

# Protecting Mobile Users on a Budget

Neil MacDonald

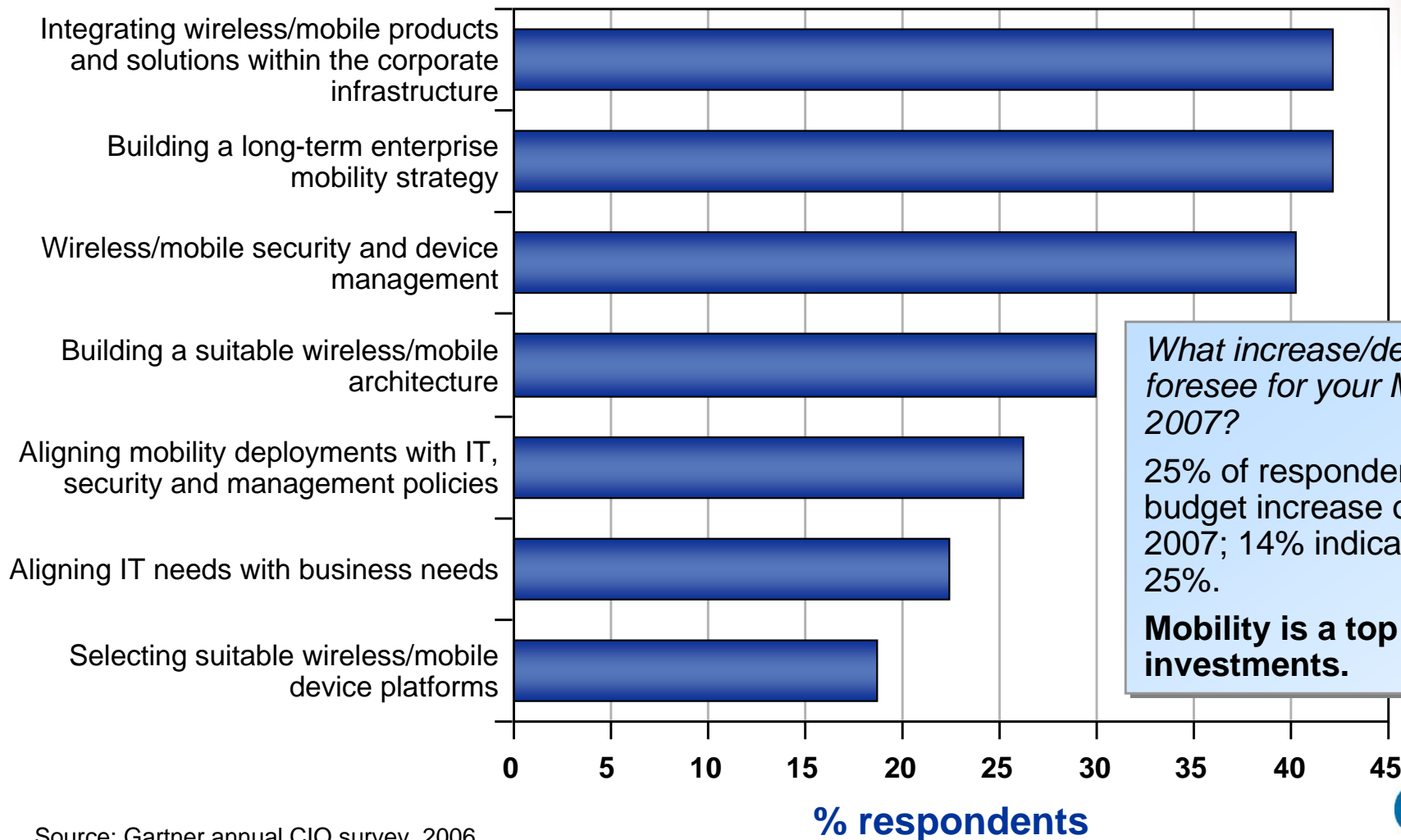
  
Gartner®  
Midsize Enterprise  
Summit. 2007

  
Gartner®

# What Mobile and Wireless Security Issues Are Keeping CIOs Awake at Night?

What are the main mobile and wireless problems facing your organization in the next 12 to 18 months?

