - Reboot
Main issues:

- Older images, like everyone else
- Panasonics
- Windows 7
- One series of standard laptop inconsistently hangs upon reboot; required update
- Small amount of laptops would not automatically identify and connect to home wireless
Implementation - Laptops

• Lessons Learned

  • Have a good handle on your asset inventory
    • “Shifting denominator”

  • Have a strategy for pooled or loaner laptops or anything that doesn’t get logged into regularly

  • Require quantification of boot/login times before and after encryption, or else you’ll get “it takes forever” (WHINE…..)
Implementation - iDevices

- Forced Active Sync encryption and password profile
- Enterprise AND personally-owned
- Began with 150, now over 500
- Obtained attestation forms for personal devices
Implementation - iDevices

- Lessons Learned
  - Active Sync is a good first step, but really need MDM tool
  - Active Sync forces encryption, prevents lower iOS’s and non-encryptable devices from connecting, and provides reports that evidence encryption
  - Issues still to be addressed:
    - Preventing jailbroken devices from connecting
    - Managing multiple devices per person
Testing identified that original strategy did not work

Environment requires an important population of users not be tied to “primary” machine. Software-based approach did not support this.

Alternative implementation strategy: one authorized pre-encrypted USB available for purchase through normal supply ordering process

Utilized port control to disallow WRITE to anything else
Implementation – USB

• Lessons Learned
  • USB transfers between Microsoft and MAC O/S
  • Need encrypted alternative for large external drive storage
  • Better training guide for users (specifically the two partitions)
• No encryption

• Restricted WRITE access via port control

• Lessons Learned:
  • Identify equipment (non-workstations) that require CD/DVD write
  • Identify and evaluate cost/benefit of encrypting media provided to customers (e.g., patients)
• Exception Process!

• Have a good exception approval process utilizing the Help Desk, with a timely service level agreement and emergency procedures.
User Impact

• Blackberry
  • Few calls to complain this totally interfered with their texting while driving

• Laptops
  • Boot/login time went from an average of 2 - 2 ½ minutes to 4 – 4 ½ minutes
  • Pre-boot authentication

• iDevices
  • Totally quiet

• USB/CD/DVD
  • Many calls for exceptions, majority were justified
This effort will single-handedly determine how smooth your roll-out will be

No such thing as overcommunication

Communication Plan:
- Normal corporate communication vehicles
- Dog and pony shows (CMIO was helpful)
- Themed posters: “Encryption is coming!”
- Walkarounds/Giveaways
Communication and Training

- Training:
  - Help Desk
    - Formal lessons
    - Additional training by supporting pilot groups
  - Encryption Website
    - Project Summary
    - FAQ’s
    - Tip Sheets per device
    - Rollout schedules
    - Video clips
Final Thoughts…

• If appropriate, offering to be a reference for your vendor is valuable to you and your peers

• Don’t be afraid to reach out and see what others are doing

• Don’t diminish POC or testing processes just to make a date
Questions??

John Blackley
John.blackley@childrens.com