Mobile Insecurity: A Practical Guide to Threats & Vulnerabilities

Scott Schelle

Chief Operating Officer, scott@bluefiresecurity.com

Bluefire Security Technologies

Situation:
Handhelds are available in 3 categories

Data Centric → Voice Centric

PDA

- Pen input
- Wi-Fi, Bluetooth
- PIM
- Light applications

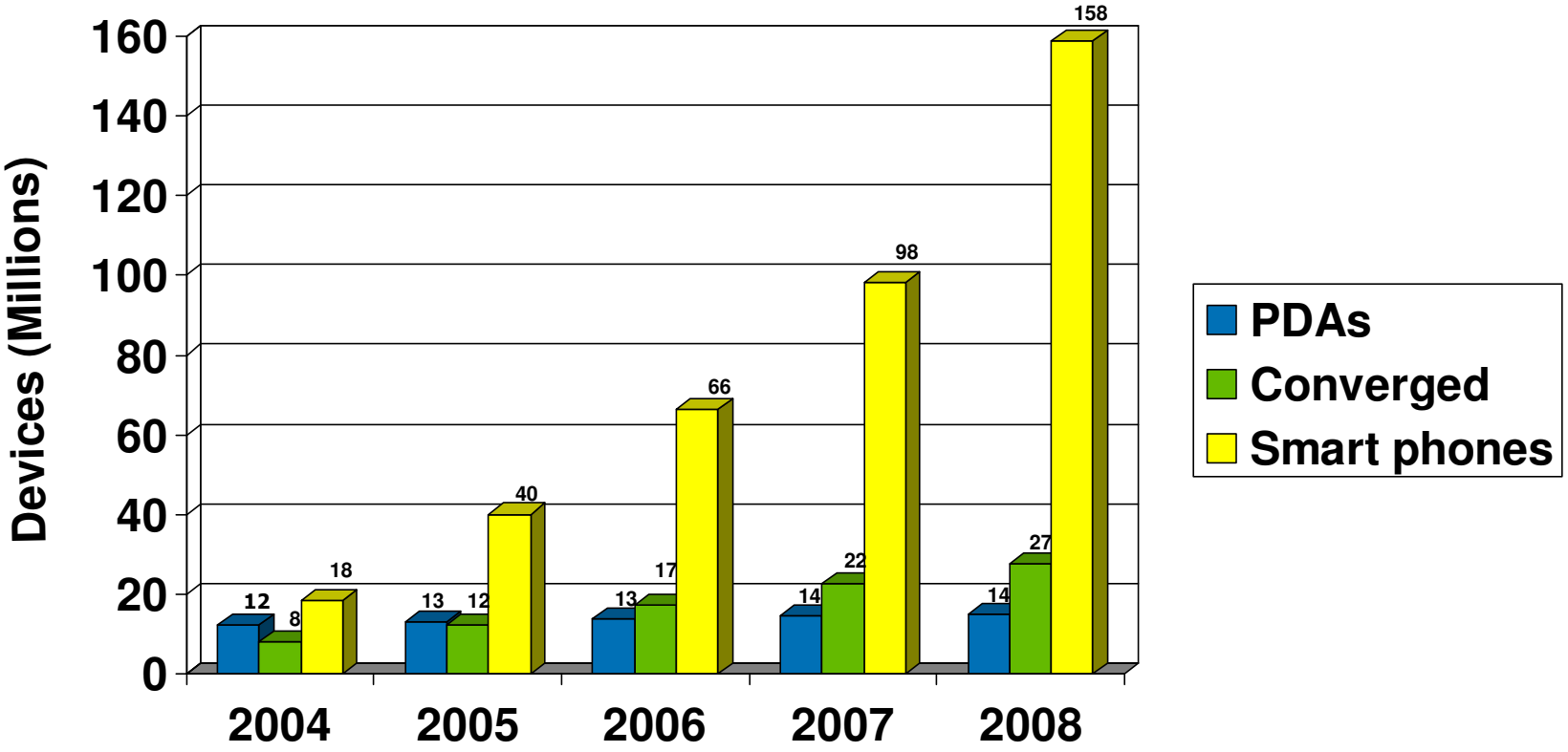
CONVERGED

- Pen input
- Wi-Fi, Bluetooth, GPRS
- Cellular data
- PIM
- Enterprise applications
- Wireless sync

