

# Apple iOS in the Enterprise

Eugene Wahrlich 2011-02-10  
eugene.wahrlich@mwrinfosecurity.com

# Why is consumerisation good for business?

- Increased productivity
- Increased business continuity
- Less cost

# Business challenge

- The social and mobile trend is not going away
- Personal mobile devices are easy to lose
- Difficult to enforce security controls on personal mobile devices
- Patch management and provisioning is hard to do effectively



# Controls that mitigate device loss

- Strong passcode policy
- Failed login wipe and remote wipe
- Full disk encryption
- Staff awareness training

# How can security controls be enforced?

- Configuration profiles
  - Passcode policy
  - Certificates
  - Force encrypted backups
  - Disallow app installation and iTunes
- Contractual restrictions for staff



**General**  
Mandatory



**Passcode**  
1 Payload Configured



**Restrictions**  
1 Payload Configured



**Wi-Fi**  
Not Configured



**VPN**  
Not Configured



**Email**  
Not Configured



**Exchange ActiveSync**  
Not Configured



**LDAP**  
Not Configured



**CalDAV**  
Not Configured



**Subscribed Calendars**  
Not Configured



**CardDAV**  
Not Configured



**Web Clips**

## Passcode



- Require passcode on device**  
Enforce the use of a passcode before using the device
  - Allow simple value**  
Permit the use of repeating, ascending, and descending character sequences
  - Require alphanumeric value**  
Require passcodes to contain at least one letter
- Minimum passcode length**  
Smallest number of passcode characters allowed
- Minimum number of complex characters**  
Smallest number of non-alphanumeric characters allowed
- Maximum passcode age (1-730 days, or none)**  
Days after which passcode must be changed
- Auto-Lock (1-5 minutes, or none)**  
Device automatically locks when time period elapses
- Passcode history (1-50 passcodes, or none)**  
The number of unique passcodes required before reuse
- Grace period for device lock**  
Amount of time device can be locked without prompting for passcode on unlock
- Maximum number of failed attempts**  
Number of passcode entry attempts allowed before all data on device will be erased

# The missing security controls

- No anti-virus
- No firewall



# Why are personal mobile devices difficult to manage?

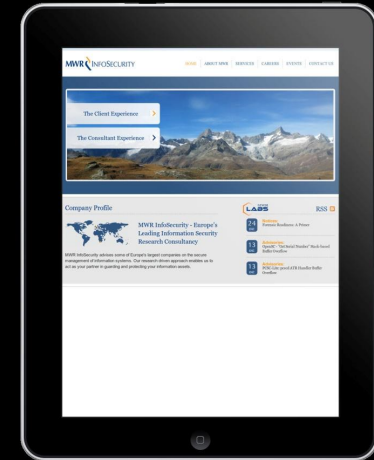
- Patching and updating can be a problem
- Keeping track of personal devices is hard
- Difficult to maintain compliance with security regulations

# Mobile Device Management

- Application whitelisting and blacklisting
- Management interface to all devices
- Easier to distribute configuration profiles
- Server-side anti-virus
- Otherwise they just provide similar functionality as the iPhone Configuration Utility

# System classification and authorisation

- Public websites
- Calendars
- Filtered email
- Email and attachments
- Intranet
- Business databases
- Shared drives
- Backups



# Case study: Intel

- 3,000 personal mobile devices used in the first month of operation
- 6,500 personal devices used in the first year
- Higher productivity
- Lower response times for emails
- Less rogue devices on their network

Source: <http://download.intel.com/it/pdf/Maintaining-Info-Security-while-Allowing-Personal-Hand-Held-Devices-in-Enterprise.pdf>



# Case study: Intel (continued)

- Why do you want to use your own devices for work?
- What would you give up to use your device for work?
- What does your personal device do that helps you work?
- Would you increase security habits for more device freedom? More paranoia please?

# Future Problems

- iOS app security is just starting to become important
- Managing many different smartphone platforms is difficult

# Summary and Conclusion

- Move with consumerisation, not against it!
- Engage your users, and find the balance between usability and security
- With the right controls and management processes, iOS devices can be used for *some* purposes whilst managing the risk.