## Problems



*What increase/decrease do you foresee for your M&W budget in 2007?*

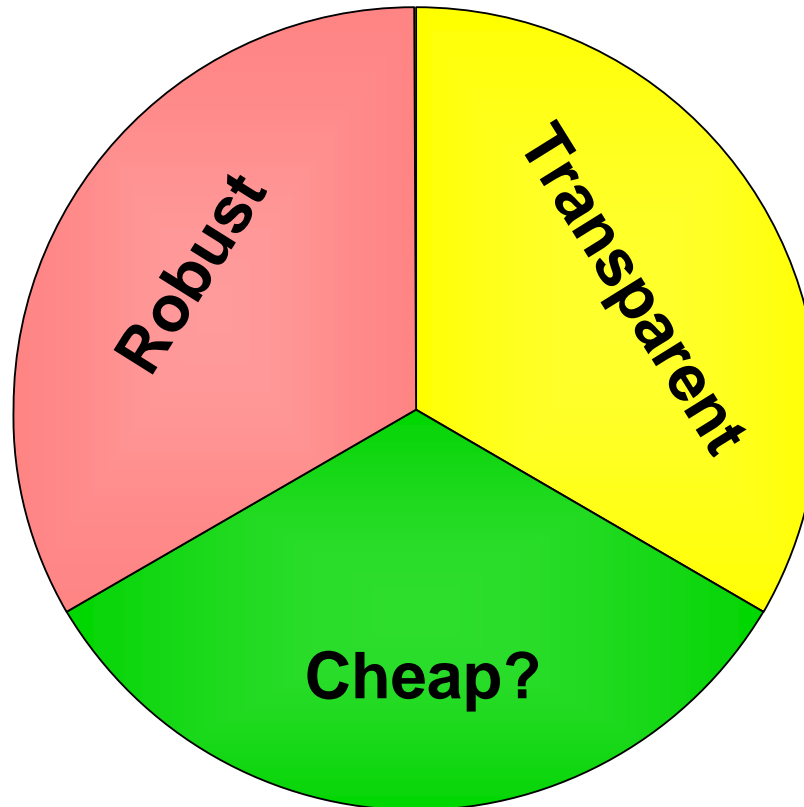
25% of respondents indicate a budget increase of 10%-25% in 2007; 14% indicate more than 25%.

