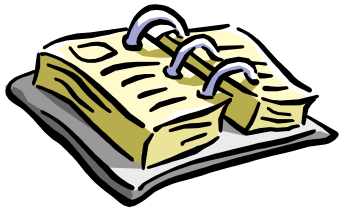
Handheld Computing Device Security Management Overview

Last updated August 10, 2004

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Information Privacy, Security and Compliance
rebeccaherold@rebeccaherold.com
515-491-1564

Agenda



- Purpose of Presentation
- What, me worry? (intro)
- Security Issues
- Security Tools
- Example Policies
- Example Discovery Tasks
- What, me worry? (more real life stuff)

Purpose

- Discuss why you as leaders should be concerned
- Provide overview of primary security issues
- Provide example policies and discovery tasks
- **NOT** a **technical** discussion of handheld device technologies or **how** to hack them!

What, Me Worry?

The loss of mobile computing devices is the number three most common security mishap according to recent 800 person survey July 2, 2004, Jupiter Research

"Overall worldwide mobile device market in Q1 2004 up 41% on Q1 2003; Smart/feature phone segment up 115%"
June 10, 2004, Canalys Research

By 2007 there will be nearly 120,000 WLAN "hot spot" gateways worldwide, providing access to private and public networks for over 200 million mobile devices used in business. More than 60% of staff in Global 2000 companies will have mobile access to corporate applications from mobile devices, & 40% of corporate data will reside on handheld devices by 2005. Feb, 2004, Gartner

An additional 2,000 PDAs (total to 3,000) will be distributed to Medicaid physicians by the Florida Agency for Health Care Administration. Aug. 10, 2004, Tampa Bay Journal

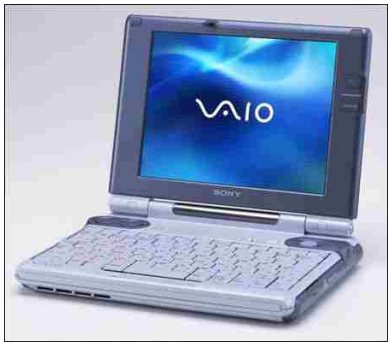
"There are now more mobile devices that connect to the Internet than laptops and PCs" CSI NetSec 23 June 2003, Steve Schall, Nokia

"PDA theft troubles wireless network managers"
26 Feb 2003, SearchNetworking.com

IRS personnel lost 2300 laptops according to August 2002 U.S. GAO report
More stories later…

What are Handheld Devices? (1)

- Pocket PCs/PDAs/etc.
- Smartphones & cellphones
- Pagers
- Laptops (sometimes)
- Notebooks, Subnotebooks & Ultra-Subnotebooks



PalmOne's Zire 72 includes a 1.3-megapixel digital camera.

What are Handheld Devices? (2)

All-in-one devices; e.g., NTT ToCoMo

"Hiptops"; e.g., T-Mobile's Sidekick II

Security Issues

- Theft or loss
- Passwords
- File access
- Viruses & other malicious software
- Unauthorized network access
- Wireless concerns
- Network bandwidth
- Device retrieval
- Device disposal
- Personal Device Ownership

Security Issues – Theft or Loss

- According to Gartner Group, **currently** the biggest threat to a handheld device is losing it, or having it stolen
- Increasingly more handhelds are showing up in lost and found areas
- Increasingly more are being reported stolen (FBI sources)

Security Issues – Theft or Loss

- The Washington D.C. Metro collected 25,700 computing items on its Metrorail system, 2,200 items in city taxicabs, and 8,200 items on Metrobuses in 2000. - *The Washington Post, Jan. 2001*
- 74 cell phones and 96 laptops were recovered at Denver International Airport's security checkpoints over two weeks alone from 1/28/02 to 2/11/02 - *USA Today, Feb., 2002*
- ~62,000 cell phones, 2900+ laptops and 1300+ handhelds were found in London taxis between March and August 2001. – *BBC, August 2001 report*

