

enterprise risk management

The Control Professionals

Mobile Device Security

January 2011

About ERM



About the presenter



Mobile Devices



Some interesting info

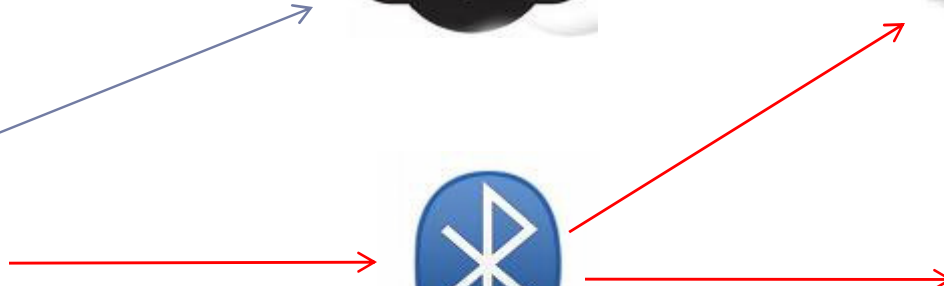
- ▶ *11% of current mobile phones are smartphones*
 - ▶ *25% by 2012*
- ▶ *Apple's iPhone currently owns 16.4% of the smartphone market*
- ▶ *Leader Nokia controls 38.2% of the global market*
- ▶ *BlackBerry-maker Research in Motion (RIM) accounts for 19.7%*
- ▶ *iPhone, BlackBerry, HD2 and Google Nexus One can all connect to a corporate Exchange server*
- ▶ *I can use my BlackBerry as a modem*
- ▶ *Life changing !!!*
 - ▶ *Personal Device*



It can do a lot of stuff!!



Laptop/Netbook



Smartphone



Smartphone

- ▶ Mobile phone offering advanced capabilities
 - ▶ PC-like functionality
 - ▶ Integrates the functionality of a mobile phone, personal digital assistant (PDA) or other information appliance
 - ▶ Provides additional information accessing features
 - ▶ Essentially a ***computer in your pocket***



Some Facts

- ▶ *Storing personal data on smartphones without thinking through the consequences should that device get lost or stolen.*
- ▶ *7/10 devices will contain email exchanges, more than half social media data, one in five some information relating to online purchases, and one in six might even point to online banking websites.*
- ▶ *Essentially carrying around a tiny device with a wealth of personal information.*



Considerations. . .



PHYSICAL SECURITY



Controls

- ▶ *Laptops/Netbooks*

- ▶ *Treat the devices as if they were your suitcase*
- ▶ *Password protection*
- ▶ *Encrypt the file-system*

- ▶ *Smartphones*

- ▶ *Treat the devices as if they were your wallet*
 - ▶ *Don't put too much information on them and there is not a problem*
 - ▶ *Keep as little info as possible, password or PIN protect each device, and use encryption wherever possible for data on add-on data cards*
 - ▶ *Do not automatically store any website logins*
 - ▶ *Don't make information too obvious (i.e. "Home"=home)*
-



Considerations. . .



VIRUS / MALWARE



Harder than PC but still possible

- ▶ Mobiles have proved so much harder to attack via virus than PCs
 - ▶ The Apple iPhone uses a locked-down system of application approval
 - ▶ Mobile malware can be used to record phone calls
- ▶ Many platforms
 - ▶ Bad guy has to work harder
 - Overcoming not one platform (as with the PC) but several
 - Each distinct in terms of what is and is not possible.



Controls

- ▶ *Antivirus*
- ▶ *Firewall*
- ▶ *Malware Scanner*
- ▶ *Latest and Greatest Patches*
- ▶ *Follow the security configuration standards*
 - ▶ *Or create one...*



Considerations. . .



DATA TRANSMISSION and Wi Fi





Regarding WiFi

- ▶ **Nothing Is Private on Open Wi-Fi**
 - ▶ On unencrypted wireless networks, everyone can see where you are surfing
 - ▶ On encrypted wireless networks, everyone with the password can see where you are surfing
 - ▶ WEP is not safe; WPA is not bullet-proof
 - ▶ The danger is the public access point. The risk is being on someone's network that you don't control

- ▶ **Paid Hotspots: Security Not Included**
 - ▶ Common misconception that whatever requires password is secure



Controls

- ▶ *Don't allow wireless card to connect automatically to any available network*
- ▶ *Connect to an available network with caution and common sense*
- ▶ *Turn off your wireless access, if not needed*
- ▶ *Turn-off any file-sharing when browsing WiFi*
- ▶ *Stick to SSL for webmail for the ENTIRE SESSION*
 - ▶ *Email clients only if they use encrypted protocols*



Considerations. . .



