



# The New “Insider” Threat

Extending Device and Data Protection  
to the Mobile Workforce

Charles Oliva  
Director of Marketing  
[www.fiberlink.com](http://www.fiberlink.com)

**FIBERLINK**

Simple. Secure. Mobility.

## > Last Slide First...

- 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 and control where mobility is most vulnerable
  - Economics allow you to get it done in 2009
  - It will support the mobile world that we are heading towards

# > Agenda

- Mobility Trends and Their Impact on IT
- The Challenges of Greater Mobility
  - Under Today's Market Conditions
  - Focus on Device & Data Protection
- Customer Approaches to Mobile Data

# > Fiberlink Corporate Overview



- **Company:**
  - Founded in 1994 and Headquartered in Blue Bell, Pennsylvania
  - Presence in North America, Europe, and Asia
- **Legacy of Leadership and Innovation:**
  - Mobility as a Service (MaaS)
  - Gartner Leadership Quadrant for 7 yrs in a row
  - Yankee's first Remote Endpoint Security solution
- **Product Platform:**
  - Scaling to millions of laptop-to-platform transactions each day
  - Unique approach to mobility management
  - Patented technology



# Mobility Trends and Their Impact on IT

**FIBERLINK**

Simple. Secure. Mobility.

Today, Everyone is Mobile

# > Fiberlink Research

1. What percentage of employees in your organization use a computer for work outside of the office (at home or traveling) at least once a week?

<i>Average = 48%</i>		
<i>Response</i>	<i>Total</i>	<i>%</i>
0	3	1%*
1-19%	58	17%
20-39%	86	26%
40-69%	85	26%
70-100%	101	30%



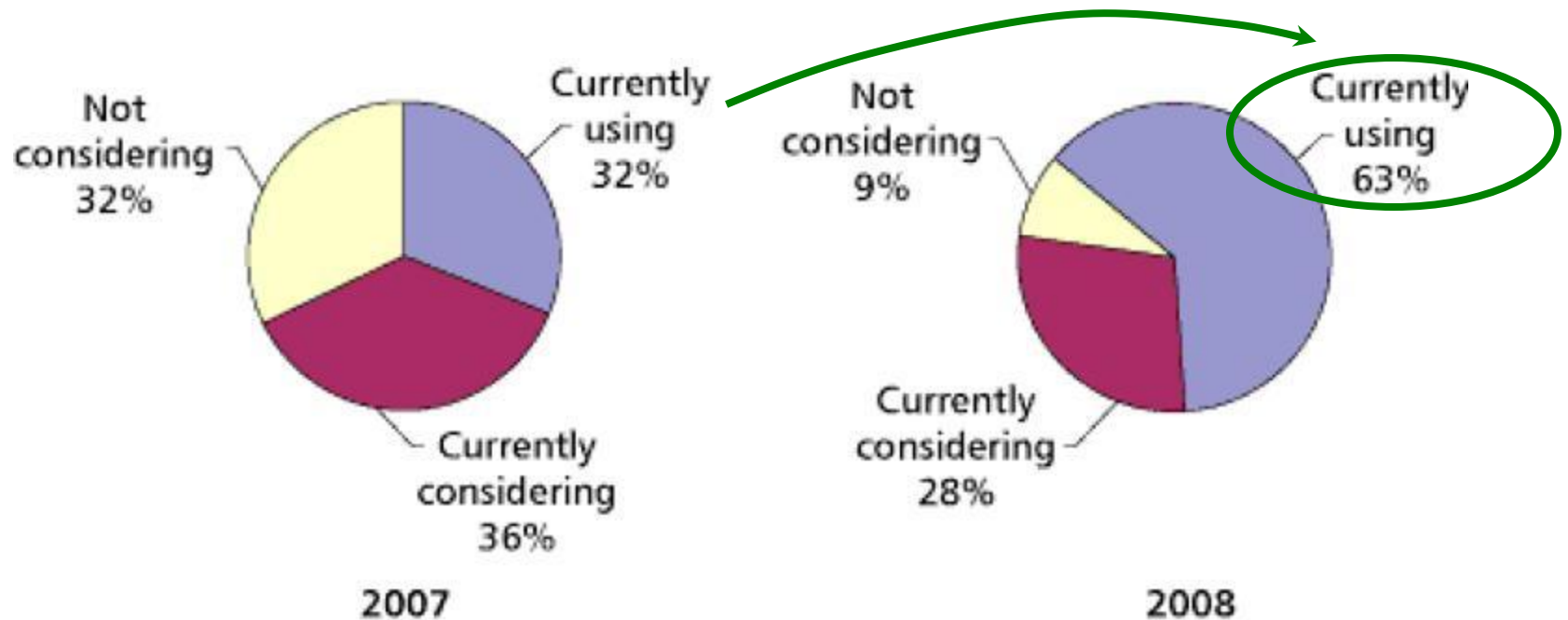
Today, Most of your Data is Mobile

## > IDC Research

**In 2005, over 60% of all corporate data was located on laptops and PCs**

# > Research from THINKstrategies

## Percent of Companies Using and Considering SaaS Solutions



Source: THINKstrategies/Cutter Consortium 2008.

Everyone is Mobile with Connectivity  
Plentiful – Office, Road, Home

Applications in the Cloud

Your Data is Everywhere

*Mostly*

This is Good  
^

But sure is Different



# The Challenges of Greater Mobility

**FIBERLINK**

Simple. Secure. Mobility.

# > A Market Shift is Underway

## Do You Know What This Is?



# > Here's Another View



**Everyone needs a more effective way to manage their mobile operations.**

# > The Issues Facing Enterprise IT

- Resources and capital are at a premium
- Current market conditions will fuel growth in aggressive vulnerability “attacks”
- Governmental regulations
- Lifestyle changes are forcing acceptance of mobile working
- Can IT control their devices and data?



FINRA

PCI

Sarbanes



**\$10 - \$150**

**\$.05 - \$5**

# > 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**

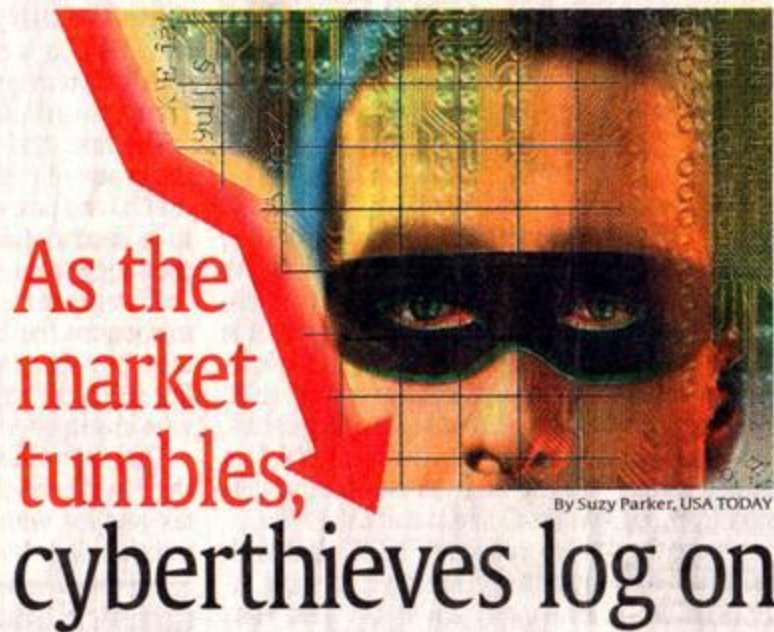
**Price range per stolen credit card**

Source: 2008 Symantec Internet Security Threat Report Trends

# > The Economy Is Not Slowing Cybercrime



Thursday, January 29, 2009



## Data-stealing scams have kicked into high gear since last fall

By Byron Acohido and Jon Swartz  
USA TODAY

Cybercriminals have launched a massive new wave of Internet-based schemes to steal personal data and carry out financial scams in an effort to take advantage of the fear and confusion created by tumbling financial markets, security specialists say.

The schemes — often involving online promotions touting fake computer virus protection, get-rich scams and funny or lurid videos — already were rising last fall

when financial markets took a dive. With consumers around the world panicking, the number of scams on the Web soared.

The number of malicious programs circulating on the Internet tripled to more than 31,000 a day in mid-September, coinciding with the sudden collapse of the U.S. financial sector, according to Panda Security, an Internet security firm.

## Cover story

It wasn't a coincidence, says Ryan Sherstobitoff, chief corporate evangelist at Panda.

"The criminal economy is closely interrelated with our own economy," he says. "Criminal organizations closely watch market performance and adapt as needed to ensure maximum profit."

Please see COVER STORY next page ▶



## Websense: Number of compromised websites at all-time high

January 21, 2009

### 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

# > Mobile Data and Device Protection in 2009

## Making A Smart Decision is Challenging

### Data/Device Protection

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

### Status Quo

1. No new investments
2. ROI and quick win priority
3. Operating cost reductions

**IT Spend**





# Customer Approaches to Mobile Data

**FIBERLINK**

Simple. Secure. Mobility.

# > Fiberlink Best Practice

## **An Approach to Mobile Data and Device Protection:**

1. Inventory and prioritize your concerns/risks
2. Establish required policies
3. Educate your employees
4. Put technical safeguards in place
5. Have real-time visibility into your users, devices, and policies
6. Automate compliance reporting and updates

# > Mobile Devices/Users Are Targets

Data In Motion:



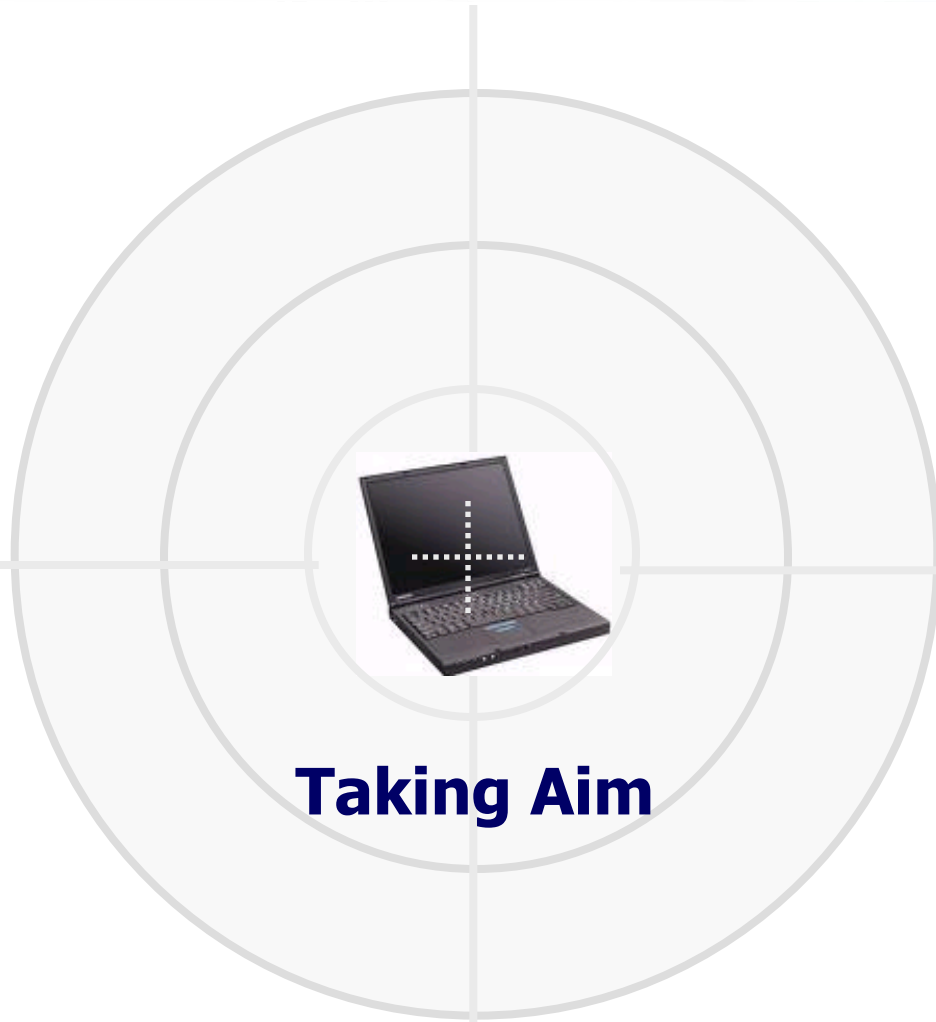
Wireless Hacking:



Lost Device:



Stolen Laptop:

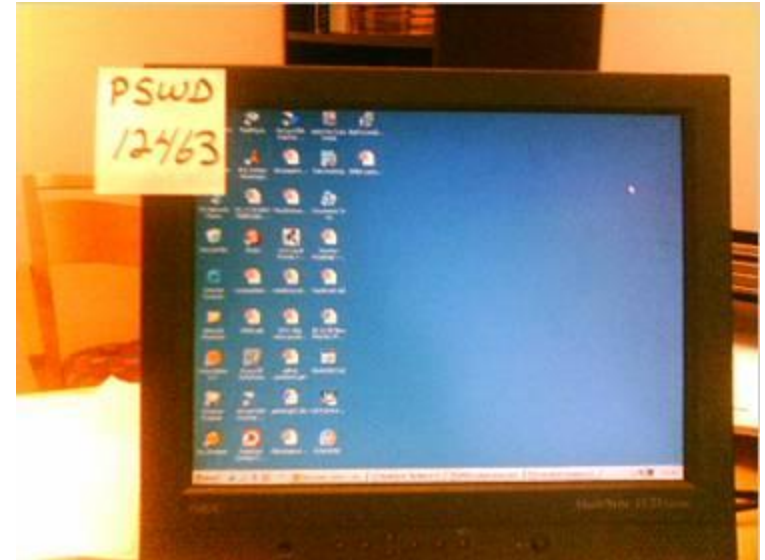
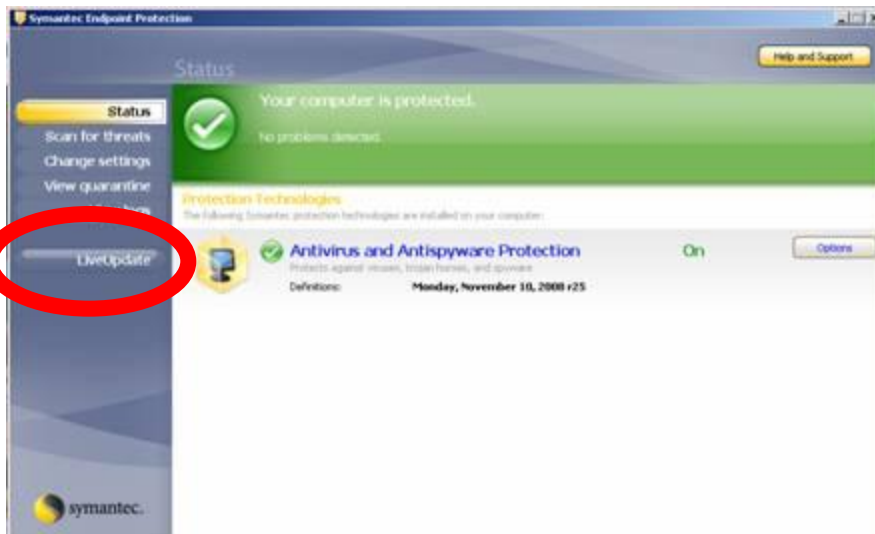


**Taking Aim**

> “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

# > Best Practice Method for Success

1. Inventory and prioritize your concerns/risks
- 2. Establish required policies**
3. Educate your employees
4. Put technical safeguards in place
5. Be able to see if things are working or not in real-time
6. Automate compliance reporting and updates

# > PCI DSS standard

Offers good practical technical safeguards...

## **Here are the 12 primary requirements of the PCI DSS :**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

# > California SB 1386

## California SB 1386 – Personal Information: Privacy

SB 1386 goes into affect on July 1, 2003. Under the law, covered parties must disclose any breach of the security of personal data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The law applies to state agencies, or a person or business that conducts business in California, that owns or licenses computerized data containing personal information.

The bill would permit the required notifications to be delayed if a law enforcement agency determines that it would impede a criminal investigation.

The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data.

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the organization.

Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

"Personal information" means an individual's (first name or first initial) and last name in combination with any one or more of the following data elements, if either the name or the data elements are not encrypted:

1. Social security number
2. Driver's license number or California Identification Card number.
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Remember your vendors have  
your data

On their laptops and USB  
sticks, likely

# > Best Practice Method for Success

1. Inventory and prioritize your concerns/risks
2. Establish required policies
- 3. Educate your employees**
4. Put technical safeguards in place
5. Be able to see if things are working or not in real-time
6. Automate compliance reporting and updates



Make it fun and personal

# > Best Practice Method for Success

1. Inventory and prioritize your concerns/risks
2. Establish required policies
3. Educate your employees
- 4. Put technical safeguards in place**
5. Be able to see if things are working or not in real-time
6. Automate compliance reporting and updates

## > Don't think too narrowly

- Data encryption, data-leak prevention, USB security are very important
- But, so is:
  - Up-to-date and ON anti-virus / malware and firewalls
  - Effective and regular patching of mobile devices
  - Access controls (even on the Internet)
  - Real-time visibility & control
    - Can you reach and wipe your laptops?

# > Phased Approach to Mobile Data and Device Protection

*Defend against network-based threats and phishing*

- Zero-Day Protection
- Intrusion Prevention
- Anti-Spyware
- Anti-Virus
- Firewall

**2**

*Defend against loss and theft (Data at rest)*

- Data encryption
- Backup and recovery

**3**

*Defend against user policy violations (Incl. data in motion)*

- Device control
- Information protection

**4**

- 1** Endpoint monitoring and remediation, patch management, vulnerability management, inventory management

*Improve administration; Support other defenses*

## > 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

## > Recent Customer Examples

### Initial Motivation – 3 flavors

1. Trying to meet specific regulations
2. Trying to protect your IP and customer data
3. Reacting to a breach of some type

# > Back to our Customers

<b>Their Motivation</b>	<b>Chosen Technical Safeguards</b>	<b>Some Keys to Get Correct</b>
Meet specific regulations	<ul style="list-style-type: none"><li>• Full endpoint security</li><li>• Encrypt your laptops and USBs</li></ul>	<ul style="list-style-type: none"><li>• Deployment ease</li><li>• Update ease</li><li>• Easy ability to prove</li></ul>

# > Back to our Customers

<b>Their Motivation</b>	<b>Chosen Technical safeguards</b>	<b>Some Keys to Get Correct</b>
Meet specific regulations	<ul style="list-style-type: none"><li>• Full endpoint security</li><li>• Encrypt your laptops and USBs</li></ul>	<ul style="list-style-type: none"><li>• Deployment ease</li><li>• Update ease</li><li>• Easy ability to prove</li></ul>
Protect IP and customer data	<ul style="list-style-type: none"><li>• Data Leak Prevention</li><li>• Remote visibility and control</li></ul>	<ul style="list-style-type: none"><li>• Heuristic-based, not context</li><li>• Easy to update</li></ul>

# > Back to our Customers

<b>Their Motivation</b>	<b>Chosen Technical safeguards</b>	<b>Some Keys to Get Correct</b>
Meet specific regulations	<ul style="list-style-type: none"><li>• Full endpoint security</li><li>• Encrypt your laptops and USBs</li></ul>	<ul style="list-style-type: none"><li>• Deployment ease</li><li>• Update ease</li><li>• Easy ability to prove</li></ul>
Protect IP and customer data	<ul style="list-style-type: none"><li>• Data Leak Prevention</li><li>• Remote visibility and control</li></ul>	<ul style="list-style-type: none"><li>• Heuristic-based, not context</li><li>• Easy to update</li></ul>
React to a breach of some type	<ul style="list-style-type: none"><li>• Encrypt your laptops and USBs</li><li>• Remote visibility and control</li></ul>	<ul style="list-style-type: none"><li>• Speed</li><li>• Ability to support intense audits, easy</li></ul>

# > Best Practice Method for Success

1. Inventory and prioritize your concerns/risks
2. Establish required policies
3. Educate your employees
4. Put technical safeguards in place
- 5. Be able to see if things are working or not in real-time**
- 6. Automate compliance reporting and updates**

# > Today's Architectures...

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

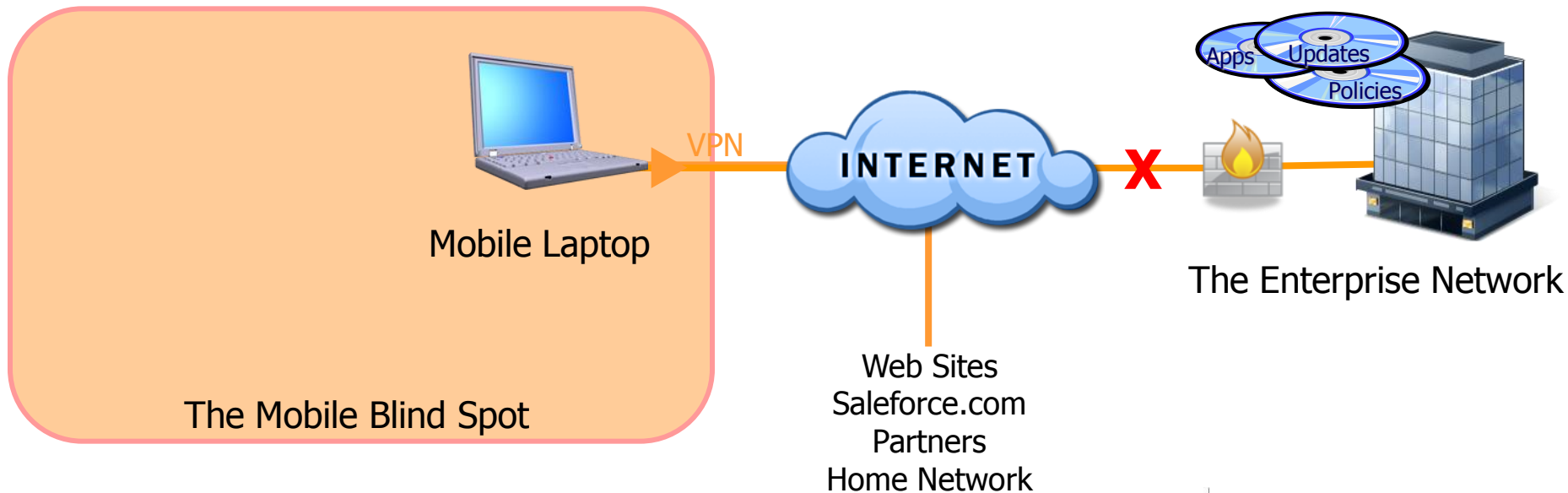


# > ...Are LAN-Locked

LAN-based architectures rely on a connection to the corporate network to receive updates, new policies, applications and to generally be in control of IT

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

IT is not in Control



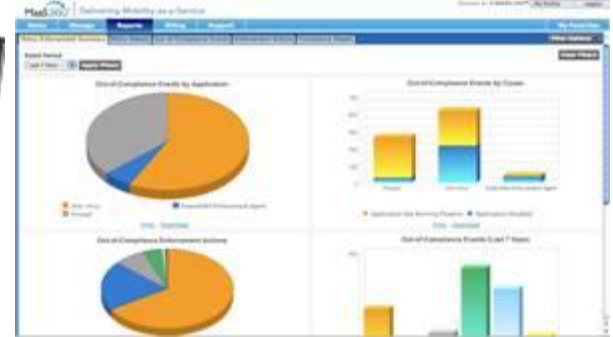
## > An approach for 2009

1. Inventory and prioritize your concerns/risks
2. Establish required policies
3. Educate your employees
4. Put technical safeguards in place
- 5. Be able to see if things are working or not in real-time**
- 6. Automate compliance reporting and updates**

# > Highly Mobile / Light on Resources

Data and Device  
Protection  
EVERYWHERE

Fiberlink MaaS360™



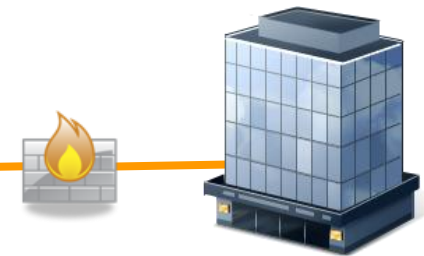
IT is in Control



The Mobile Blind Spot



Web Sites  
Salesforce.com  
Partners  
Home Network



The Enterprise Network

# > Benefits of a Managed Platform

- Protects the corporate network and data
  - Secures your data
  - Blocks non-compliant systems from connecting
- Addresses the “mobile blind spot”
  - Monitors, protects and updates mobile computers everywhere
- TCO and ROI of SaaS / the Cloud
  - Versus large infrastructure build outs and maintenance
  - Plus, many other productivity and efficiency gains
- Real-time visibility and compliance
  - Visibility to know you’re in control
  - Complete compliance report / audit trail

# > The Last Slide - Summary

- 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 and control where mobility is most vulnerable
  - Economics allow you to get it done in 2009
  - It will support the mobile world that we are heading towards



Thank You



Please Stop By Our Table  
For More Detail

Questions? [coliva@fiberlink.com](mailto:coliva@fiberlink.com)

**FIBERLINK**

Simple. Secure. Mobility.