Security Issues – Theft or Loss

- eMarketer, June 8, 2004: The number of mobile devices shipped worldwide increased by 41% between Q1 2003 and Q1 2004. Motorola's shipments increased dramatically - from just 2,440 devices in Q1 of last year to 313,2480 this year, an increase of 12,748%
- Andersen Consulting, 10/25/2001: 10%-15% of handhelds and cellphones are lost or stolen; estimated average value of information on each is $10,000 - $20,000
- NOTE: There are cable and lock systems that hook into PDA stylus slots, such as the Kensington Technology Group's "PDA Saver". However, the devices aren't universal because of differing stylus designs
- July, 2001: 112 cellphones were found on United airlines planes in the O'Hare airport alone
- Federation of Communication Services, 06/07/2001: Over 15,000 mobile phones are stolen each month in the UK alone

Security Issues - Theft or Loss

Not many options...

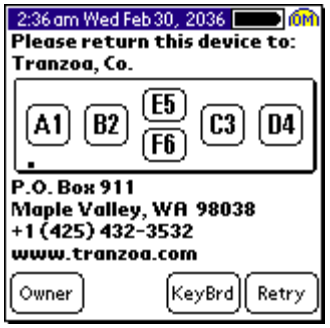
- http://www.force.com/

  Neck straps, security chains, etc.

Security Issues – Passwords

- Many (probably most) people do not use the password feature
- Using the password helps to protect data AND discourage would-be thieves
- Doing a hard reset on most devices, however, allows a hacker to remove the password
- Password Keepers also becoming popular to use on handhelds
- @stake: Handheld passwords almost always the same as the user's network passwords

Security Issues - Passwords



Just a few possibilities…

- http://www.tranzoa.com
  - OnlyMe
- http://www.cic.com
  - Sign-On
- http://www.goati.com
  - ForeverSecure; PDASecure; etc.

Security Issues – File Access

Attacks occur related to synchronization issues:

- Leaving desktop workstations on and unprotected when a user is out of the office
- Centralized backup and restoration of mission-critical data•
- Restricting access to particular types of data based on job function•
- Establishing an electronic "paper trail" (audit feature) that details what data was retrieved and by whom
- Related issue: sync issues impact integrity

Security Issues – File Access

- Software tools enable hackers with or without physical possession of a Palm to import password-protected files to a file viewer
- Sensitive business and work-related information is often stored on handhelds
- Users are **not** encrypting the files, and do **not** use access controls
- Can extract data from handhelds by reading "raw memory" or from host system backup files

Security Issues - File Access

Just a few possibilities…

- http://www.iscomplete.org
  - Restrictor
- http://www.electricpocket.com
  - Enforcer

Security Issues - Viruses

- Viruses & malicious code have started infecting PDAs (eg., Palm_Liberty.A trojan, erases all data on Palm; Phage.936, Vapor, etc.)
- Aug 6, 2004: Both Symantec and Kaspersky Labs have detected a backdoor Trojan horse program, Brador, that can give an attacker complete control over a Pocket PC mobile device.
- If a virus resides on a Palm OS, and users sync the PDA with desktops, they can easily transfer a virus or worm into a corporate network, where it can do significant damage.

Security Issues - Viruses

- September 2001: Cellphones in Japan hit by "malicious email spamming virus."
- Summer 2001: Timofonica spammed thousands of cellphones in Spain
- Existing desktop anti-virus products aren't designed to look for or block Palm OS-based viruses or worms
- Virus signature updates may not be automated for handhelds; claims to otherwise:
    - Symantec AntiVirus for Palm OS
    - F-Secure & Fujitsu Siemens for PocketPC
    - McAfee VirusScan for Handhelds

Security Issues - Viruses

Just a few possibilities…

- http://www.dataviz.com
  - DocumentsToGo
- http://www.cesinc.com
  - Quickoffice
- http://www.mcafee.com
- http://www.symantec.com
- http://www.finjan.com

Security Issues – Unauthorized Network Access

- Many (or most) handhelds are configured to connect to their corporate networks
- Handhelds usually authenticate as if they were the end-user…stealing information authorized to the end-user, and even the end-user's identity, is **VERY** possible
- Handheld users often use the same passwords for their network access, exposing the corporate LAN from the Palm Pilot.

