



The New “Insider” Threat

Extending Device and Data Protection
to the Mobile Workforce

Skip Taylor
Vice President, Product Marketing
www.Fiberlink.com

FIBERLINK

Simple. Secure. Mobility.

> Agenda

- Mobility Trends and Their Impact on IT
- Addressing Challenges of Greater Mobility
 - Under Today's Market Conditions
- Solutions Around Improving Mobile Visibility
 - Closing the Awareness Gap
- WiFi Security – a Brief “Tutorial”

> Fiberlink Overview



- **Company** – Founded in 1994. Headquarters in Blue Bell, Pennsylvania. Presence in NA, EMEA & Asia. Over 250 employees.
- **Leader in Mobility as a Service (MaaS)** – Help enterprises leverage new developments in mobile technology to increase productivity, lower costs and improve overall management
- **Leadership** – Recognized by industry analysts as an innovator and leader in the mobile market.
- **Financials** - Privately held, profitable and growing. Investors include Goldman Sachs, GE and TCV.

Today Everyone is Mobile and Access is Everywhere



Road Warriors



Planes

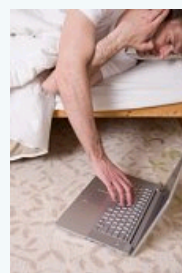
Trains



Automobiles

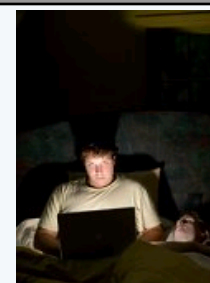
Highly Mobile Employees: 25%

Day Extenders



Morning

Noon



Night

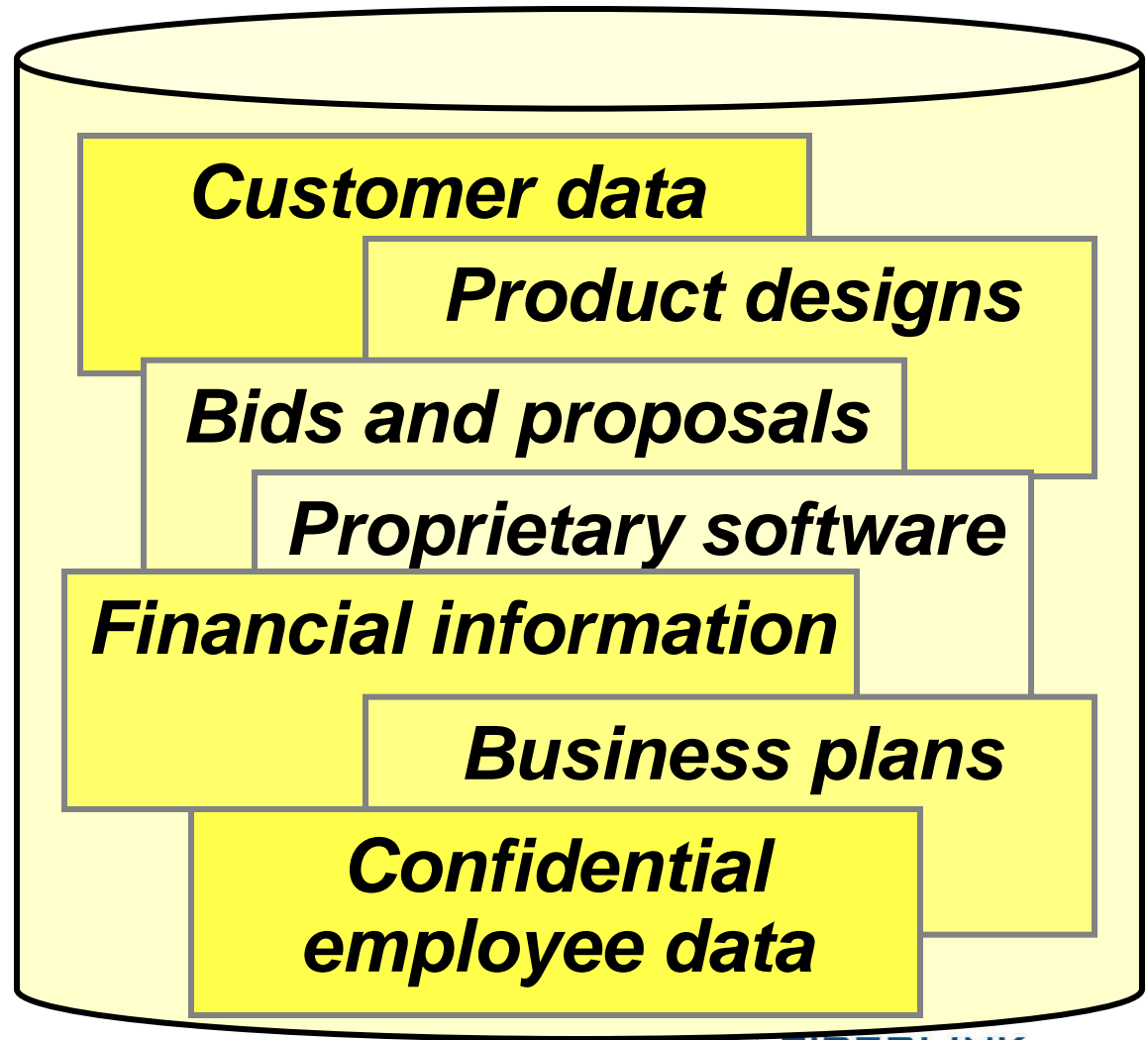
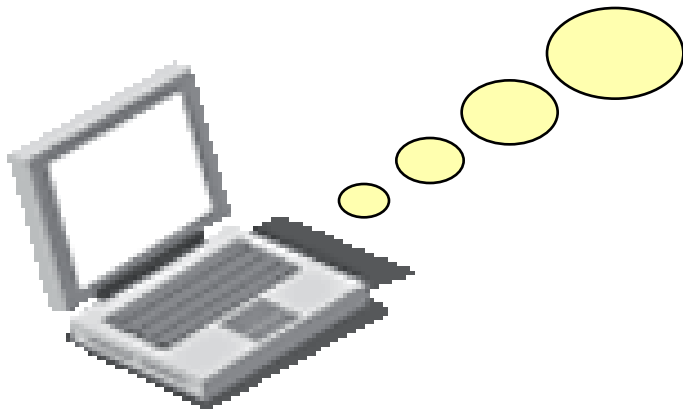
Employees with Laptops: > 50%