**Mobility is a top priority for IT investments.**

# Security Budget Challenge

**Mobile Security?  
Pick Any Two ...**

**Failures Damage  
Your Reputation  
Threats Are  
Increasing**



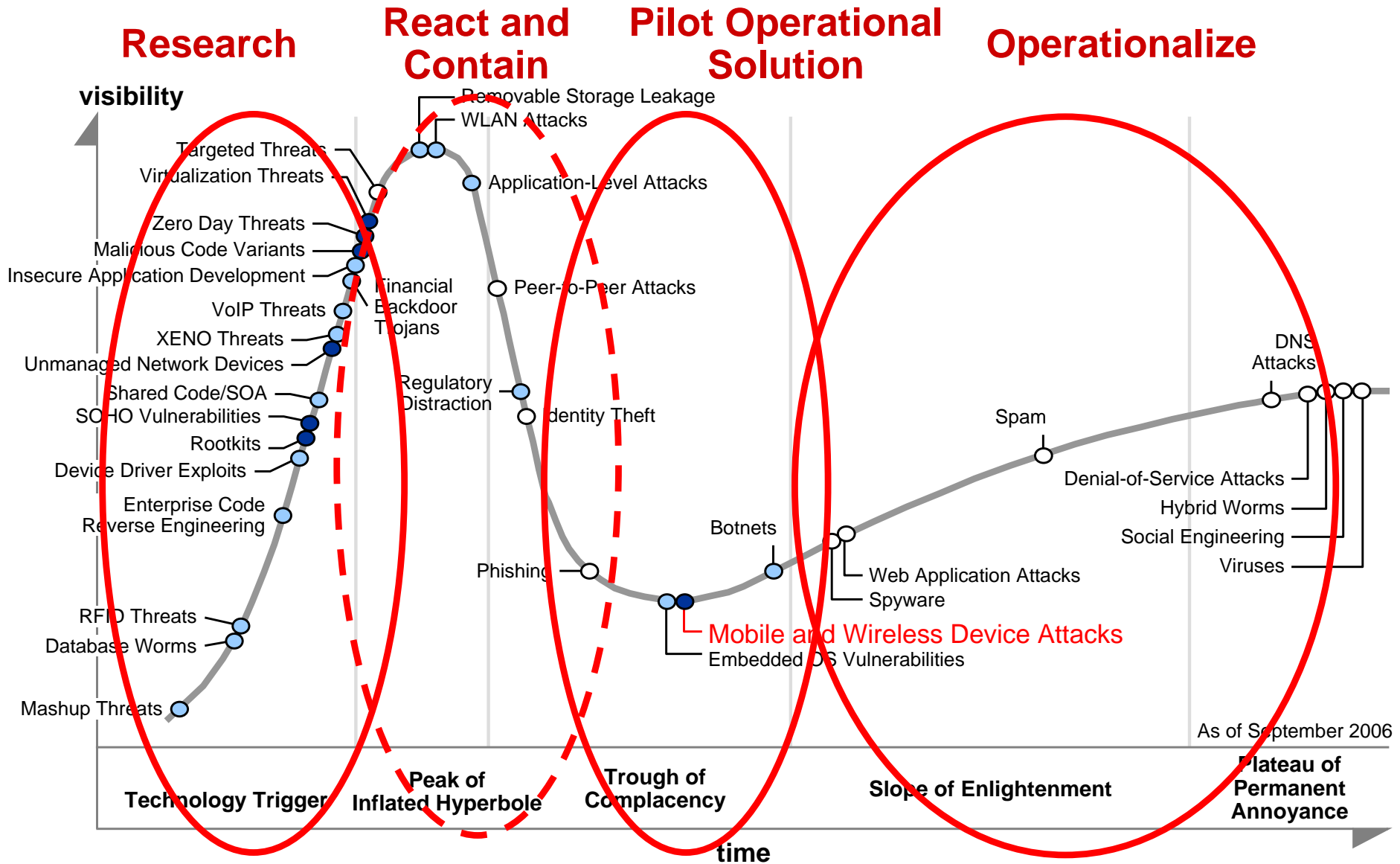
**Users Complain  
About Security  
Tech Support Costs  
Will Rise**

**Budgets and IT resources are limited  
Security and management demands  
are increasing**

# Key Issues

1. How can enterprises streamline processes and technology choices to reduce mobile security costs?
2. How can the top mobile security threat scenarios be addressed with limited budget?

# Gartner Threats Hype Cycle: Operationalize the Routine



Years to mainstream adoption:

○ less than 2 years

● 2 to 5 years

● 5 to 10 years

▲ more than 10 years

○ obsolete  
⊗ before plateau

# Use What the Notebook OS Provides

## Windows XP SP2, Vista

## Issues

WUS/SUS to stay current on patches

Verification of update levels

EFS & BitLocker for data encryption

Incomplete, hard to manage

NX flag to block code from running in data memory

Legacy support

Use bundled software firewall

Limited tracking, user alerts

Demote users from Administrator

Incomplete controls

Run IE7 or Firefox

Application compatibility

Restrict uPnP, USB, CD, DVD

Incomplete controls

Use bundled VPN, NAC & WPA

Third-party compatibility

Hard-coded document & site filtering

Manual filters, hard to manage



# Use What the Mobile OS Provides

## Phones & PDAs

Embedded data encryption

Bundled mobile policy updater

Over-the-air sync & backup

Track location via GPS

Remote lockdown/erase

Remote reset/rebuild

Restrict memory cards

Restrict Bluetooth settings

Use bundled VPN & NAC

Document & site filtering

## Issues

User may disable the defaults

Usage may require cradle

Usage may cost extra

Usage may cost extra

Not available on all models

Not available on all models

Varies by model

User can change settings

Third-party compatibility

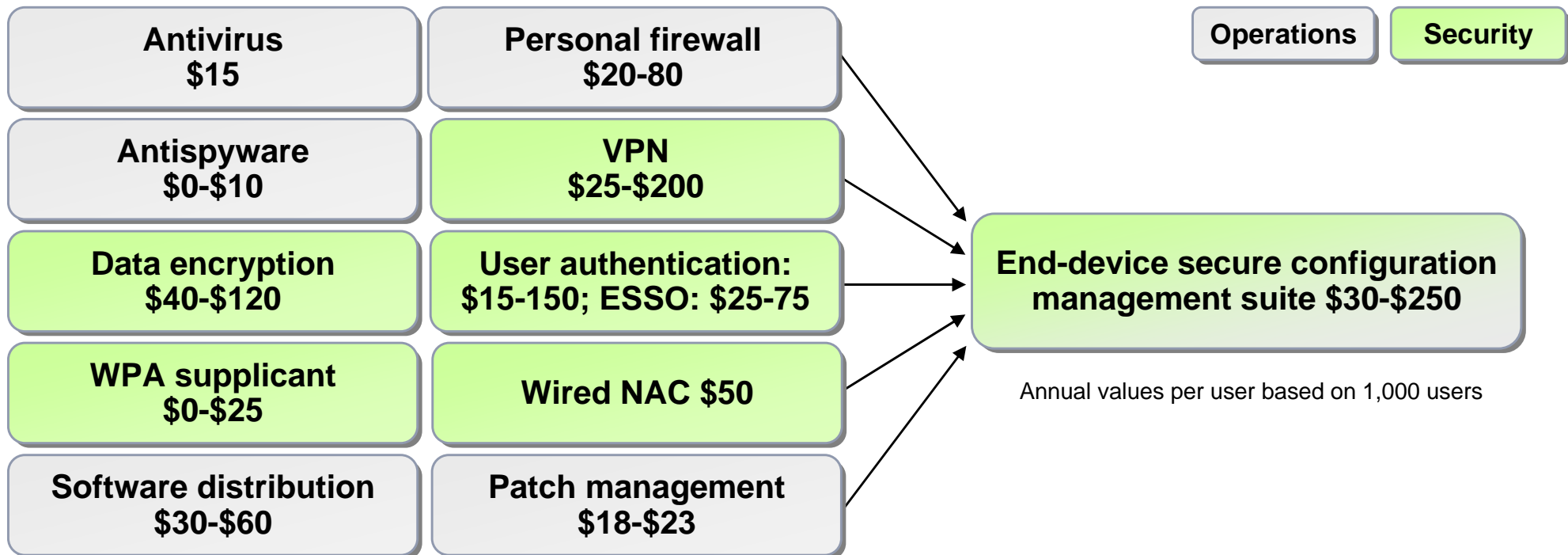
Not available on all models



# Use Gateway and Carrier Security Already Provided

- All corporate mobile e-mail should flow through enterprise e-mail server malware removal
- Buy device encryption, backup & recovery from carrier
  - Pay for managed business e-mail & security services from the carrier rather than build your own server infrastructure
- All carrier mobile communications services should include malware filtering
  - Demand this, it's a competitive choice
- Web access/surfing can be filtered through your primary enterprise firewall and Web security gateways (through a remote access VPN)
  - Extra shielding for the mobile user, and you already paid for it

# Trade Point Security Functions for Converged Suites: Reduce Seat Costs Up to 22X



Save **less** than expected: repeat these purchases with different products on notebook and mobile platforms



Save **more** and be a hero: buy products that work across notebook, PDA, and smartphone platforms, as well as multiple OSs.