SMART PHONE

- Keypad input
- Wi-Fi, Bluetooth, GPRS, CDMA
- Cellular voice & data
- PIM
- Wireless sync

Situation:
Handhelds are becoming pervasive



Sources: IDC, In-Stat, ABI

Situation: New breed of HP devices deliver advanced capabilities

- Robust Communications
  - LAN: 802.11
  - WAN: GPRS & CDMA
  - PAN: Bluetooth & IR
  - Future: EDGE & EV-DO
- Access
  - Email & Internet
  - Applications & Enterprise
  - Sensitive Information
  - Wireless sync
- Storage
  - Standard: 64M
  - Available: 1G
  - Soon: 2G

Situation: Market leaders are making significant investments in handhelds

- Help drivers manage deliveries and inventory and process orders.

- Deploy 500,000 Windows Mobile devices for the 2010 Census.

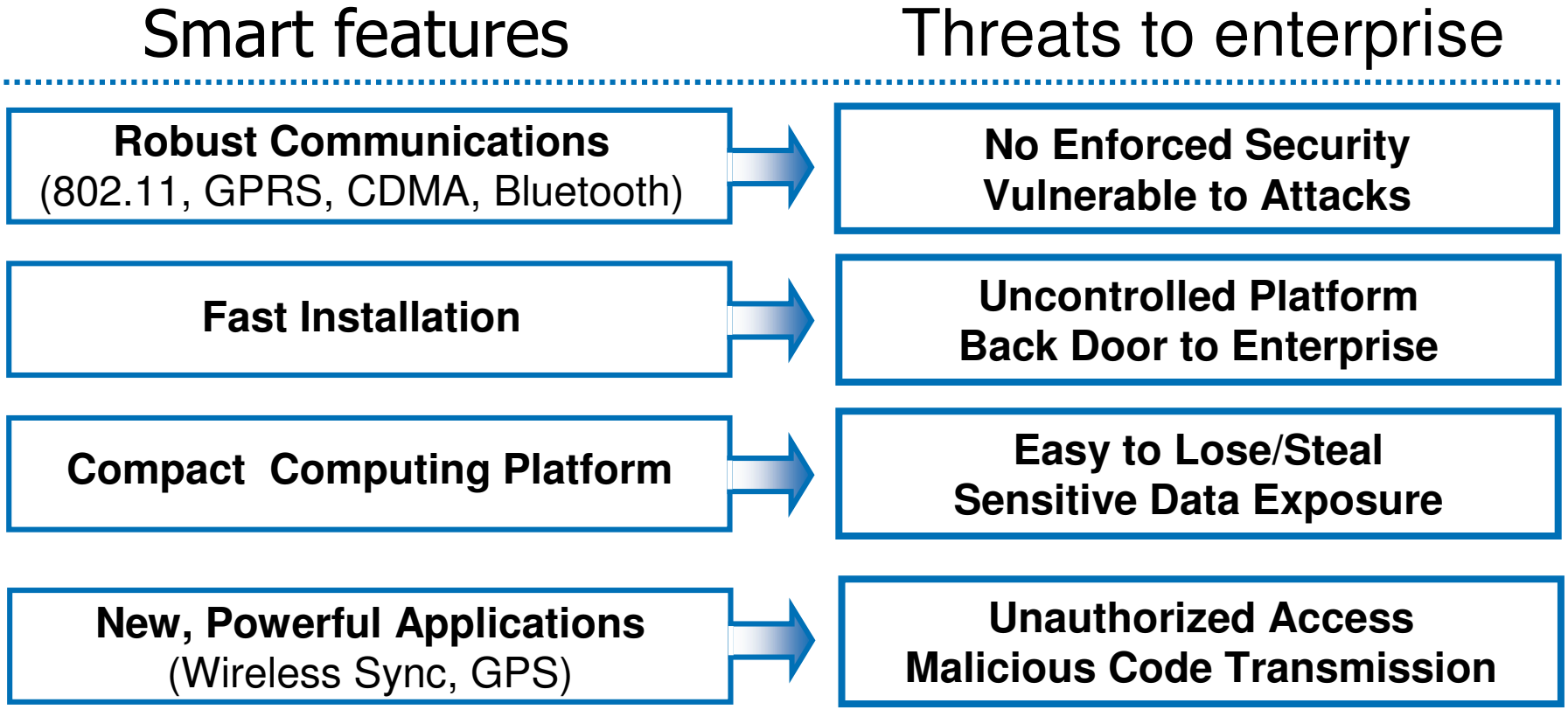
- Enable physicians to write prescriptions on their PDAs.