Security Issues – Unauthorized Network Access

- Can easily copy files, including password list files (eg., .pwl) and certificate files (eg., .pfx)…there are many hacker tools available to do this
- As handheld sales increase, so do the number of connections to corp networks, increasing risks of security breaches
- May need to reconfigure firewalls if wireless connections are allowed. Install firewalls at APs.

Security Issues – Unauthorized Network Access

- Palm's debugging program can be exploited by anyone; the Palm OS developer's manual is online (NOTE: Debug vulnerability closed in v4.0)
- The program is installed on all devices, and is designed to be used only by application developers and technical support; however, it is EASY for anyone to access.

Security Issues – Unauthorized Network Access

- The debugging program in many handhelds allows anyone to type in commands such as 'coldboot' to wipe all data from the device, or 'export' to copy everything onto another computer.
- The program can also be used to access a user's Palm password.
- "An attacker can copy the contents of the average Palm in about five minutes and decrypt a password in a few seconds. " (Network News, March 2001)

Security Issues – Unauthorized Network Access

Just a few possibilities…

- http://www.sage-inc.com
  - Brickserver
- http://www.vaultus.com
  - Mobile Platform
- http://www.carraigltd.co.uk
  - Carraig Secure Data

Security Issues – Wireless Concerns

- Eavesdropping on connections is a REAL possibility.
- Perhaps less likely with infrared protocols, but this is changing. Such protocols are defeatable, and once a hacker accesses the transmission, they have access to everything to which the user has access.
- Wireless devices connections are also vulnerable because typically they're immediately connected to the user's network.

Security Issues – Wireless Concerns

- Device cloning
- Denial of Service attacks
- War Driving: Using sniffer programs to find WLAN nodes, wireless handhelds, etc.
- Jan 2002 Information Security poll: 90% of 1,268 participants are concerned about wireless networking
- May 29, 2002 CISSPforum posting: Aerial wireless audit in "metropolitan area" at 3000 ft. found 382 APs, 91 APs used default SSIDs, 92 AP had WEP

Security Issues – Wireless Concerns

- Software code exists that can zap passwords off targeted Palm Pilots through the PDA's hotsync function. (Hotsync is used to transfer data between the user's PC and a Palm Pilot.)
  - Called Notsync, the code fools the targeted Palm Pilot into thinking it is talking to the user's desktop computer, rather than a hacker's PDA.
  - The hacker then downloads the target's password via the target machine's infrared port.
- Instant messaging applications are easy to intercept and to spoof
- "Beaming" is popular way for PDA users to share information and games

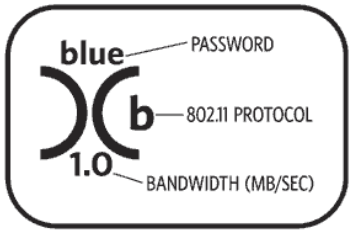
Security Issues – Wireless Concerns

- Texas A&M University, 2001: Implemented WLAN over 120 acres using wireless VPN; anyone using a handheld in area with a wireless node is routed to a VPN server.
- "Hot spots": public wireless access points. Eg., in airports, NOT secure, data is probably in clear & handhelds subject to attack
- Symantec 2002: "You may get a virus just by walking next to somebody who has an infected device, depending on the susceptibility of your device."