[Mobility] is not limited to the traditional 'hot' employee categories, who are typically 'road warriors' seeking to access corporate applications while on the move or in public places; increasingly it also includes part-time and full-time home workers and so-called 'day extenders.'

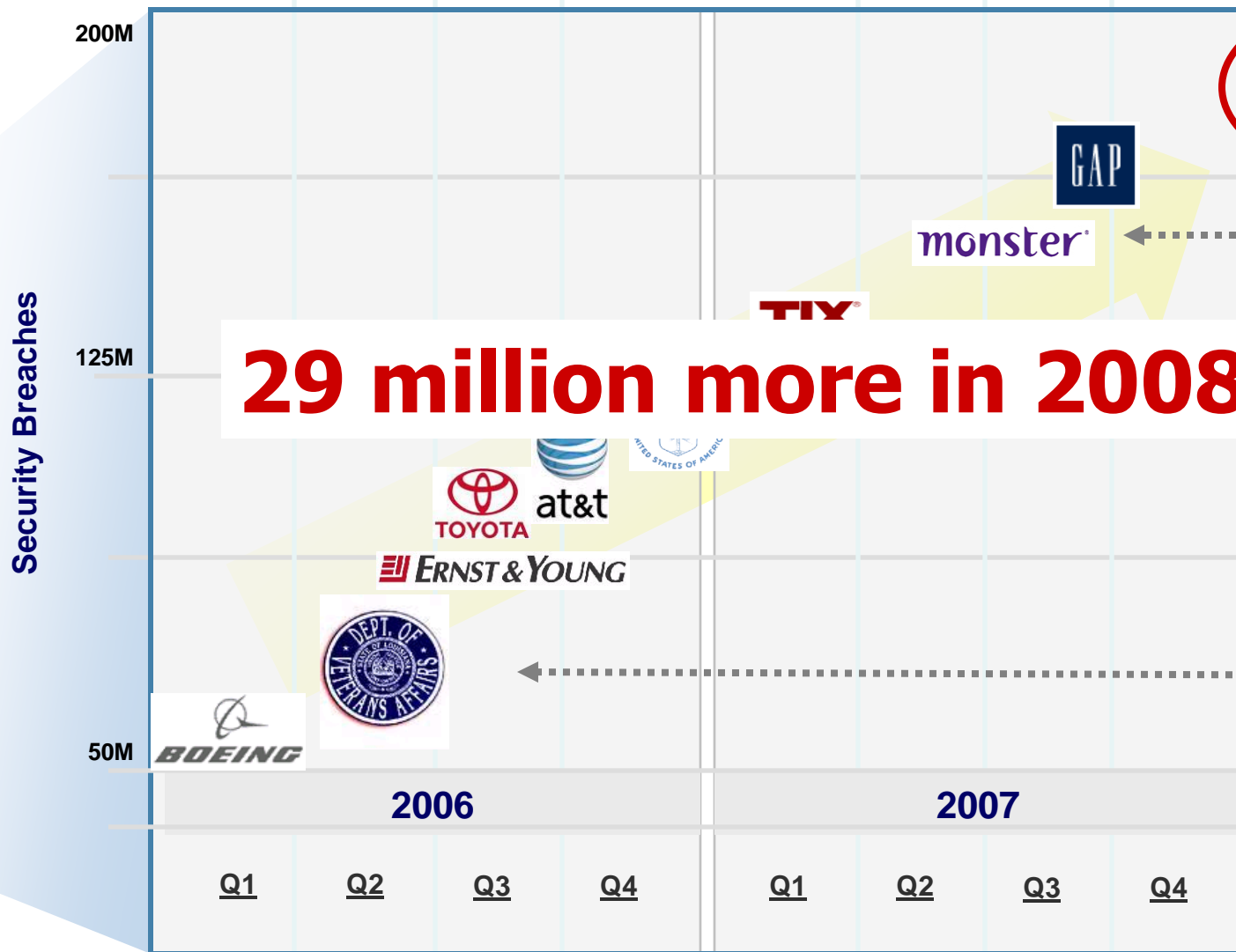
- Jeremy Green & Pauline Trotter, Ovum, 12/05

> More Data is Exposed on Laptops

IDC estimates that 60% of corporate data resides on laptops and PCs



> Security Breaches Are Growing



29 million more in 2008!!

