CSO PERSPECTIVES

Mobile Security Lessons Learned from a Global Company

Jim Huddleston, CISSP, CISM, CIPP, CGEIT

Director, Global IT Risk Management

How much control do we need?

- What is the Business Case?
- What do we need to control?
  - Apps
  - Security
  - Voice/Data Usage
- Control may infer tracking
  - (Legal Issues, Intl)
- Personally Owned vs. Business Owned has implications
  - How dare you try and control MY iPhone/iPad
  - How much can you actually control? Do you want to?

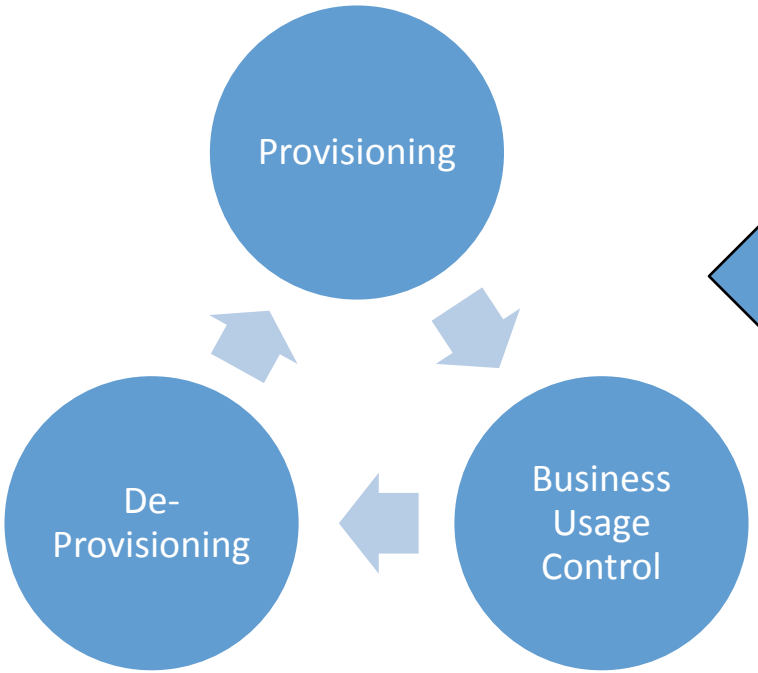
How much control do we need?

How do we execute control?

- Do we control device provisioning/setup?
- Central management? (MDM)
- De-Centralized management? (regional MDM)
- Manage via email?

Enforcement/Settings Capability

Device Life-Cycle Management



Mobile Device Management Platform
Support of Selected Devices
User Authentication
Encryption
Setting Policies
Remote Provisioning/Controls

Policies/Regulatory and Business Considerations

- Background (Sybase Study)
  - By 2013, 75% of all workers will be mobile
    - 20% of those will use a mobile device to do their work
  - 36% of cell phone owners will have either lost a phone or had one stolen
  - In the near future nearly 25% of all workers will have lost a mobile device that could provide access to confidential information
- Complications and Challenges
  - Workers using personal devices for work
  - Speed of introduction of devices
  - Increased diversity of mobile devices (iOS4/iOS5, iPhone, iPad, apps…)
  - Increased proliferation of mobile applications
  - Adapting existing policies to these devices
  - How to manage the devices and enforce policies

Policies/Regulatory and Business Considerations

User Awareness Education

- Use of company information on the device – policy adherence
- Use of customer information on cevice – contract adherence
- What to do if lost or stolen
- How are they allowed to use it for business, for personal use
- Rules over the technology
  - App store
  - Content (music, video, etc)
  - Internet access (appropriate use)
  - Use in combination with home computing

Policies/Regulatory and Business Considerations

Application Considerations

Apps in app store that enable business application/network access

- File transfer/remote desktop/Salesforce.com/documents to go

- Are your business applications (web based) compatible with Safari
- Use Thin Client for access to enterprise apps
- Suitability for business applications to be used on the device
- Access to malicious apps/sites

Policies/Regulatory and Business Considerations

Messaging

- Exchange ActiveSync (downloaded to device)
  - Mail
  - Contacts
  - Calendar
- Text Messaging
- Instant Messaging (numerous apps for this)
- Social Networking (web and app front ends)
- Personal Email (allowed?)

Policies/Regulatory and Business Considerations

Mobile Device Management Systems

- Capabilities to look for
  - Over the air management
  - Inventory and asset management settings
  - Role based access
  - Selective wipe
    - Wipe email
    - Wipe apps
    - Wipe configuration (Wifi, VPN, certs)
  - Application inventory

Policies/Regulatory and Business Considerations

Mobile Device Management Systems

- Capabilities to look for
  - App distribution
  - Run only permitted apps
  - Require certain apps on device
  - Cert management (Wifi, Exchange, VPN)
  - Password/encryption policy settings
  - Lockout certain features
    - Camera, app install, web access, iTunes use
  - Remote device lock/unlock/wipe
  - Cell network usage (roaming, international calling)

Policies/Regulatory and Business Considerations

Alignment and Support

Security/Risk
- Align with company policy and external requirements. Create mobility policy

Support
- Define appropriate support
- Plan for scale and demand of business

Productivity
- Select, define and create applications for use by the business

Policies/Regulatory and Business Considerations

Business Considerations/Risk

- Usage business case (business, development)
- Cost
- Regulatory/contractual
- Pervasive access to applications (appstore)
- Incompatibility with business applications
- Incompatibility with infrastructure (wireless, VPN)
- Data is accessible over cellular network
- Data is accessible over wireless/Bluetooth
- What data should be stored on the device?
- iTunes
  - Backup on local workstation
  - Personal use (audio/video/apps)
  - Only one backup is kept by iTunes (backup retention)