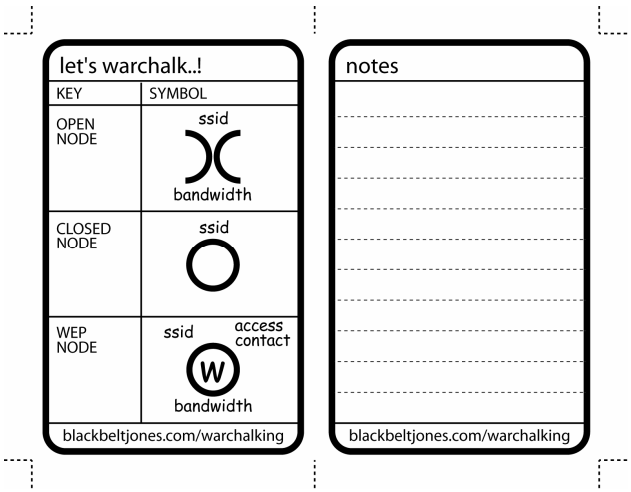
Security Issues – Wireless Concerns

- MAC address will let the hacker using your handheld into your network
- Peter Shipley stats: in 2001, San Fran bay area, found 9000+ APs, 60% in default config, most connected to backbone network NOT DMZ, most did not use WEP, ½ of those using WEP used the default encryption key

Security Issues – Wireless Concerns



- "War chalking": http://www.warchalking.org/
- PriceWaterhouseCoopers:
  - Over 10 million new wireless LAN/PC connections were installed in 2002
  - Over 30 million Bluetooth chipsets shipped in 2002



Security Issues – Network Bandwidth

- There have been reported wireless network crashes as the extra data traffic generated by the devices causes bandwidth overload.
- DOS attacks via wireless expected to increase dramatically
- Story of insurance company giving 600 agents handhelds as "prizes"

Security Issues – Device Retrieval

How will you get the PDAs with mission critical information back during:

- Strikes
- Layoffs
- Dismissals
- Job transfers

Address this in your asset management program!!

Security Issues – Device Disposal

What do you do with your device when you no longer need/want to use it?

- Physically destroy
- Remove memory and storage chips and cards

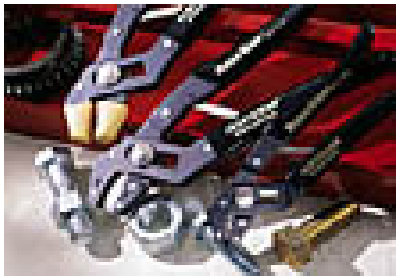
Address this in your asset management program!!

PalmOne's Zire 72 includes a 1.3-megapixel digital camera.

Security Issues – Personal Device Ownership

- Moves control away from company and into the hands of the employee
- Conflict of interest can arise
- Potential for multiple, unsecured, connections
- Support issues
- Inappropriate use and potential legal actions with disgruntled users

Security Tools



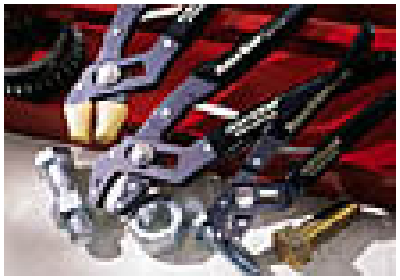
For Palm OS:

A few options include the following:

- PDA Defense
- JAWZDataGator v2.1.1
- Handango Security Suite
- Memo Safe
- PalmSafe
- TopSecret
- BSAFE Encryption and SecurID
- Security Toolkit for Palm™

* Pocket Blue
* OnlyMe
* TealLock
* JotLoc
* PDABomb
* eWallet
* The Safe

Security Tools



For RIM (Blackberry):

A few options include the following:

- **PocketBlue**
- **PDA Defense**
- **Handango Security Suite**
- **Blackberry Enterprise Server**

Security Tools

For Windows CE (now PocketPC):

Some options include:

- PocketLock
- Handango Security Suite
- Multipass (MIPS)
- CryptoGrapher
- Sentry 2020/CE
- Pocket CodedDrag
- CodeWallet
- CypherCE
- eWallet
- PocketSafe
- The Safe