1/1/2008: Over 217 million data records of U.S. residents have been exposed due to security breaches since Feb. 2005.

8/23/07: Details of some 1.6 million job seekers had been stolen. Fewer than 5000 were outside the US.

7/06: 100,000 credit and debit I account numbers through unauthorized intrusion" into its computer systems that process and store customer transactions including credit card, debit card, check, and merchandise return transactions.

5/3/06: Data of all American veterans were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 million veterans.

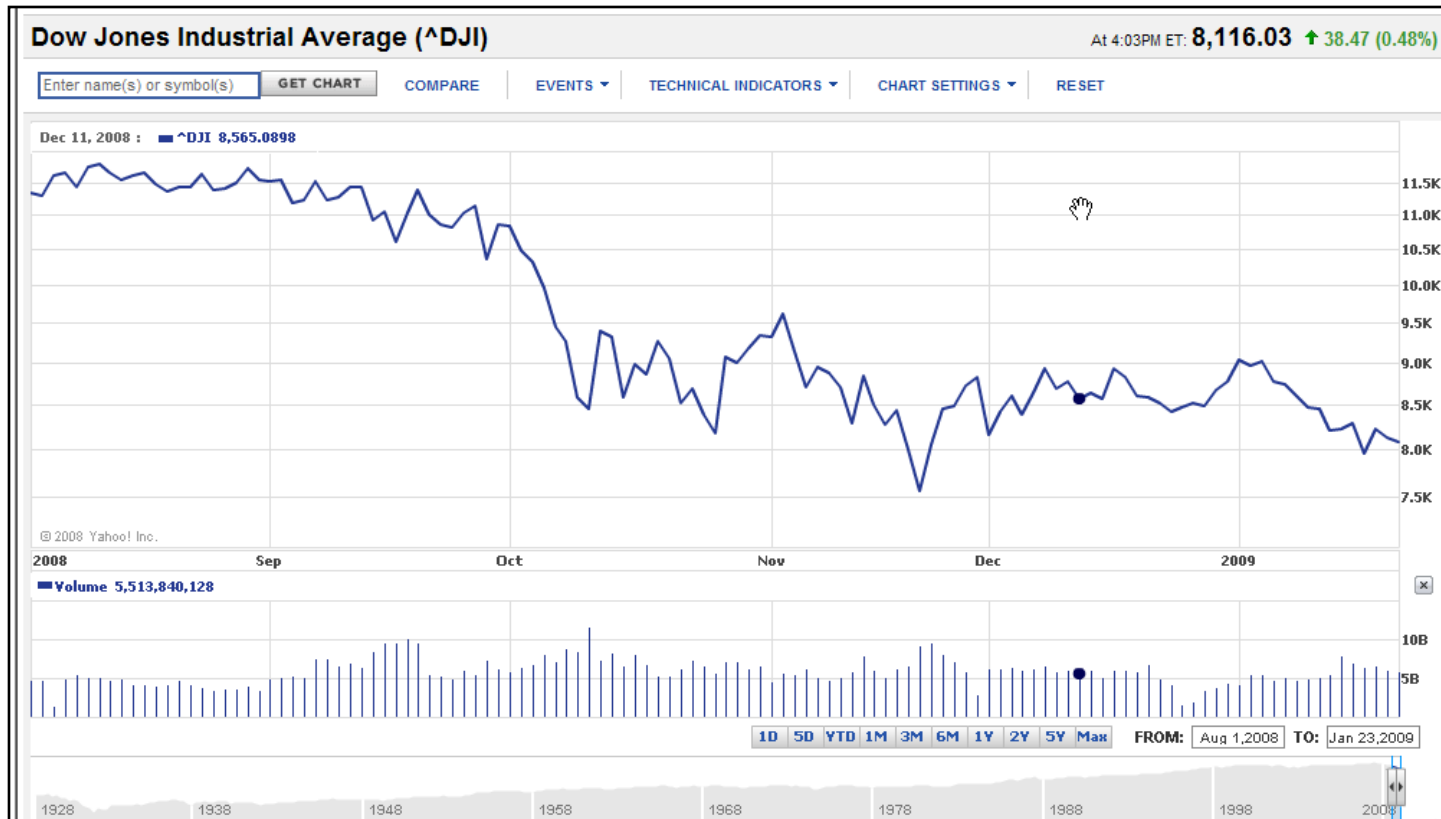
> A Market Shift is Underway

Do You Know What This Is?



“Satellite” View

> Here's Another View



You need a more effective way to manage your mobile operations?

How are Current Market Conditions Affecting Mobility?

- Budget tightening
 - What are IT buying priorities?
 - Security investments on “back burner”
 - Expenses based on ROI or TCO
- Corporate assets frequently off LAN
 - A shift from company sponsored to user requested teleworking
 - Gas prices
 - Interest in cost containment
 - Quality of life issues



Mobility is Not Slowing

> Investment Balance in Down Markets

Attempting To Make A Smart Decision Can Be Challenging

Device Protection

1. Deploy applications
2. Keep devices current
3. Account for new risks

Status Quo

1. No new investments
2. Actual ROI priority
3. "Willing to take risk"

IT Spend



> “Hackers” are More Aggressive of Late

A recent study:

- Of the top 100 most popular sites on the web, 70 percent are either hosting malicious content or contain a hidden redirect
 - Up 16 percent over the first half of 2008
- The number of legitimate websites compromised, exceeds the amount of sites specifically created by cybercriminals

Websense Security Labs. – SC Magazine 1/21/2009

> The Hackers are Motivated!