# Pick Mobile Application Platform Vendors With Integrated Security Features

	Enterprise Security	Transmission Security	Device Security	App-lication Security	Device Mgmt.	Portal Mgmt.
<b>RIM</b>						
<b>Motorola/Good</b>						
<b>Nokia/Intellisync</b>						
<b>Microsoft</b>						
<b>Sybase</b>						

(More vendors from the MAG and wireless e-mail market — not included here)

Strong sec/mgmt. offerings  
 Weak sec/mgmt. offerings

**The top five wireless e-mail vendors are driving convergence; only RIM and Good cover all areas.**

# Mobile E-Mail Security: Native Support Saves \$

	Advantages	Disadvantages	Choose When
<b>Native Support</b>	<ul style="list-style-type: none"> <li>• Less expensive</li> <li>• Single platform/vendor for applications and security</li> <li>• Security integrated into application</li> <li>• Better performance (battery life, bandwidth)</li> </ul>	<ul style="list-style-type: none"> <li>• Security limited to e-mail (other applications not supported)</li> <li>• Security features may be better implemented in third-party tools</li> </ul>	<ul style="list-style-type: none"> <li>• Selected mobile e-mail platform security support meets your requirements</li> <li>• There is no plan to deploy applications other than e-mail</li> </ul>
<b>Third-Party Tools</b>	<ul style="list-style-type: none"> <li>• More flexibility to select security features</li> <li>• A single platform to support all applications</li> <li>• Support for more devices and back-end platforms (such as S/MIME).</li> </ul>	<ul style="list-style-type: none"> <li>• More expensive</li> <li>• Fragmented market (many vendors to deal with)</li> </ul>	<ul style="list-style-type: none"> <li>• More applications are involved</li> <li>• Security requirements are complex or vary by user group or application</li> <li>• Different devices need to be secured</li> <li>• Compliance is needed</li> </ul>

# Don't Allow What You Cannot Support Set Rules That Can Be Enforced

## Three Levels of Support



**Not Supported**  
**= Not Allowed**  
*= not your problem*

**Data Interface Support Only**  
Can connect to enterprise information sources for data retrieval through controlled ports; no application development support, requires security software compliance

**Fully Supported**  
All support privileges of notebooks and desktops, including application development support



**No Cost**

**Containable Cost**

**Manageable Cost**

*By permitting limited access for some individually purchased mobile devices, the PC support group can implement the first and third options.*

# Cornerstones for Mobile Security

## **Consistency**

The key attribute of strong security

## **Exposure**

Minimization increases security

## **Commitment**

Vigilance requires time and money

## **Reasonableness**

Overwhelming force wastes money and may not achieve goals

# User Behavior Threats: Remove Options That Increase Vulnerability

## Security Guidelines

We recommend...

You should ...

This is a good idea ...

Are you sure you want  
to disable the firewall?

Yes

Cancel

To: Head of Security  
From: Company CEO  
Mr. Grunt,

I am too important to be bothering with all these authentication requirements. Please arrange for all board members to sign on to all systems using a two-digit PIN. You get to explain it to the auditor for me.

Mr. Big.