"Through 2005, less than 30 percent of enterprise PDA use will be officially sanctioned by IT management and less than one-third of PDAs carrying enterprise data will be comprehensively managed."

Gartner, Inc.

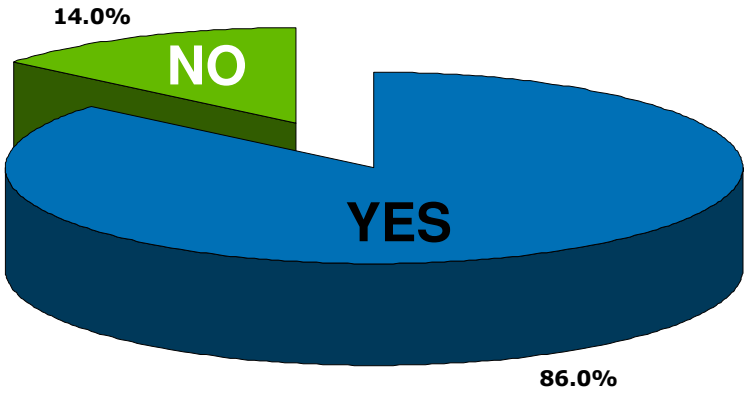
Predicts 2004: Handheld Computers, November 2003

Situation: Handhelds and smart phones will get smarter and more vulnerable

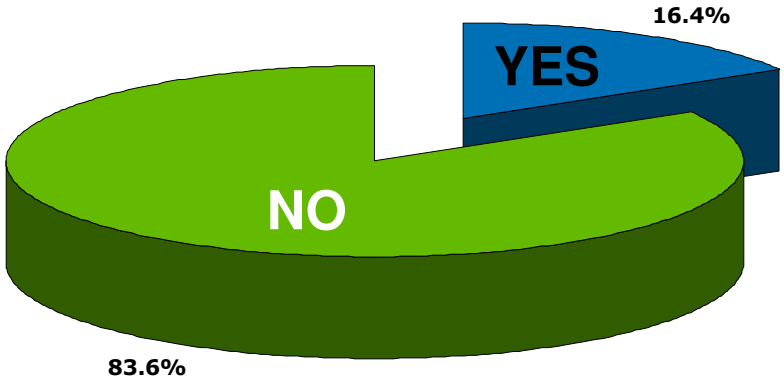


Situation: Threat from employee PDAs and smart phones ignored

Does your employer know that you have used your personal PDA/smart phone for business use?



Does your employer set guidelines for the use of personal PDAs/ smart phones?



Sample size: 288 out of 755 Internet-connected households that indicated usage of personal PDAs/smart phones for business purposes.