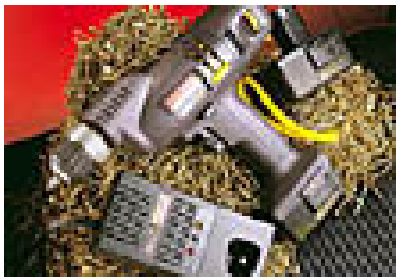
Security Tools

For Psion:

Some options include:

- **Clock5**
- **Password 1.00**

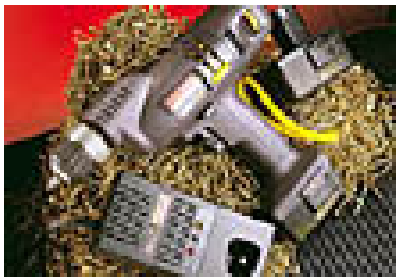
Security Tools



Just a few web Sites for more information:

- **http://www.handango.com/**
- **http://www.palmgear.com/**
- **http://www.pdabomb.com/**
- **http://flashnet.pda.tucows.com/palm/util_security.html**
- **http://www.protectdatasecurity.com/**
- **http://www.fieldsoftware.com/PrintPocketCE.htm**
- **http://www.clicklite.com**
- **http://www.intel.com/museum/25znniv/hof/moore.htm**
- **http://www.pointinception.com/product/?id=2**

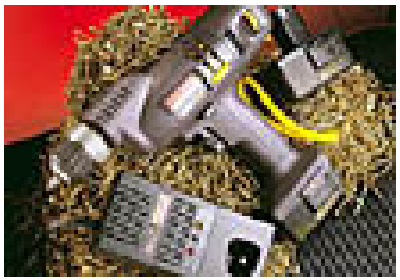
Security Tools



Just a few web Sites for more information:

- http://www.jkware.com/palm/palm.html#PC
- http://www.palmix.itil.com/newpalmix/products/sword_home.htm
- http://www.softwinter.com/sentry_ce.html
- http://www.sbm.nu/englisch/windowsce/thesafe/docu/readme.htm
- http://www.rsasecurity.com/
- http://www.certicom.com
- http://www.ntru.com

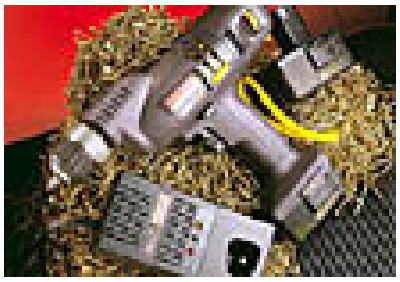
Security Tools



Just a few web Sites for more information:

- www.cisco.com VPN gateways for PDA VPN clients
- www.freewarepalm.com Data encryption
- www.certicom.com VPN clients for PDAs
- www.mobilecloak.com Electromagnetic shielding bag
- www.dentonsoftware.com Secure databases and authentication solutions
- www.f-secure.com Anti-virus, encryption, and authentication solutions
- www.asolutions.com Hotsync security and IrDa port security, database
- www.pointsec.com Encryption and authentication solutions
- www.paraben-forensics.com PDA forensics tools
- www.trustdigital.com Password protection, hotsync protection, data encryption, bit wiping, VPN client

Security Tools



Web Sites for Handheld Anti-Virus Software:

- http://www3.ca.com/Solutions/Product.asp?ID=171
- http://www.mcafeeb2b.com/products/virusscan-wireless/default.asp
- http://palmtops.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.f-secure.com%2Fpalm%2F
- http://www.symantec.com/sav/
- http://www.antivirus.com/free_tools/wireless