STORING PERSONAL DATA

CONFIDENTIAL



Controls

- ▶ *Password or PIN protect your device*
- ▶ *Enable lockout or timeout of sessions*
- ▶ *If personal*
 - ▶ *Do not store anything that you cant live without if you lose it*
 - ▶ *Try to encrypt anything sensitive*
- ▶ *If corporate*
 - ▶ *Ensure on the policies and procedures addressing storing and utilizing sensitive data*
 - ▶ *Utilize devices that can enforce encryption*
- ▶ *Sanitize*



Considerations. . .



BLUETOOTH



Here is how easy it is



- ▶ **Step 1.** You should have a handset that supports JAVA MIDP-2 and has Bluetooth connectivity to use the Magic Blue Hack software. It is a free software available from getjar.com.
- ▶ **Step 2.** Download the software and install it in your mobile.
- ▶ **Step 3.** There is no need to install the software in the mobile which you want to hack.
- ▶ **Step 4.** Turn on the bluetooth of your handset and run the MagicBlueHack from your mobile.
- ▶ **Step 5.** Select the connect option from the menu. It will then search the bluetooth devices around. The Bluetooth of your friend's mobile should also be turned on to be found.
- ▶ **Step 6.** Select the device to be hacked and it may ask for permission to start Bluetooth service with another. You may also need to be paired with the devices and exchange passkeys.
- ▶ **Step 7.** After the connection is established you can make calls to any desired number and also send text messages via the hacked number. The charges will be applicable to the hacked mobile.
- ▶ **Step 8.** Enter the destination phone number in the number box and select the make call option from menu. It will then make call from the connected device to your destination number. It will happen without notifying the owner of the connected device.
- ▶ **Step 9.** You can also receive any call of that hacked device by pressing the answer call option.
- ▶ **Step 10.** To send text SMS you have to enter the destination number in the box and type in the text in the SMS Text Box and select send SMS option from the menu. You'll not be charged for the SMS but the hacked device will be.



Controls

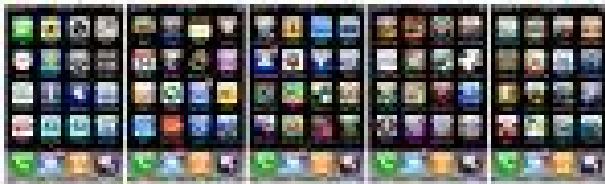
- ▶ *Lock down Bluetooth.*
 - ▶ *By default, Bluetooth is on*
 - ▶ *Set Discoverable to No*
 - ▶ *Set Security to High—or if device supports it add Encryption*
 - ▶ *Disable any unnecessary services*



Considerations . . .



APPLICATIONS



Did you know

- ▶ The iPhone can be exploited in under 5 minutes !!
- ▶ ***Applications are a weak link!***
- ▶ iPhone / iPad
 - ▶ SAFARI
 - ▶ Quicktime
- ▶ Hack into your BlackBerry under 3 minutes !!!



Jail-Breaking the Iphone

- ▶ ***Jail-breaking***

- ▶ Unlocking
- ▶ Process used to open the software of an iPhone or iPod touch
- ▶ Allows the user greater access to the device to install software and make changes to it

- ▶ **Apple tightly controls its iPod and iPhone products.**

- ▶ This control extends to preventing users from installing some kinds of software or making deep, system-level changes to the devices
- ▶ Rationale for this is that preventing these changes ensures that the device operate smoothly, with fewer errors, and provide a high-quality experience

- ▶ **The opposing view**

- ▶ Apple is denying users the freedom to use their belongings the way they'd like
- ▶ Trying to control what gets installed on the devices





Prone to Security Issues

- ▶ A new worm is targeting jailbroken iPhones and adding them to a mobile botnet
 - ▶ The worm starts off scanning local networks for jailbroken iPhones that have installed Secure Shell (SSH) and that haven't changed their default password
 - ▶ If the worm finds an unprotected iPhone, it will copy itself onto the device and add it to its botnet
 - ▶ The worm changes the device's password and thus prevents users from changing the password themselves
 - ▶ Connects all infected devices to a central server in Lithuania that directs them to participate in
 - ▶ Distributed denial-of-service attacks
 - ▶ Send spam
 - ▶ Deliver malware to other machines
- ▶ "iBotnet.A"
 - ▶ Third major piece of iPhone-centric malware over the last month
 - ▶ The first iPhone worm was a fairly innocuous piece of malware that replaced the iPhone's regular homescreen with Rick Astley wallpaper
 - ▶ The second piece of malware harvested personal data from iPhones
 - ▶ Including user email, contacts, SMS messages, calendars and multimedia files.