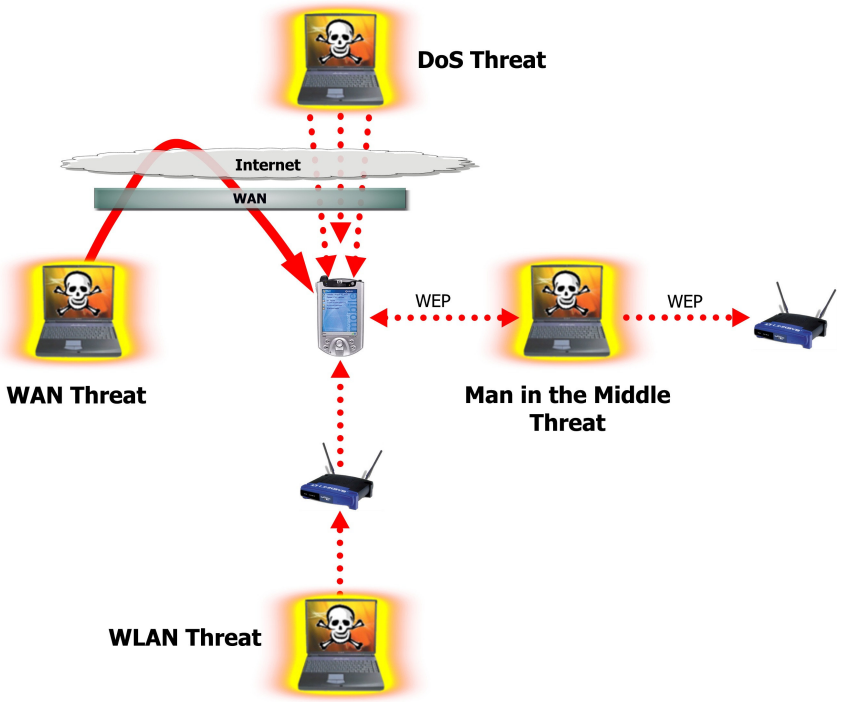
Sources: TNS NFO & Bluefire Security Technologies

"Through 2006, 90% of mobile devices containing enterprise data will have insufficient power-on protection and data encryption to withstand casual to moderate hacker attacks."

Gartner, Inc.

Predicts 2004: Handheld Computers, November 2003

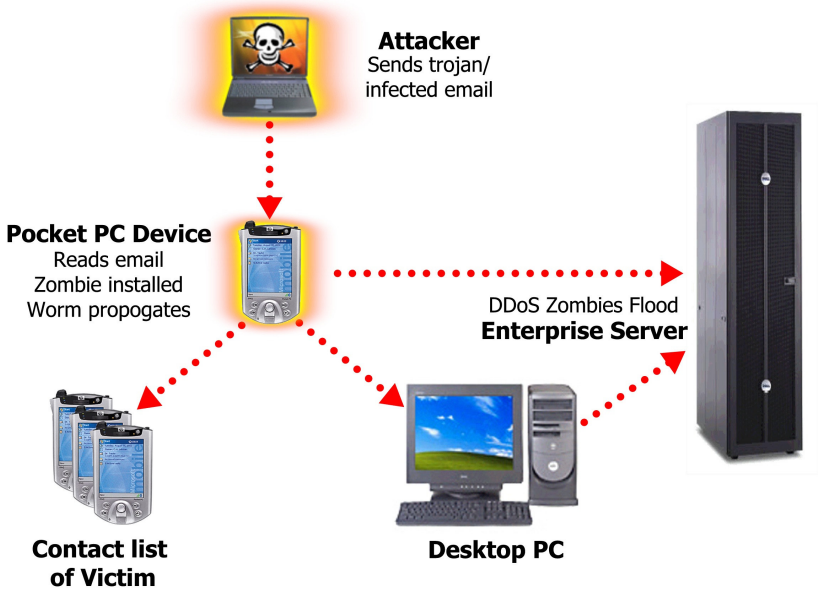
Wireless security challenge: Handhelds are vulnerable to multiple attacks



- **Theft & corruption** of confidential data
- **Unauthorized access** to enterprise network
- **Disruption** of transactions
- **Loss** of data
- **Forced** hard reset
- **Malicious code** passed to the enterprise

HP WORLD 2004
Solutions and Technology Conference & Expo

Wireless security challenge: Handhelds can be a transport for malicious code



- **Distributes** in the same way as desktops:
  - Email, downloads, file sharing
- **Opens a backdoor** to the enterprise network
- **Corrupts** handheld device & data
- **Infects** enterprise
- **Disrupts business**

"Security flaws could allow unauthorized access to private information on Bluetooth-enabled wireless phones. Buyers should demand security guarantees from manufacturers – and disable Bluetooth if it isn't needed."

Gartner, Inc.