Other Issues…

- Organizations risk not only security breaches, but overspending and inefficient working practices
- Jeopardy of legal non-compliance (e.g., HIPAA, GLB, etc.)
  - 2002 healthcare survey: 78% of physicians using handhelds for personal, clinical, and/or business functions
- Organizations must establish policies, regulations and standards for handheld users

Other Issues…

- Review the security features of possible handhelds
- Identify those handhelds acceptable for your organizational use
- Require handheld users to implement the security features
- Create procedures to ensure compliance
- **COMMUNICATE** the policies and procedures to all personnel
- Perform audits…THOROUGHLY…to determine all handhelds used within your organization

Start with a Risk Analysis (1)

- Identify your risks
- Identify levels of security necessary to address the risks
- Base technical designs and policies upon results

Start with a Risk Analysis (2)

A few of the questions to consider:

- What information is on the handhelds?
- What legal requirements apply for the information?
- How do the handhelds interface with the network infrastructure?
- How is the information protected?
- How is the device protected?
- Who owns the handhelds; the company or the individual?

Policies - Handhelds

May 2002 Pointsec Mobile Technologies & Infosecurity Europe survey :

- 2/3 of orgs have NO handheld security guidelines
- Most handheld users download everything to their handhelds, including PINs, passwords, customer files, etc. and over 71% do NOT encrypt
- 89% use handhelds as business diary
- 67% of orgs provide workers with handhelds, but give no training or usage guidelines

Example Policies – Handheld Devices

1. The installation and use of synchronization software from corporate systems to and from handhelds must be approved by management prior to use. (Consider requiring a specific IT team to install such software)

2. Handhelds containing business information must be physically secure when left unattended. (Tell your users how in documented procedures.)

3. If business information is stored on the handheld, access controls and encryption must be employed. (Provide procedures for acceptable controls)

Example Policies – Handheld Devices

4. Employees must back-up data, using an approved corporate method, on a regular basis to avoid loss of valuable corporate information. (Syncing is one way to accomplish)
5. Handhelds used in the course of corporate business are subject to audits just like any other electronic device, even if employee-owned.
6. Handhelds must use centralized synchronization on the corporate network. Local synchronization is not allowed.

Example Policies – Handheld Devices

7. All handhelds owned by the organization must display ownership information and login banner upon start-up. Information to be displayed includes the following:
   - User name
   - Organization name
   - Business address
   - Business phone
   - Approved login notice regarding ownership and monitoring

Example Policies – Handheld Devices

8. Power-on passwords must be used on all handhelds containing corporate information.
9. Passwords must be used to enable data transfers to and from the corporate network and the handheld.
10. Handheld passwords must comply with corporate password policies.

Example Policies – Handheld Devices

11. Network systems passwords (for example, Outlook, Netware, NT, etc.) are **not** allowed to be stored on handhelds.
12. Handhelds must be configured to automatically power off following a maximum of 10 minutes of inactivity (less time is recommended.) A password must be required to re-establish access with the handheld.
13. Individuals are not allowed to share handhelds or handheld passwords.

Example Policies – Handheld Devices

14. Handheld passwords must be different than other passwords used on the corporate network.
15. Handhelds are not allowed to connect to non-corporate networks (such as the Internet) simultaneously while connected to the corporate network.

Example Policies – Handheld Devices

16. Files loaded onto handhelds must be in PDF format (this prevents corrupting files and data).
17. Specify the applications that CANNOT be used on handhelds.
18. Handheld devices that are lost or stolen, or belong to terminated personnel, must be immediately locked out from network access.

Example Policies – Handheld Devices

19. Allow only certain classification(s) of data to be accessible by handhelds (this requires that you have a data classification process in place).
20. Require the use of dynamic (single-use) passwords for handhelds. (eg., via tokens, etc.)
21. Require the use of personal firewalls on handhelds (e.g., PDA Defense)
    http://ipw.internet.com/protection/security/998941225.html

Example Policies – Handheld Devices

22. Disallow handhelds to be used in wireless modes. (Determine feasibility based upon your business and environment.)
23. Require wireless transmission from handhelds to be encrypted. (Accomplish using VPNs, etc.)
24. Only handhelds provided and configured by your organization can be used to process and/or access corporate information.