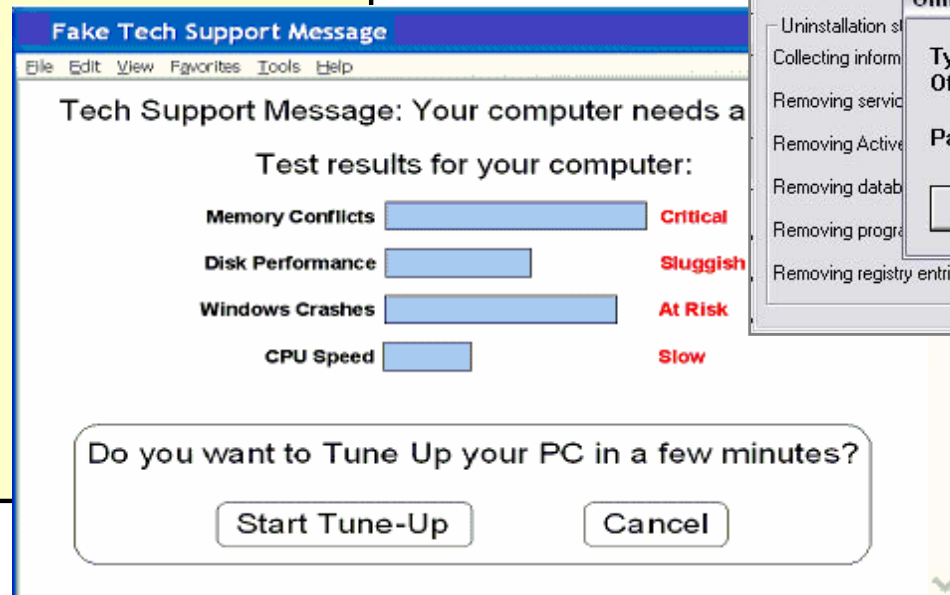
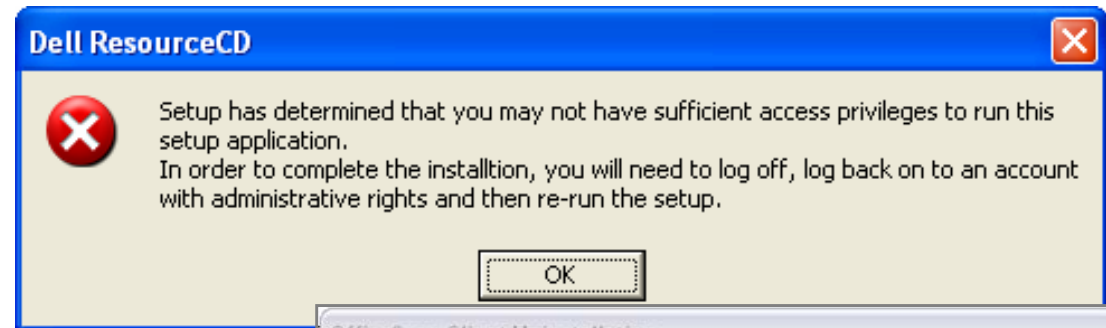


"Place your eye  
against dashboard  
for retinal scan"

# Configuration Threats: Minimize Images and User-Driven Changes

## Corporate Image Catalog

- Workstations
- Windows
- Research
- Sales
  - Red Team
  - Blue Team
- Marketing
- Executive
- Servers
  - Windows
  - Linux
  - Sun



# Data Leakage Threats: Encrypt Data, Track Usage and Disposal



[www.crimereduction.gov.uk/graphics/burglar1.gif](http://www.crimereduction.gov.uk/graphics/burglar1.gif)



[www.leics.gov.uk/kiosk.jpg](http://www.leics.gov.uk/kiosk.jpg)



# User Authentication Threats: Add Something Unique to the Login

~~User ID: joesixpack  
Password: ilikegolf~~

*dumb and dumber!*

User ID: joesixpack  
Password: 3ionGtepK0TZ

*OS supports, but user screams*

## Consider User ID plus . . .

*token, software or hardware*



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with  
RSA SecurID software token

*picture password*



**4-digit PIN**

[ \_ \_ \_ \_ ]