Controls

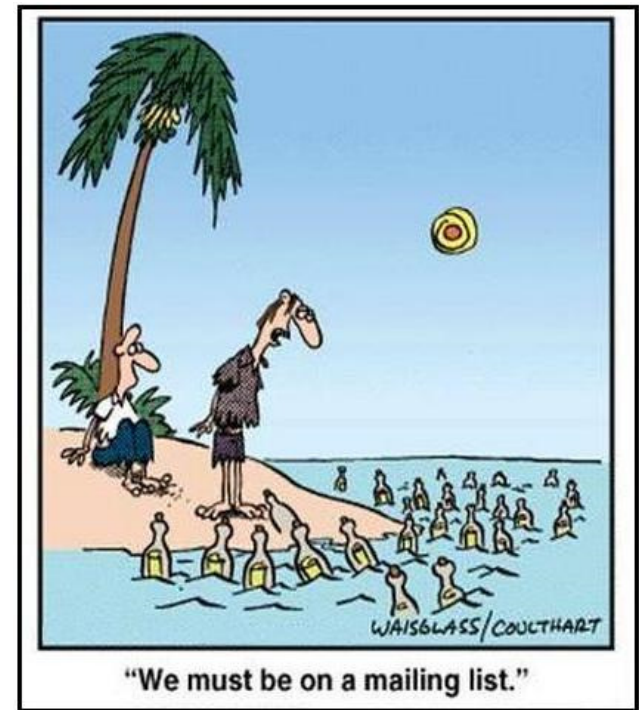
- ▶ *Understand the implications of “freeing up” a device*
- ▶ *Do not install any applications that you do not really need*
- ▶ *Make sure you know where is the application coming from*
- ▶ *Have security protection applications on your devices*
- ▶ *Do not forget or ignore the security patches being available*
- ▶ *Encrypt any sensitive data*



Considerations. . .



SPAM



Did you know?

- ▶ Spam has grown exponentially in Asia
 - ▶ United States and Europe are expected to experience a similar problem in the next 18 months
- ▶ Could even be a lot worse than what we've seen on PCs
 - ▶ SMS
 - ▶ MMS
 - ▶ WiFi
 - ▶ Bluetooth
- ▶ Increased risk since you have to open the text message



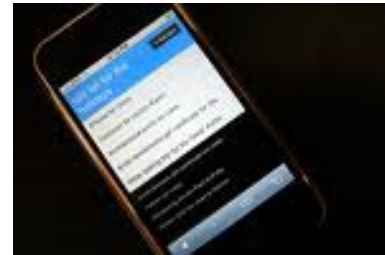
Controls

- ▶ *Install an SMS filter or a security application that includes filtering*
- ▶ *Never reply to spam-mail*
- ▶ *Do not leave your mail-address on each and every site you visit*
 - ▶ *Create a new e-mail-address which you use solely for this purpose*
- ▶ *Beware of unknown senders*
- ▶ *Share your number cautiously*



Is there a single list of the basics?

- ▶ *Use a password*
- ▶ *Use a firewall*
- ▶ *Use VPN or encrypted login sessions*
- ▶ *Don't visit any sites you wouldn't visit on a public terminal*
- ▶ *Use validated/certified and safe applications*
- ▶ *Do not discard security*
- ▶ *Understand what you store*
- ▶ *Use encryption on sensitive data*
- ▶ *Wipe prior to tossing*
- ▶ *Use common sense*



What about the Corporate Environment



- ▶ *Establish and enforce strong authentication policies for devices trying to access corporate networks*
- ▶ *Require employees to use a corporate VPN and encryption when handling sensitive data*
- ▶ *Devices and software applications are configured as per configuration standards*
- ▶ *Corporate security policies prevent workers from transferring sensitive data to mobile devices or unauthorized computers*
- ▶ *For laptops/netbooks consider air cards, which require a service plan, instead of hot spots for wireless connections*
- ▶ *Establish ground rules for the use of devices like the iPad, and develop policies and procedures that take the security limitations of the device into consideration and adequately protect sensitive business data*



What about the Corporate Environment

- ▶ *Perform Risk and Security Assessments on your mobile devices*
- ▶ *Set resource controls*
- ▶ *Provide Security Awareness and Training*
- ▶ *Eliminate any unnecessary services and gizmos*



So Summarizing. . .

- ▶ You need to protect against the following:
- ▶ *Physical Breaches*
- ▶ *Virus and Malware*
- ▶ *Unprotected WiFi and Data Transmissions*
- ▶ *Sensitive Data Compromise*
- ▶ *BlueTooth*
- ▶ *Applications*
- ▶ *Spam*



Keep your Mobile happy