Example Policies – Handheld Devices

25. All handhelds used must be approved by the CISO. (Again, determine feasibility based upon your organization, industry, etc.)
26. Information about all handhelds used must be maintained in a central inventory within Info Security. Inventory info must include person's name, title, department, phone number, manager, and handheld model and serial number.

Example Policies – Handheld Devices

27. All handhelds must be covered by the corporate-approved handheld insurance. (Important for large-scale use, and very mobile users.) E.g.,

    http://www.e-insurancedirectory.com/cusc.php (UK)

    http://www.thesignal.com/ (US)

28. Each handheld must have a corporate security tracking tag attached.

    E.g., http://www.stoptheft.com; http://www.stuffback.com

Example Policies – Handheld Devices

29. All wireless APs must utilize firewalls.
30. All wireless APs must be approved by Info Sec prior to installation.
31. All wireless APs must be documented and reviewed regularly for accuracy by Info Sec.

Example Policies – Handheld Devices

32. All handheld computers must be physically destroyed when they are no longer used for business processing.

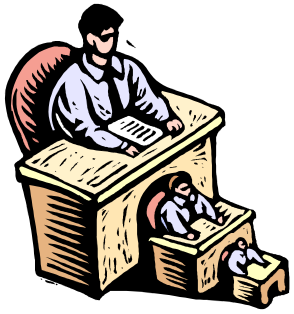
33. The memory chips and storage cards in handheld computers must be removed before disposal.

Example Policies – Handheld Devices

34. Handheld devices must not be donated to external organizations when they are no longer needed for business processing.

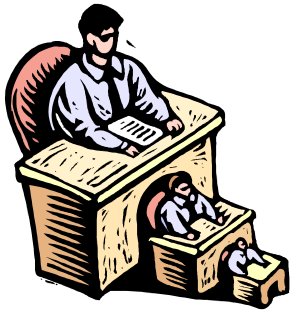
35. Non-employees and visitors to facilities with sensitive and mission critical information must check their handheld devices and cell phones with the security guard.

Policy Considerations



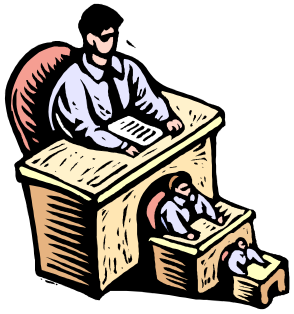
- Your industry…and the information you process and/or handle
- Applicable laws and regulations
- The classification of information you are **ALLOWING** to be processed on handhelds

Handheld Discovery Reviews



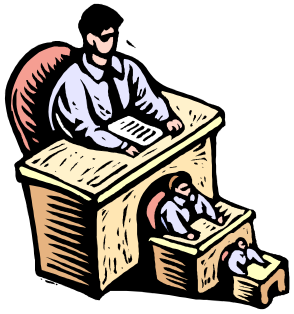
- Management questionnaire
- Physical review
- Software inventory/discovery utilities
  - E.g., Network Audit Toolkit; http://www.sofotex.com/download/software/5113.html
- Checks if device settings are in compliance. If not, utilities can do any of the following:
  - Automatically change the settings to be in compliance.
  - Prevent the device from functioning until its settings are in compliance.
  - Send a message using e-mail or Short Message Service (SMS) to management, highlighting the policy violations.
  - Wipe all sensitive data off the device.