+

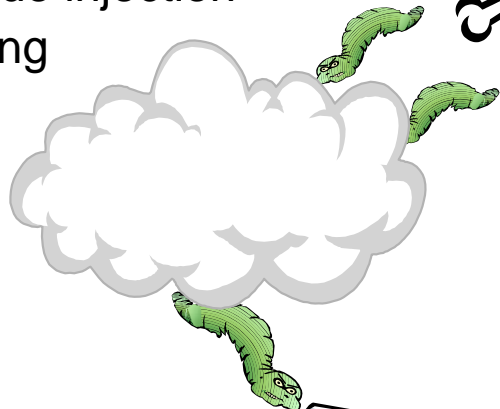


*fingerprint*

# Network-Borne Threats: Manage Device Firewalls

## Internet & visitor net...

- port attacks
- malcode injection
- phishing



hotel



Employee

VPN

Buffer Overflow



## Bluetooth...

- peer-to-peer attacks
- billboards
- sniffing



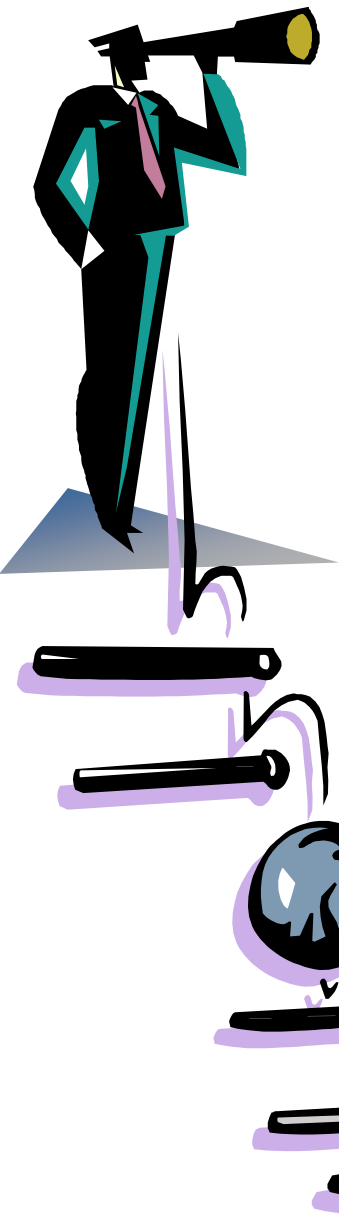
## Home/public Wi-Fi ...

- eavesdropping
- port attacks
- malcode injection
- evil twin



# Wireless Viruses Problem Overview: When Will Wireless Viruses Hit You?

## Threat Time Frame



2003

SPAM



2004

Malicious content,  
limited spreading



2005

Wireless-targeted  
viruses emerge



2006

Propagation is difficult,  
intermittent

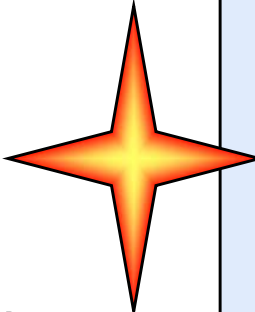


2007

Wireless viruses  
commonplace

2008

Wireless Commerce risks



# Recommendations

- ✓ Small mobile devices are workstations; treat them so.
- ✓ Avoid separate products for each mobile platform.
- ✓ Use what the OS and network operators provide
- ✓ Require your carrier to filter against malware.
- ✓ Control system configurations.
- ✓ Avoid giving administrative access to users.
- ✓ Minimize user control of security decisions and settings.
- ✓ Assure that device firewalls are working!
- ✓ Minimize and standardize devices allowed/supported.
- ✓ Block most attachment types in e-mail.

# Protecting Mobile Users on a Budget

Neil MacDonald



Midsize Enterprise  
Summit. 2007



# Protecting Mobile Users on a Budget

Neil MacDonald



Midsize Enterprise  
Summit. 2007