Policies/Regulatory and Business Considerations

Business Considerations/Risk

- Voice and video communications/recording
  - Privacy
  - Business use
  - Private use
- Usage plans through provider
  - Large amounts of data can be easily transferred
  - Data plan
- Messaging (locally stored information)
  - Email
  - Contacts
  - Calendar
  - User experience
  - iMessage
- Personal vs. Business Owned

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Network use and access
  - Additional bandwidth required on corporate networks?
  - Access to enterprise applications and data
  - VPN
- Support
  - Field support staffing and expertise
  - Help Desk
    - Access to MDM or Exchange
    - Expertise for troubleshooting/usage questions
  - Physical Support
    - Broken Devices
      - Disposal/Repair
      - Wipe prior to shipping for repair/exchange

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Support
  - Physical Support
    - Peripheral Devices (cost/replacement)
      - Keyboard
      - Desk stand
      - Bluetooth devices
      - Connector enabled capabilities (Apple TV)
- Cost
  - Device purchase/maintenance
  - Cell use (domestic, roam, international) voice
  - Apps
  - Cell use – data

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Compatibility and integration
  - Web apps (Safari/Dolphin/?)
  - Enterprise Standards
    - MS Office (.doc, .xls, .ppt)
    - SW distribution
    - Hardware/Software inventory
    - Remote diagnostic/access for support
    - Downloaded apps
    - Messaging
      - Mail functionality (UI)
      - Mail functionality (ease of use)
      - Mail functionality (different than workstation)

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Accounts
  - Who owns the account assigned to the device
    - Apple ID
  - How is it assigned?
- Verify if application encrypt their data
  - Determine if encryption is required
  - The only app from Apple that uses encryption is email
  - Majority of apps do not encrypt their data
- Only allow iOS 4.x
  - File level encryption only in iOS 4.x

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Create company policy regarding mobile devices
  - No hacking of devices
  - Business use only
  - Governed by appropriate use
  - Company owned?
  - Wipe on lost, dtolen, termination
  - Remove backups from iTunes/iCloud
  - Require corporate developed apps to encrypt data
  - Central MDM required

Policies/Regulatory and Business Considerations

Best Practices (Apple and Others)

- Mail session encryption
- Wipe devices when lost/stolen
- Enforce passcode lock
- Enforce autolock after x minutes of inactivity
- Enforce autowipe after x failed passcode attempts (default 10)
- Refresh Policies and Update
  - Process for review and update of policies
- Centrally manage devices
- Only use iOS 4.2.x and above
- Virtual desktop recommended for access to enterprise applications
  - No local device compatibility issues
  - Data not stored on the mobile device
  - Application can change with no effect to device
  - No local performance impact since device is not running the application

Policies/Regulatory and Business Considerations

Enterprise Implications and Risk

- Use may be governed by regulatory or contractual requirements
  - Can data even be allowed to be stored on the device
  - Encryption requirements (certificates/PKI)
  - Backup/restore requirements
  - Access management
    - From device
    - To device
- Internal Application Development
  - Web apps vs. Custom (device specfic) apps
  - iPad - data stored under ProtectionNone class is available without passcode to other apps like iTunes and third party applications
  - Develop Criteria for Securing Data
    - Just use HW encryption
    - Application encrypts the data
    - What data should actually reside on the device?

Policies/Regulatory and Business Considerations

- iPad/iPhone
  - Backups can be forced to be always encrypted in iTunes
  - Backup does not backup email
  - Backup does backup the following -
    - Contacts
    - App store application data
    - Call history
    - Keychain
      - Encrypted (can transfer to new device) needs password
      - Not encrypted (only can restore to original device)
    - Network settings
    - Calendar accounts and calendar events
    - Any attachments in calendar entries
  - Backups decrypt application encrypted data
  - All enterprise apps should invoke user authentication in the app
  - Enterprise apps delivered over the air are not in the iTunes library or backups

Policies/Regulatory and Business Considerations

Areas of vulnerability

- Lost or stolen devices (find my iPhone)
- Unauthorized data access
- Combining work and personal devices
- Immature management technology (getting current with devices and keeping current)

Personal vs. Corporate Use

- Pervasive and a commodity
- Who will own the asset?
- How will it be controlled and managed?
- What are the rules of engagement? (personally owned)
  - Business can wipe device
  - Limited Business use (rmail only?)
  - Remote access?
  - What will the business pay for? (device, voice, data, tethering…)
  - Only use of selected vendors? (AT&T, Verizon…)
  - Immediate business notification of device loss
  - What level of support will be provided… or not
  - Signed agreement by employee (review with legal and HR)

Personal vs. Corporate Use

What are the rules of engagement? (business owned)

- Corporate policy adherence (example – appropriate use)
- Supported business use(s)
- Supported applications
- Data protection requirements (centrally enforced?)
- Personal use of device
- Exceptions?
- Business uses that are supported? (customer issues with use?)
- How will support be provided? (corporate, Apple, ?)
- What will the business purchase (Peripherals? – keyboard, etc)

Policies/Regulatory and Business Considerations

Next Generation Considerations

- More social/video capabilities and device integration
- More business applications migrated to the mobile platform
- More powerful
- More memory/storage
- Devices will supplant laptops over time (years)
- Wireless communication will continue to increase enabling more to be done over the network and faster
- MDM's will evolve to enable more control