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

\$10 - \$150

Price range on the black market for a full set of identity information

\$.05 - \$5

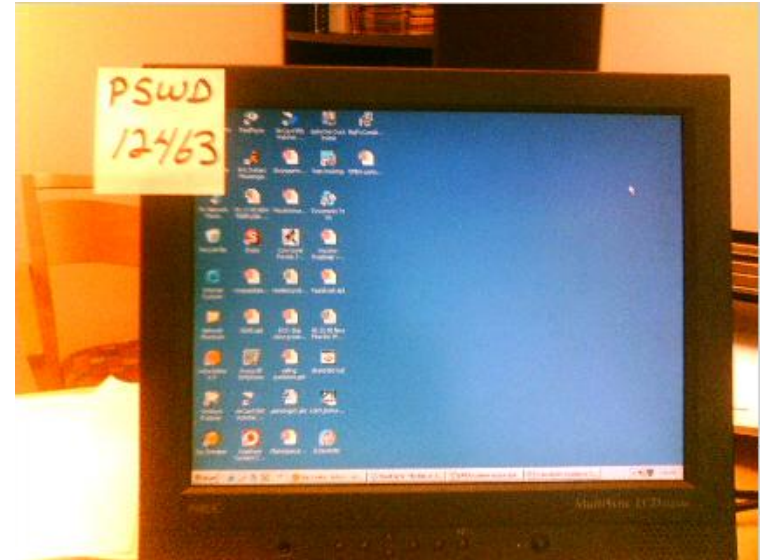
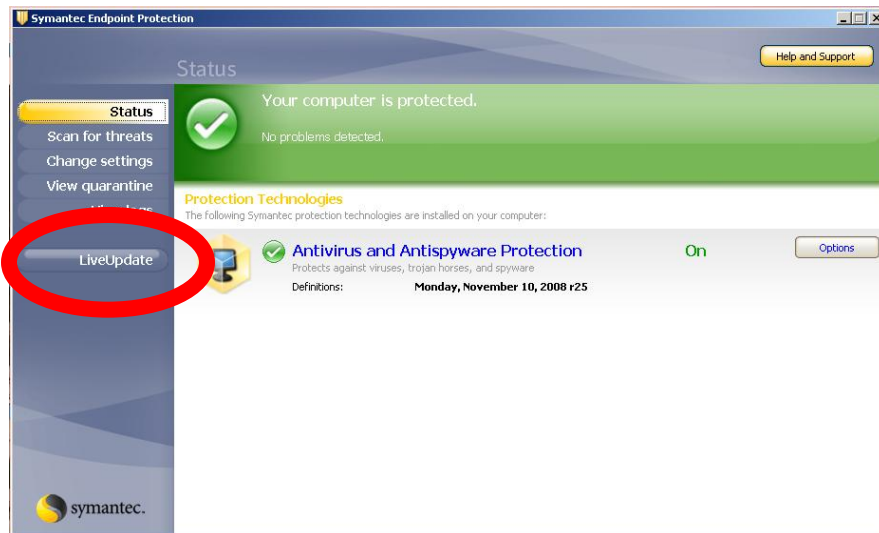
Price range per stolen credit card

Source: 2008 Symantec Internet Security Threat Report Trends

> “The best laid plans of mice and men often go astray” – Robert Burns

Human Engineering Issues

It's often difficult to see end-user behavior around security and admin



Organizations must automate the process and make it seamless to the end user

> Mobile Devices Are Targets

Data In Motion:



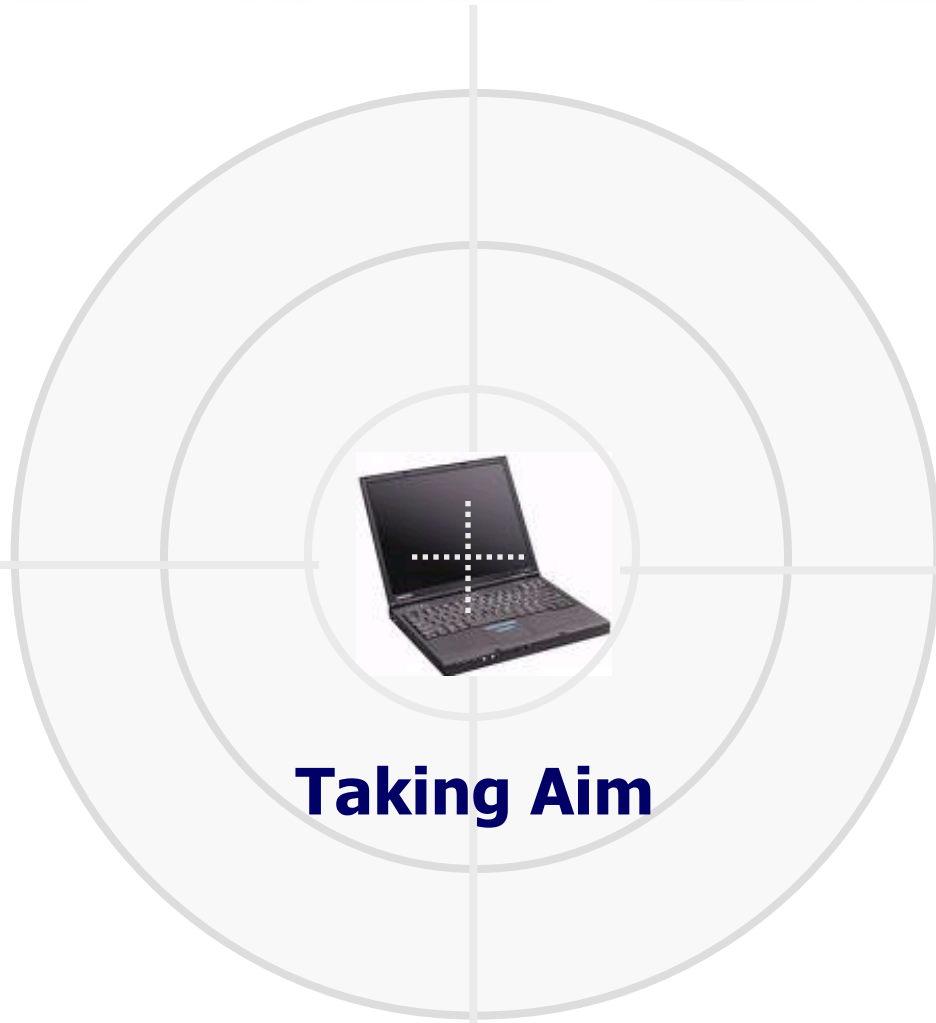
Wireless Hacking:



Lost Device:

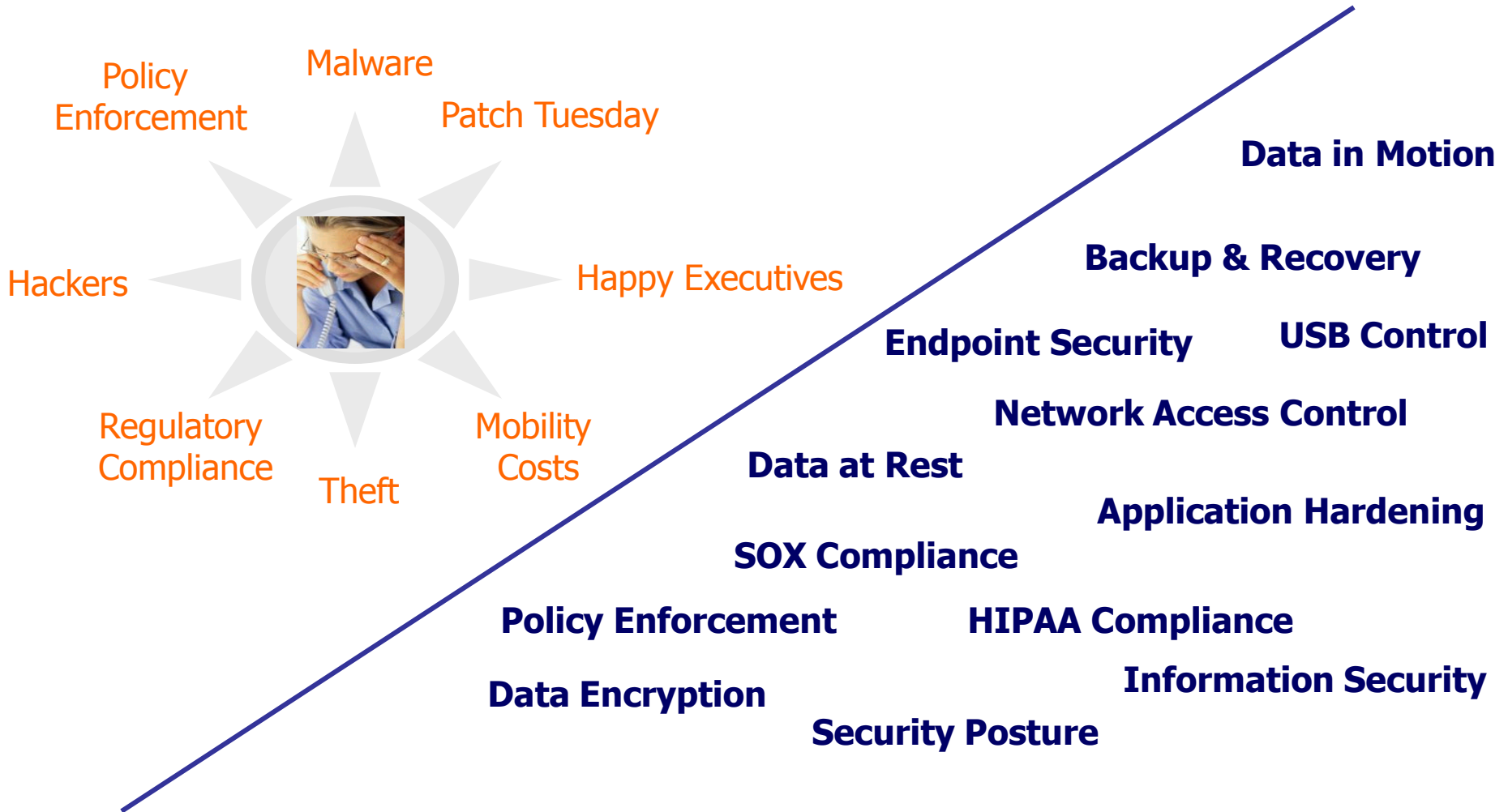


Stolen Laptop:



Taking Aim

> Decisions, Decisions...

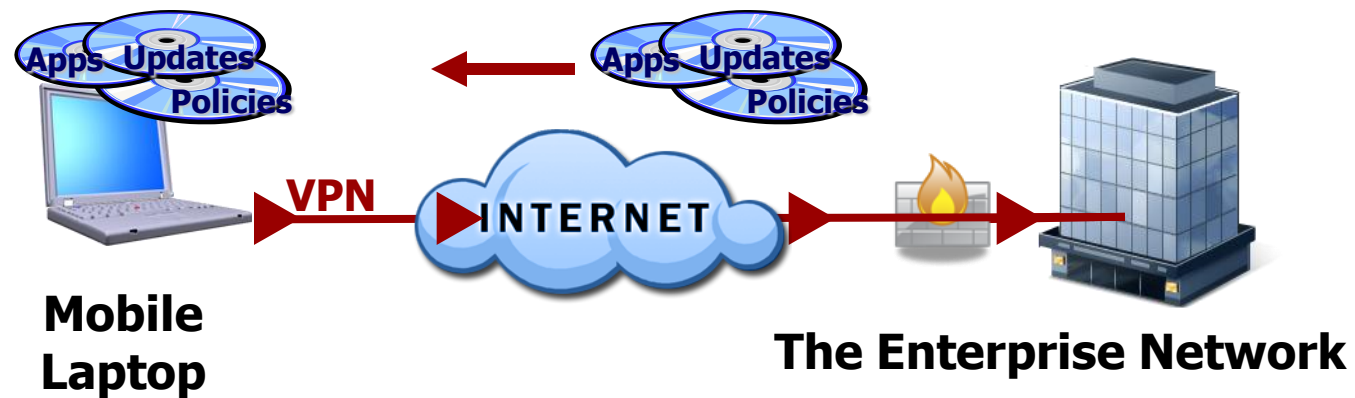


How do you cost effectively extend this protection to the remote device?

> Today's Architectures are LAN-Locked

LAN-based solutions rely on a connection to the corporate network to receive updates, new policies, and applications

IT has some Control

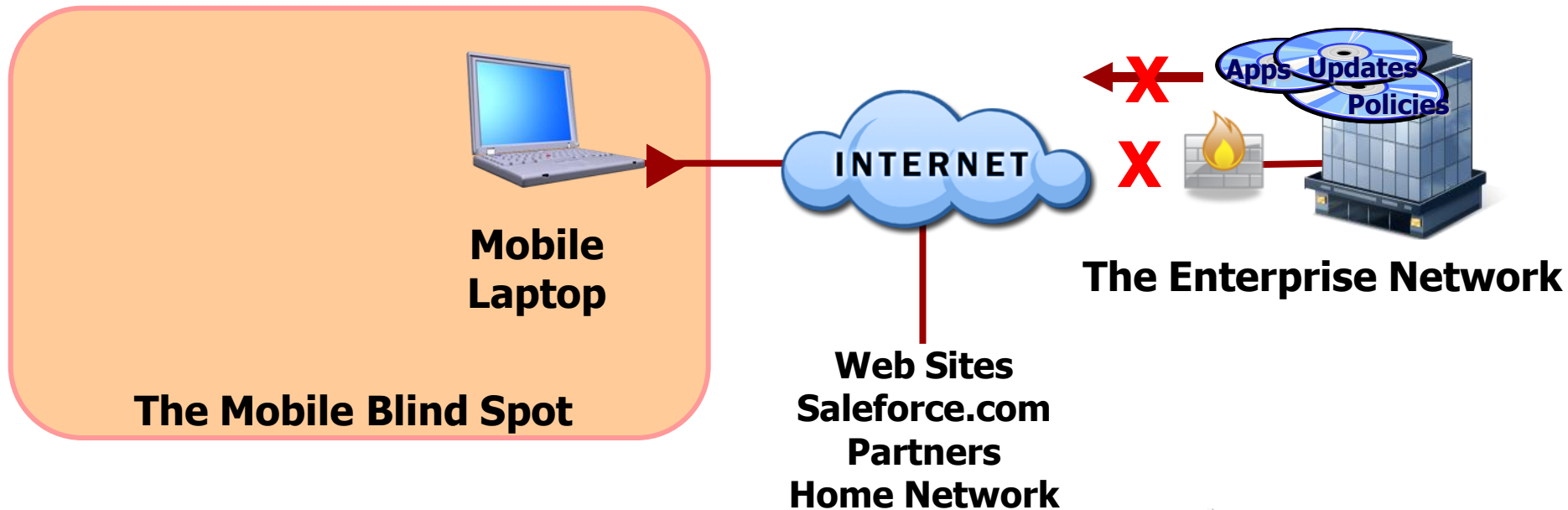


> Updating the Untouchables

LAN-based architectures rely on a connection to the corporate network to receive updates, new policies, and applications

When the device is not connected to the corporate network, it is in the "Mobile Blind Spot"

IT is not in Control



> A Look at Access Control (NAC)

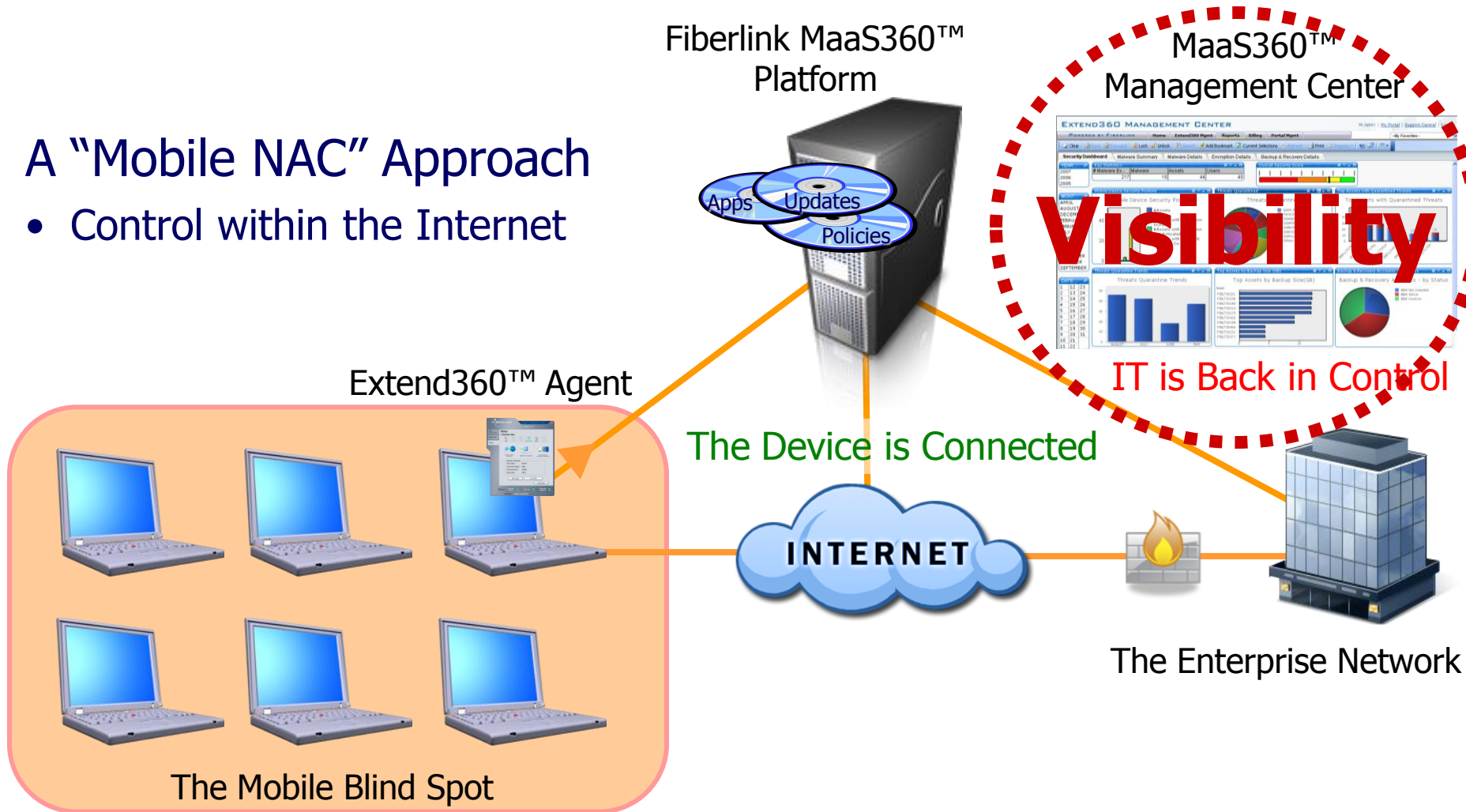
- Initiatives by Cisco, Microsoft, and others
- Fundamental goal: Protect the network, not specifically the data or device
- Users must connect to the LAN (physically or through a VPN)
 - What if they gain Internet access only
- Addressing “baseline” problems
 - AntiVirus, AntiSpyware, Personal FW
 - Not all remediate, many just block the user
- The products do not address “the mobile blind spot” and their unique threats

Improving Mobile User & Device Management

> Address the Problem Where it Occurs – “In the Cloud”

A “Mobile NAC” Approach

- Control within the Internet






Mobility Management Platform Benefits "In The Cloud"

- **Protects the corporate network and data**
 - Blocks non-compliant systems from connecting
- **Addresses the "mobile blind spot"**
 - Monitors, protects and updates mobile computers with any Internet connection
- **Reduce the overall cost of mobility**
 - Fewer help desk calls (< TCO)
 - Mobile optimization of existing investments (> ROI)
 - Manage the hidden expense of access
- **Real-time compliance reporting**
 - Audit trail provides visibility to The Blindspot
 - Visibility to know you're in control

> Why Now and Not Later?

- Current market conditions require a “smart spend”
 - Improving efficiency first but manage risk as well
- Cost containment is now a bigger priority
 - Minimize waste with better visibility
- Companies will fall prey to those expecting a weaker, “no budget” approach to data and device protection
 - The growth in number of compromised legitimate websites
- Fast implementation and industry savvy to smooth over the integration challenges
 - Cost effectively improve risk mitigation, overall governmental compliance, mobile device management, and people productivity across the organization



Do You Have an Insecure WiFi Blind Spot?

FIBERLINK

Simple. Secure. Mobility.

Securing WiFi

> Is it a False Sense of Security?

- Not all WiFi access points are the same
- Public access points don't want security
 - Too painful for the user to manage it
 - Desire simple connection only
- Even secure points are at risk
 - Home and office environments with WEP are exposed
 - 46% of companies still use WEP for securing WiFi
- How easy is it to break WiFi security?



A Short “Training” Video

FIBERLINK

Simple. Secure. Mobility.

> The Internet as a Hacking Source

The screenshot shows a Microsoft Internet Explorer browser window with the YouTube website open. The address bar contains the URL `http://www.youtube.com/results?search_query=hacking+wep&search_type=`. The search bar contains the text "hacking wep". The search results are displayed in a grid format, showing four video thumbnails and their details. The first video is titled "Hacking WEP Encryption" and has 4,234 views. The second video is titled "IEFD ep. 2 - Wireless Hacking - Cracking WEP" and has 131,005 views. The third video is titled "Hacking WEP by Đă@K" and has 66,728 views. The fourth video is titled "Wireless WEP Key Hacking" and has 66,728 views. On the right side of the page, there is an advertisement for AT&T, featuring a pink Nokia 6085 camera phone and the text "better than flowers".

YouTube - Broadcast Yourself. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address `http://www.youtube.com/results?search_query=hacking+wep&search_type=` Go Links >>

Google C Go Bookmarks 156 blocked Check AutoLink AutoFill Send to Settings

You Tube Broadcast Yourself™ [Sign Up](#) [QuickList \(0\)](#) [Help](#) [Log In](#) [Site:](#)


[Home](#) [Videos](#) [Channels](#) [Community](#)


hacking wep Videos Search [settings](#) [advanced search](#) [Upload](#)


"hacking wep" video results 1 - 20 of about 154


[Videos](#) [Channels](#) Sort by: [Relevance](#) Uploaded: [Anytime](#) Display:

 **Hacking WEP Encryption**
WEP being hacked. MORE: hacks1010.webs.com...hacks hacks1010 **hacking wep** wpa tsk cell phone upload
Added: 3 months ago
From: [sloggyman83](#)
Views: 4,234
★★★★★
01:47
More in [Education](#)

 **IEFD ep. 2 - Wireless Hacking - Cracking WEP**
To download a High quality version visit our website, www.infinityexists.com...Cracking 128 bit WEP aircrack airodump aireplay **hack hacking** Infinity Exists (more)
See duplicate videos
Added: 10 months ago
From: [Gregorpm](#)
Views: 131,005
★★★★★
04:42
More in [Howto & Style](#)

 **Hacking WEP by Đă@K**
Hacking WEP in anyone wireless network....kismet wireless **wep** aircrack **hacking**
See duplicate videos
Added: 1 year ago
From: [darkkill666](#)
Views: 66,728
★★★★★
03:36
More in [Sports](#)

 **Wireless WEP Key Hacking**
com For a **Hacking** Guide. This video
Added: 6 months ago
From: [jortes187](#)

 **at&t**
better than flowers
Give mom a **FREE*** Nokia 6085 camera phone
[Get a free phone](#)
*Signif. restrict. apply

Copyright 2

Done Internet

> All You Need to Break a WEP Key

Programs Used: (These are all free and easily downloaded online)

- Backtrack 2 Final- CD Bootable Linux Operating System with built in auditing/cracking tools
- Airodump- Captures wireless packets from access point
- Aireplay- Injects packets at the access point to create traffic and increase cracking speed
- Aircrack- Statistical algorithm to crack WEP 64/128 bit codes. Current version can crack 64bit in 2 minutes and 128bit in < 6.
- Aircrack-ng- Used to create an Evil Twin attack
- Ettercap- Man In the Middle Attacks, can also sniff data and

> 46% of Corporations Still Use WEP as a Standard

The reason is:

- It takes time, money and resources to setup a better WLAN infrastructure

Take these steps:

- Use an enterprise-grade WLAN solution, such as PEAP (802.1x), that requires authentication
 - Verifies identity
- Ensure all systems have an active personal firewall
- Ensure all devices are current and have AV and ASpyWare running

This may be a real Blind Spot!

> Relevance: Why Increase Visibility and Reach?

- Are devices safe for corporate connectivity?
 - Unsecured Internet everywhere
 - Home and WiFi hotspot exposures
- Do you know what's happening to proprietary data?
 - Will government compliance efforts be compromised?
- Do you know how and where users are connecting?
- New SaaS applications keep more mobile users off the LAN and out of sight
 - ADP, Concur, Salesforce.com
- You can not protect or fix what you can not see

> Summary: What's It All Mean To You?

- Increased mobility is creating new device and data threats
 - Insiders are becoming outsiders
- Mobile devices are the most vulnerable
- Economic challenges won't slow malicious efforts to get data
- Implement security solutions that reach the "unconnected users" – the Mobile Blind Spot
- Consider a cloud based solution to improve overall visibility where mobility is most vulnerable
 - Fewer resources to support
 - Better overall economics than purchasing hardware



Thank You

Please Stop By Our Display
For More Detail

Questions? STAYLOR@Fiberlink.com

FIBERLINK

Simple. Secure. Mobility.