Handheld Discovery Reviews



- Monitor and discover access points (APs) E.g.,
  - Netstumbler; http://www.netstumbler.com
  - IBM's Distributed Wireless Security Auditor
    http://www.ibm.com/news/us/2002/06/172.html
  - AirDefense Inc.
    http://www.airdefense.net/

Handheld Discovery Reviews



- Facilities entrance check
- Acquisitions review
- Systems log reviews
- Inventory reviews

Internet Resources

- Mail lists:
  - Pocket PC Wire –

    http://e-newsletters.internet.com/cewire.html
  - Palm Boulevard – http://e-newsletters.internet.com/palmb.html
  - RIM Road – http://e-newsletters.internet.com/rimroad.html
  - Psion Place – http://e-newsletters.internet.com/psionp.html
  - Visor Village - http://e-newsletters.internet.com/visorv.html

Internet Resources

- Web sites:
  - http://www.pdastreet.com/
  - http://searchWireless.techtarget.com
  - http://www.memoware.com/
  - http://www.pdasupport.com/
  - http://www.idstrip.com/
  - http://rr.sans.org/PDAs/PDAs_list.php
  - http://www.netstumbler.com

What, Me Worry?

Gartner, January 2002:

Estimates over 250,000 cell phones and handhelds will be lost at airports alone this year. "The actual cost of hardware replacement is negligible compared to the potential liability for compromised sensitive data."

What, Me Worry?

- Since 1996 when Palm Pilot was introduced, over 9 million PDAs were sold by the end of 2000…a large majority to professional people to use for work
- The Consumer Electronics Association estimates 6.1 million handheld units were sold in 2000, representing a 50% increase over 1999
- Over 75,000 people received handhelds for Christmas in 2000.
- *TRIVIA: Do you know what is generally considered the first handheld device?*

What, Me Worry?

- (Summer 2001) Datacomm Research projects that by end of 2003 three hundred and fifty **million** units will have been shipped in the shape of either a smartphone (90%) or a handheld computer (10%)
- (Summer 2001) Data Corp projects that 19 million handhelds and 13 million smartphones will be sold in 2003 alone

What, Me Worry?

- In-Stat Group (10-25-2001): 6 million PDAs were sold in 2001; 11 million will be in 2002
- 10-23-2001 Reuters: Around 150 crew members on the Navy destroyer USS McFaul, stationed on the coast closest to Afghanistan, have and use handhelds for communications (personal and military); focus in report was on physical security.

What, Me Worry?

- Strategy Analytics (2002) predicts global handheld revenue will increase 500% by 2006, as unit shipments surpass 85 million units
- Fall 2001, Forrester: 66%of survey respondents indicate employees select their handhelds; but 72% indicate the company will choose within two years
- The time to do something about handheld use in your organization was months ago!!

What, Me Worry?

- Dec. 2001: MA State Troopers used Blackberries at Boston's Logan airport to improve physical security, conducting background checks in less than 1 minute; bad native security, but they are using Pocket Blue software for full encryption.
- June 2002 Gartner: 2 million people use wireless today; expect this number to double by next year.

What, Me Worry?

- June 2002 Int'l Data Corp: Currently 3000 public "hot spots" (high speed Internet access points); project to grow to 40,000 by 2006.
- June 10, 2002, Newsweek: Peter Shipley stats…1/2 of 200+ networks found in Berkeley area were unprotected by encryption or access controls; unnamed source in Omaha, NE recently found 59 hot spots, with 37 unprotected.

What, Me Worry?

Handhelds Have Cool Benefits!

- Portable
- Inexpensive
- Easy to use
- Wireless Capabilities

Accompanied by inherent risks…

See above list

What, Me Worry?

- Remember…people consider these as PERSONAL digital assistants, and most believe they can do whatever they want with them, whenever and wherever they want.
- Are your personnel already using handhelds for work? How do you know????
- Do your contractors or consultants store your company's information their handhelds? How do you know????
- What work-related information are personnel storing on their handhelds? How do you know????

Handheld Computing Device Security Management Overview

Last updated August 10, 2004

Rebecca Herold, CISSP, CISA, CISM FLMI
Information Privacy, Security and Compliance
rebeccaherold@rebeccaherold.com
515-491-1564