Disable Bluetooth, February 2004

Wireless security challenge: Cabir worm targets smart phones via Bluetooth

- How it works
  - **Detects** other Bluetooth-enabled Symbian phones
  - **Transfers** malicious code to new host via Bluetooth connection
  - **Installs** the application and infects itself
  - Demonstrates that **wireless carrier networks can be bypassed** to propagate worms
  - **Reported variant**: installs text file that includes the entire novel Ulysses
- Future vulnerabilities
  - Use text messaging to propagate code that **shuts down cell phones or defrauds pre-paid phone card providers**
  - Recent Bluetooth conference demonstrated the ability to **steal all the contact information on a PDA wirelessly, in less than 5 seconds**

Security policy evolution: Extend perimeter to protect handheld devices

1980s

- Stable environment
- Easier to control & manage
- Traditional network security technologies effective

1990s

- Occasionally connected
- Harder to control & manage
- Expose enterprise to new vulnerabilities
- Extend security perimeter
- Employ device-side security technologies (personal firewalls, VPN, AV)

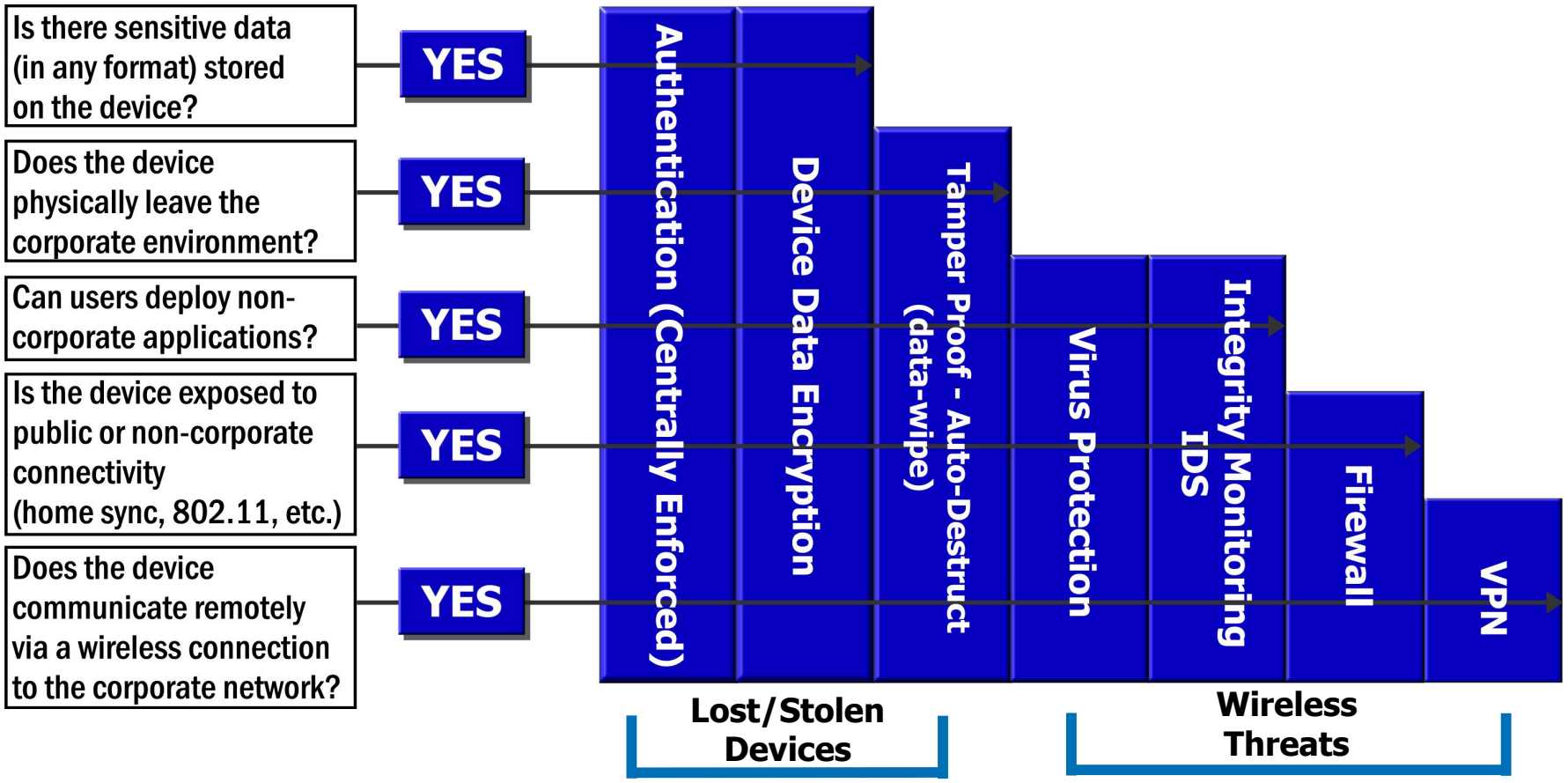
TODAY

- Operate in hostile environments
- Easy to lose, steal & attack
- Most difficult to control & manage
- Network security ineffective
- Extend security perimeter
- Manage as part of infrastructure
- Deploy device-side security (personal firewalls, VPN, authentication, encryption)

Policy deployment – Step 1
Develop a handheld security strategy

- **What devices will you support?**
  - Corporate v. employee
  - Operating systems
  - Wireless PDAs, smart phones
- **What sensitive information will be stored on handhelds?**
  - Corporate email
  - Contact lists
  - Documents
  - Applications
- **What types of communications will be allowed to/from the devices?**
  - Internal v. external use
  - Remote access
  - Internet access
  - LAN, WAN, PAN
- **What kind of security measures will you enforce?**
- **How will you handle lost and stolen devices?**

Policy development – Step 2: Decide how to protect your information



Policy development - Step 3
Implement enforceable policies

Security Issue	Policy Details
Authorized Technologies	• **Specify supported OSs & devices** • **Prohibit business use of non-supported devices**
Confidential Information	• **Detail what information can and cannot be stored on the device**
Lost & Stolen Device Protection	• **Enforce power-on passwords** • Device wipe • **Require encryption of sensitive files**

