Mobile Device Security – Is there an app for that?

Session Objectives

- The security risks associated with mobile devices.
- Current UC policies and guidelines designed to mitigate these risks.
- An approach for security management of mobile devices will be reviewed.
- A discussion of the types of mobile device security apps and software.
- Provide links to articles and websites for further review.

Scope of Session

- There are many types of devices/media that this discussion applies to:
  - Cell Phones, Smartphones, PDA, Tablets, Laptops, USB drives, external hard drives
  - IOS, Android, Blackberry OS
  - Other device/media types?
IT’S NOT THE TYPE OF DEVICE THAT MATTERS:

IT’S THE DATA AND INFORMATION
– In this session – Electronic – not paper
– MANY FORMS
• WORDS, IMAGES, VOICE
  – OTHERS?

**UC Policies and Guidelines**

• UC - IS – 3
  • ELECTRONIC INFORMATION SECURITY
    RISK ASSESSMENT
    ACCESS CONTROLS
    ENCRYPTION
    PORTABLE DEVICES AND MEDIA
    MINIMUM REQUIREMENTS FOR NETWORK CONNECTIVY

• UC – IS -2
  • INVENTORY, CLASSIFICATION AND RELEASE OF ELECTRONIC INFORMATION
    – CONFIDENTIALITY
    – INTEGRITY
    – AVAILABILITY
Mobile device management plan

- Step 1 Plan: Usage Policy
- Step 2 Plan: IT Architecture
- Step 3 Plan: Security Policy
- Step 4 Implement: IT Architecture
- Step 5 Implement: Enable Email, Contact, & Calendar
- Step 6 Implement: Enable Application Deployment
- Step 7 Implement: Enable Network Connection

Mobile device management plan

- Step 8 Manage: Regulatory Compliance Governance
- Step 9 Manage: Reports & Dashboard
- Step 10 Manage: Monitor & Audit

Plan: Usage Policy

- Define the smart device use policy. Consider the following:
  - Corporate devices Vs. employee devices
- Separation of personal Vs. corporate data on device
- Personal use or only corporate use?
  - Can you play Angry Bird on your device?
- Agreement with employee to abide with corporate security policies (e.g., remote wipe, or record of their phone calls may be viewed by corporate)
Plan: Usage Policy

- Would confidential data be allowed on smart devices and how will it be monitored and controlled?
- What type of smart devices will be allowed?
  - Apple only? Android only? Or limit by operating systems?
- How are you going to manage the backup?
- Would you want the device to connect to corporate network?
- Which apps would you like to deploy?
  - Corporate apps? Own Marketplace?

Plan - IT Architecture

- Cloud based solution vs. internally deployed
- Hosted vs. self supported
- Number of devices supported and scalability
- Changes to the current IT architecture

Plan - Security Policy

- Password Policy control
- Encryption requirements
- Port Control (WiFi, Bluetooth, camera)
- Remote lock/unlock/wipe
- Asset tracking
- Device configuration (VPN, Email, WiFi)
- Delivery and control of applications to the device
- Blacklisting/Whitelisting
- Audit and Monitoring
Deploy the IT and security architecture and provision the device.

- Provide emails of device owners to System Managers (SM)
- SM sends a self-registry link to users
- Users enter the registry information and obtain credentials
- SM downloads the security policies on the device
- Device is ready for use

Enable Email, Calendar and Contact Information on the device.

- For ActiveSync/Lotus Notes users
  - Combine ActiveSync/Lotus Notes capabilities with selected solution to implement email policies
  - Is the corporate anti-virus updated for mobile virus checks? Or should virus scan be performed by middle-server?

Enable deployment of corporate mobile applications on the device

- Typically browser-based apps are enabled
- Whitelisting/blacklisting policies are deployed?
- Authentication protocols?
Allow the device to access corporate network

- Remote Access Policy?
- VPN connection?
- Encryption policy?
- Authentication protocols?

Manage regulatory compliance and governance requirements

- HIPAA
- PCI

Manage reports and dashboard

- Executive and detailed dashboard
- Customize reports
Manage monitoring and provide audit support

• Real time vs. offline analysis
• Audit support for smart devices

Bring your own device (BYOD)

• BYOD is a concept that allows employees to utilize their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations.
• At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices.
• Management decision – Risk/Benefits/Costs

Yes there is an app for that. In fact there are many

• Good
• Airwatch
• Mobile Iron
• Sophos
Challenges

• Users’ sense of ownership over their device and resistance to “big brother”.
• Diversity of mobile device hardware and software.
• Diversity of email systems in use across the campus.

Opportunities

• Classification of systems/users with sensitive data.
• Policy guidance for what systems and data can be accessed from personal devices.
• Technical controls where appropriate and possible.
• Awareness training.
• Consolidation of IT infrastructure to increase control opportunities for mobile device access to data.

What questions should we be asking?

• Does the organization have mobile devices or media with electronic information?
• Are they aware of UC policies?
• Are they aware of campus/medical sciences policies?
• Have they performed an information risk assessment?
• Have they developed an information security plan for mobile devices?
Resources

- Securing Mobile Devices – ISACA
- 123 - IT Governance and Mobile Security – ISACA
- NIST draft 800-124 - Guidelines for Managing and Securing Mobile Devices in the Enterprise
- Balancing risks and controls in a bring your own device environment – ISACA
- 10 key considerations for Mobile Security – ISACA
- 5 considerations for choosing an MDM solution – ISACA
- Keeping Pace With Legal Requirements As Mobile Devices Inundate Offices
- 10 Mobile Device Management Apps to Take Charge of BYOD
- Tactical Mobile Device Security Measures to Meet HIPAA Compliance

Resources

- HIPAA and Mobile Device Security: An Emerging Trend for Healthcare Internal Auditors - AHIA
- Mobile device security NIST HIPAA conference May 19, 2009
- For BYOD Best Practices, Secure Data, Not Devices – CIO.com
- Critical Control 7: Wireless Device Control – SANS
- 7 Things you should know about mobile security – EDUCASE
- Stanford University Mobile Device Management

UC Websites

- UCI
  - http://www.healthaffairs.uci.edu/article/06/designDevelopment.html
- UCSD
  - http://blink.ucsd.edu/technology/security/mobile-security.html
- UCD
- UCB
  - http://security.berkeley.edu/MSPD/articles/index248.html
- UCLA
  - http://security.mednet.ucla.edu/body.cfm?id=57
- UCM
  - http://it.ucmerced.edu/support/guides-faqs/mobile-devices
- UCPA
UC Resources

- UCR
  - http://csc.ucs.edu/security/mobile.html
- UCSC
- UCSF
  - http://it.ucsf.edu/policies/recommending-mobile-device-security-strategies
  - http://it.ucsf.edu/pages/mobile-device-security-settings