Remote/Internet Access Attack Protection	• **Allow network access via ISP or Hot Spot ONLY if the device has the following:**
	  - Personal firewall
	  - VPN
	  - Integrity monitoring
	  - Device quarantine

Doing nothing will cost you: Risks & reactive management drive costs

Do Nothing

- No policy
- Employee-owned devices
- No central management or control
- Multiple operating systems and device models
- No enforced security

Enterprise Risks

- How do you know if information is lost or misused?
- How do you trace and close down the source of a leak?
- How do you know if the system has been hacked?
- How do you know what employees are downloading?

HP WORLD 2004
Solutions and Technology Conference & Expo

Gartner recommends 3 approaches for PDA and smart phone support

- Level 1
  - Full security – similar to PCs and notebooks
  - Enterprise-issued standard PDAs and smart phones
- Level 2
  - Support employee-owned devices
  - “PDA firewalls”
- Level 3
  - No support
  - Ban handheld devices

Source: Gartner, Inc.
Important Elements of Support Plans for PDAs and Phones
December 2003

"Gartner urges enterprises to install personal firewalls on all devices that go outside the enterprise network perimeter and all devices equipped with wireless LAN access. The need is immediate and payback is immediate."

Gartner, Inc.

Emerging Trends in Software Infrastructure, December 2003

Best practices: Corporate-owned handheld devices

- Define a mobile security policy
- Centrally enforce and monitor handheld security
  - Device-side security
  - Central management and control
  - Event logging
- Block unauthorized handheld network activity
  - Personal firewall/intrusion prevention
- Enforce power-on passwords
  - Define lengths, composition rules & maximum attempts
- Use device wipe to protect lost and stolen devices

Best practices: Corporate-owned handhelds

- Encrypt sensitive data on handhelds and storage cards
  - AES
  - Folder encryption
  - Dynamic size allocation
- Protect handheld integrity from viruses, Trojans and worms
  - Anti-virus software
  - Monitor changes to core system assets
- Shield enterprise from compromised handhelds
- Disable Bluetooth & IR
- Secure data in transit

Best practices: Employee-owned handhelds

- Define a mobile security policy
- Register devices with IT
- Bring defective hardware to IT for repair
  - Prohibit sending equipment to manufacturers/retail service centers
- Verify that sensitive information has been removed from device upon termination
- Install corporate-managed handheld security software on devices

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP