Hack In The Box 2007 - Dubai
Ahmad Elkhatib

Securing Your Data On The Move

khatib@umich.edu

Who, from the audience, uses these devices?

Who, from the audience, has lost one of these devices?

Why Secure Data?

What does it cost your company to be in the papers with a security breach?

- Loss of reputation and image
- Reduced ability to attract and retain customers

Regulations may apply as well

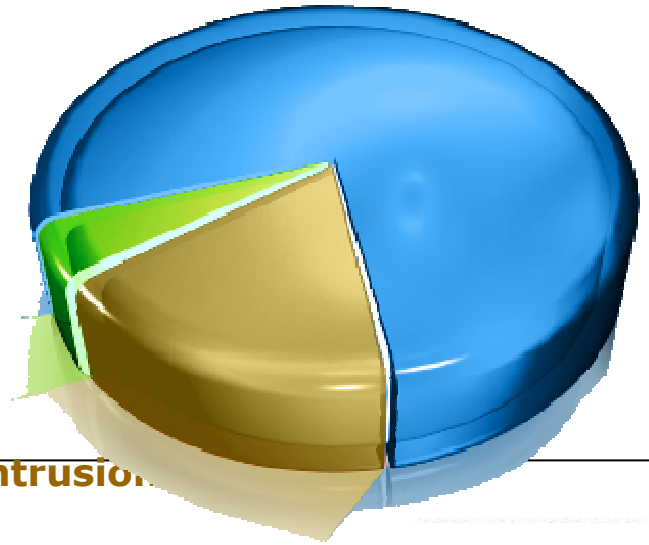
- Personal Privacy Laws: 33+ US States w/ personal privacy laws, HIPAA, PIPEDA (Canada)
- Governance laws such as: SOX, GLBA, Basel II (Europe), Data Protection Act (UK), Personal Information Protection Law (Japan) Privacy Act (Australia)
- HSPD12, FISMA (US Government)

Ensure company trade secrets and proprietary information are fully protected

Why Secure Data? – Network vs. Endpoint Security

- Old assumptions about security policy should be re-visited due to mobility trends
- Traditional endpoint threats include:
  - Virus
  - Worm
  - Network attack
- New security concerns include:
  - Porous wireless networks
  - Frequently disconnected computers
  - Large volumes of data outside the physical security perimeter

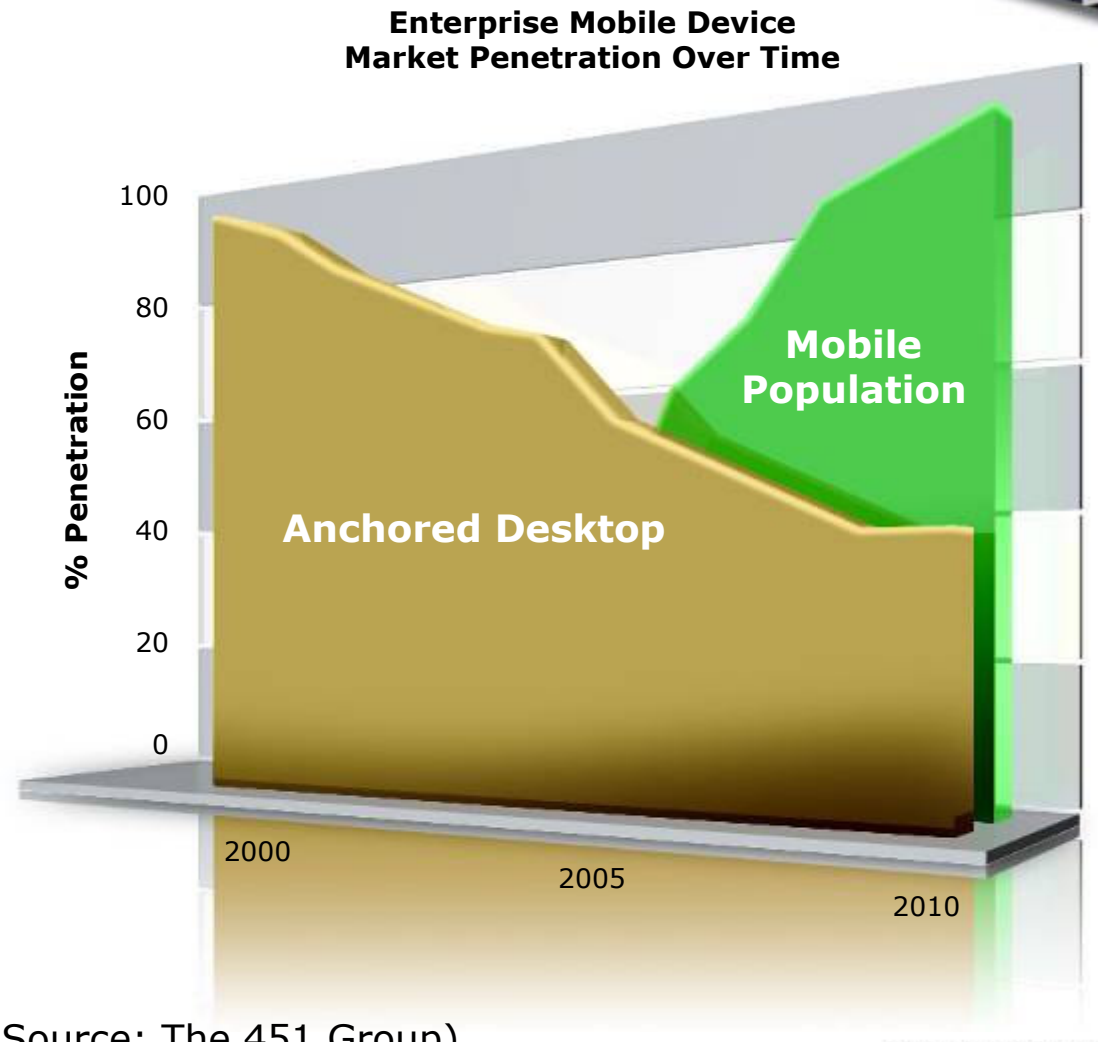
Reported Information Loss
Jul - Dec 2005
(Source: Privacy Rights Clearinghouse)



Why Secure Data? – Mobility Is The Future

Factors Driving Trend:

- Dropping cost of notebook PCs
- Growing availability of high-speed wireless network access
- Advancements in Internet application platforms
- Proliferation of push e-mail to smartphones and PDAs



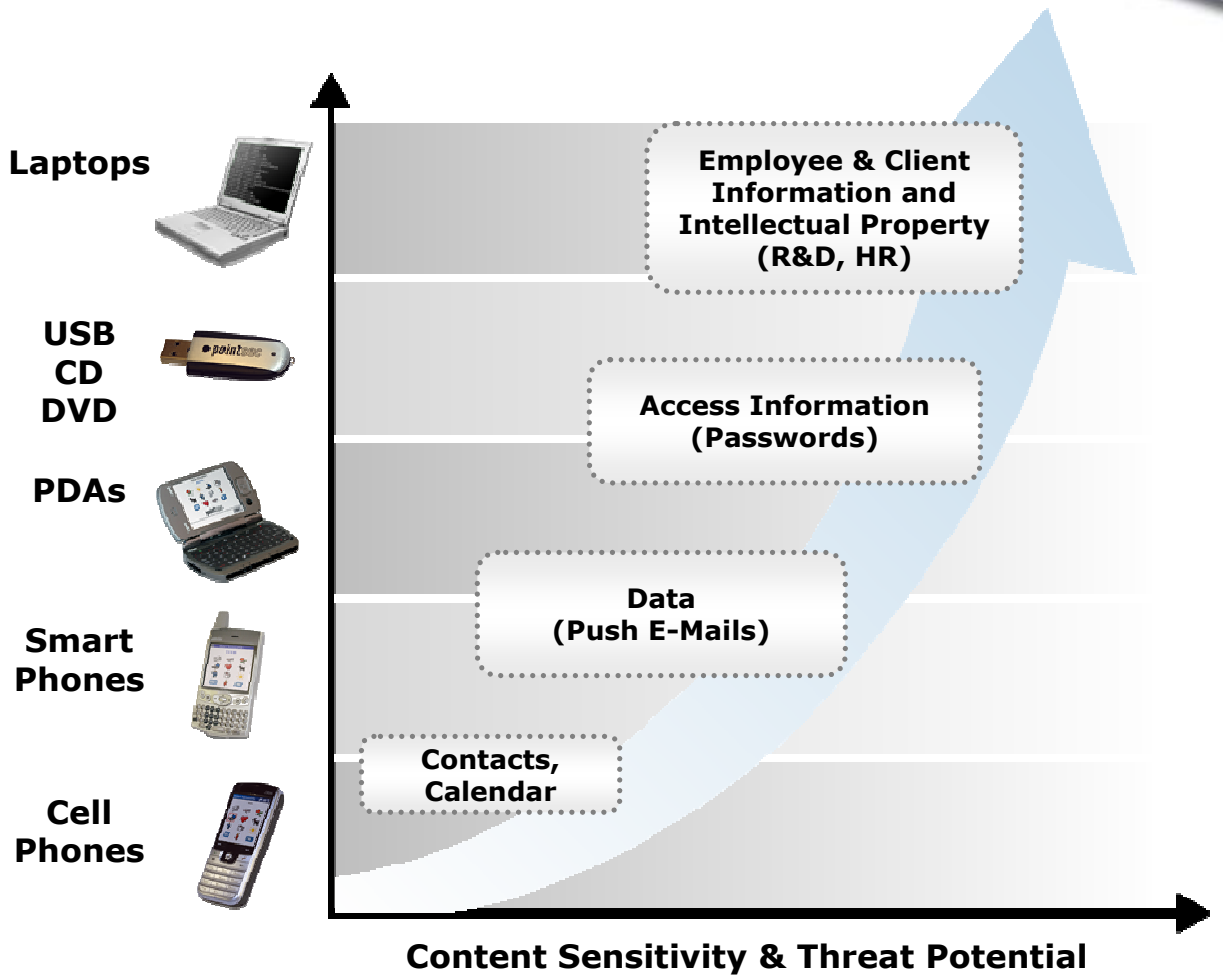
(Source: The 451 Group)

Mobile Device Hierarchy

Climbing Up Mobile Device Complexity

Enables:

- Faster processing (Remote work on large files)
- More wireless network connection options (Access to company data)
- Increased storage capacity (Sensitive data at risk)

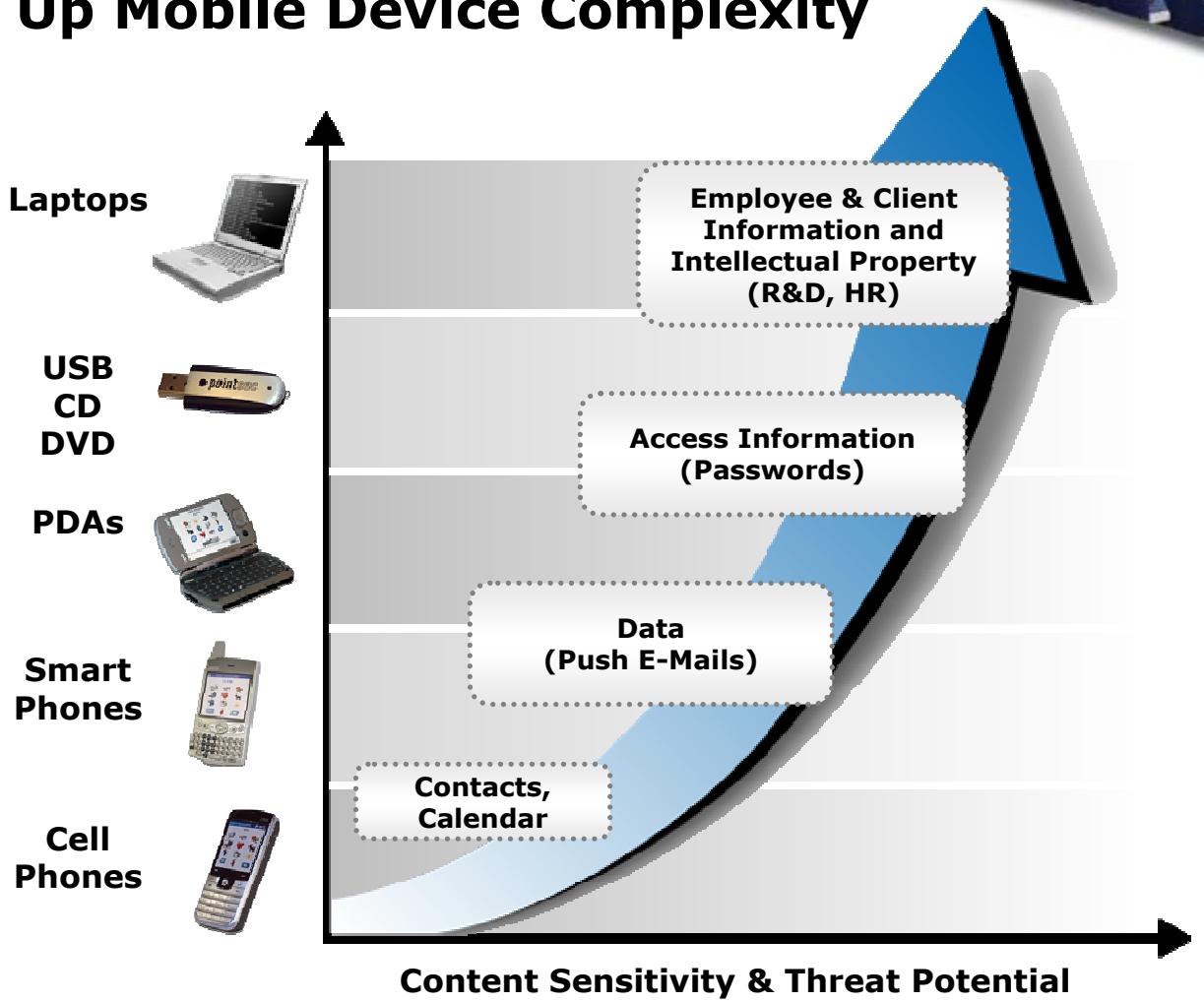


Mobile Device Hierarchy

Climbing Up Mobile Device Complexity

Enables:

- Faster processing (Remote work on large files)
- More wireless network connection options (Access to company data)
- Increased storage capacity (Sensitive data at risk)



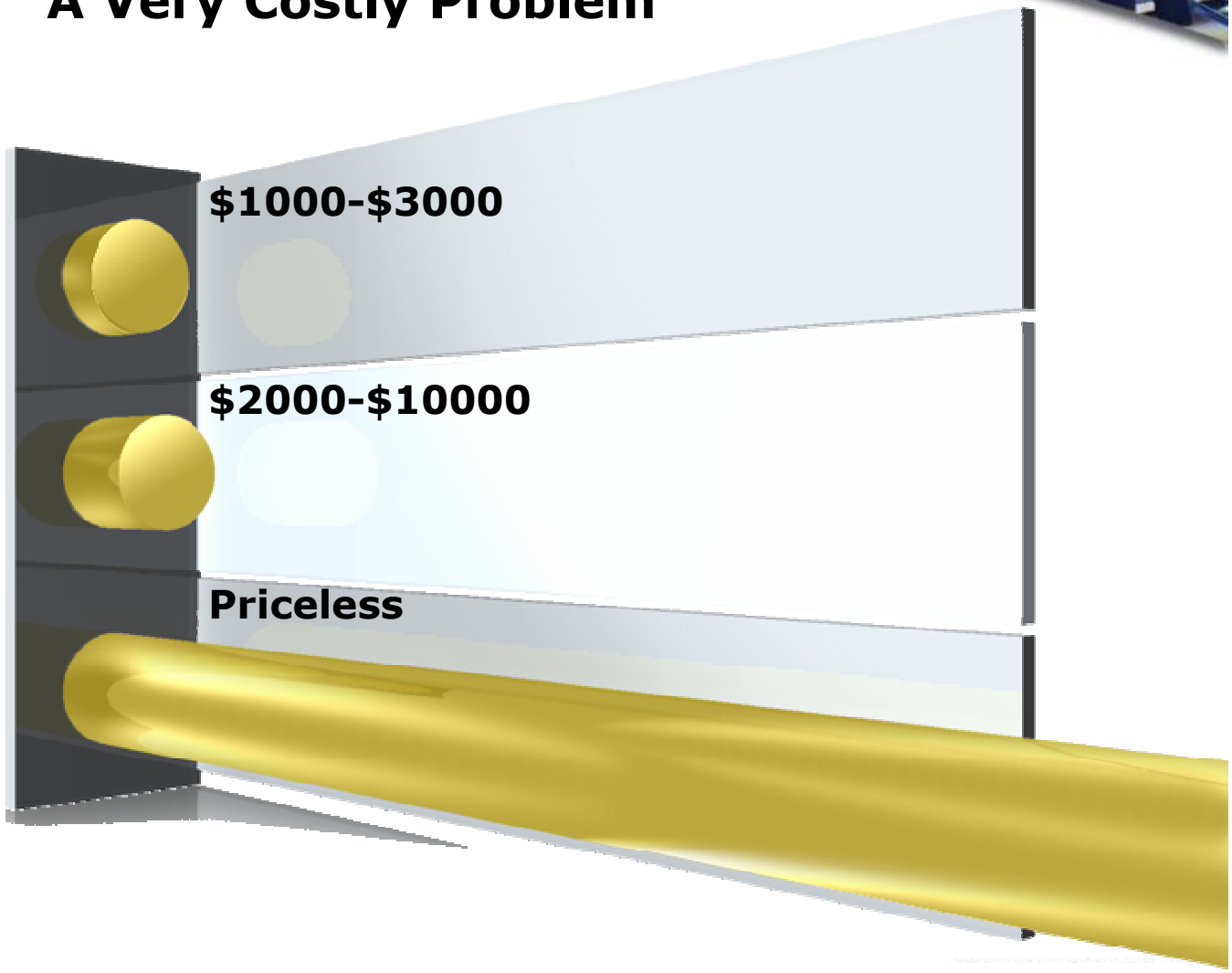
Cost Impact of Lost Equipment

A Very Costly Problem

Replacement
Hardware
Software

Recovery
Police report
Insurance claim
Data recovery effort
User downtime

Image
Damaged reputation
Resulting lawsuits
Loss of customers
Lost shareholder confidence



Global Statistics

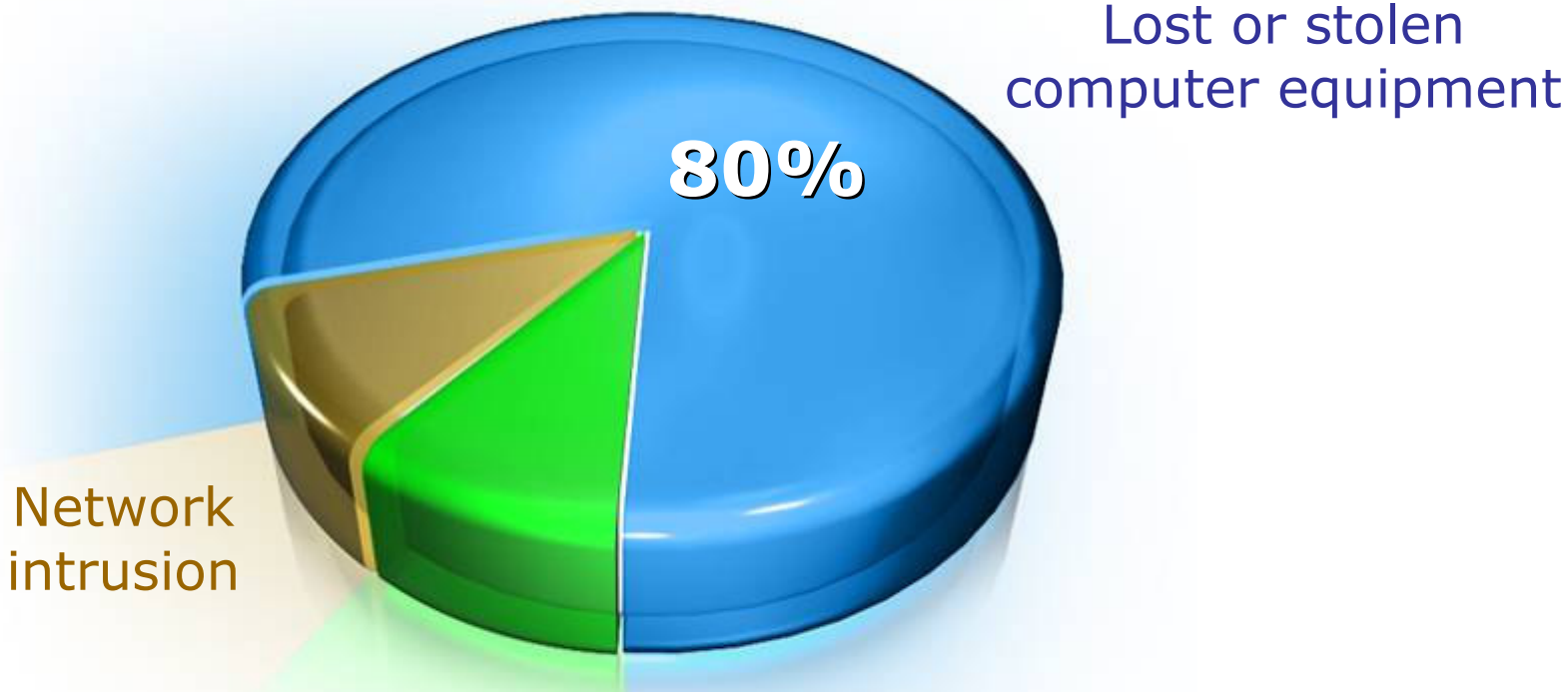
A Symantec report suggests that an ordinary laptop holds content valued at **$972,000**, and that some could store as much as **$8.8 Million** in commercially-sensitive data and intellectual property

One enterprise client estimated the value of data lost on a single laptop computer at

$7 Million

Global Statistics

Information Loss



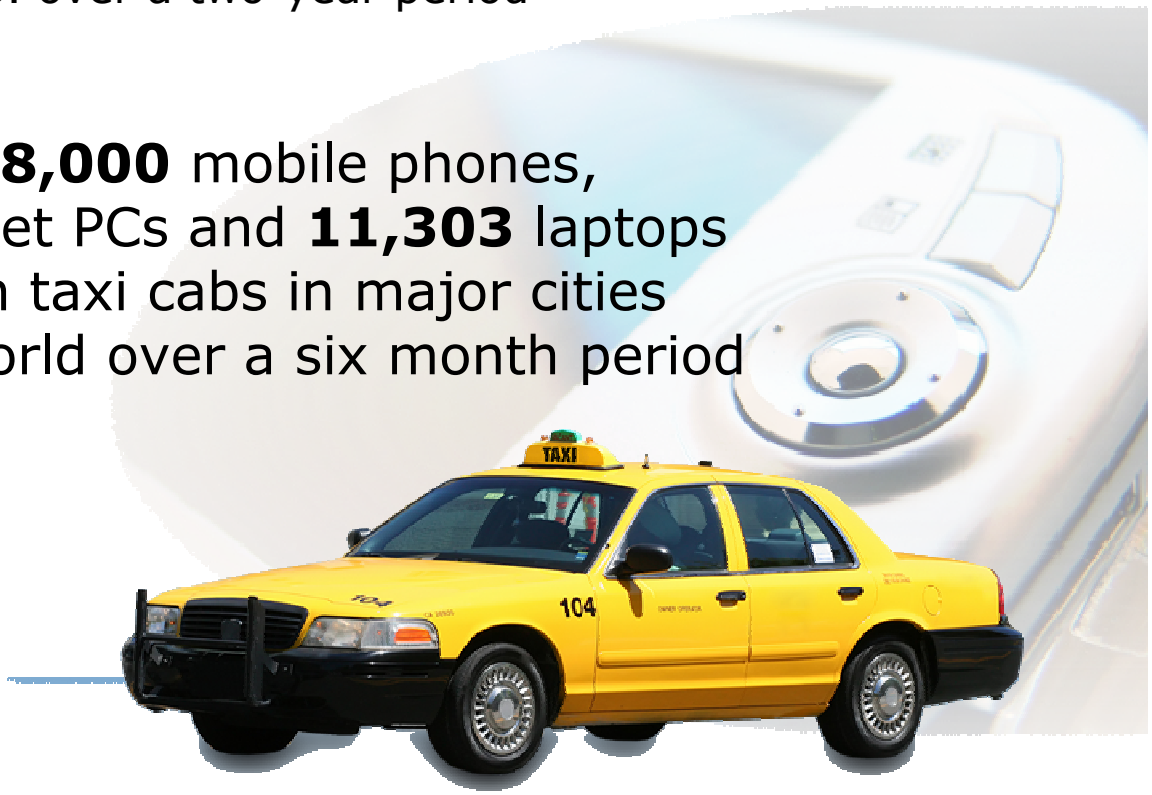
Of that 20%, half of those intrusions are made with network credentials from lost and stolen equipment

(Source: Kensington Group)

Global Statistics

According to Gartner, 47% of corporate data resides on mobile devices, and **350,000** mobile devices were lost or stolen in the U.S. over a two-year period

Over **208,000** mobile phones, **31,469** pocket PCs and **11,303** laptops were left in taxi cabs in major cities around the world over a six month period



Primary Research

100 used devices where purchased on eBay and at airport auctions

All of them had **"supposedly"** been **"wiped-clean"** or **"re-formatted"**

We were able to recover data on **7 out of 10 devices**

We found interesting data, including:

Personal and customer databases, payroll, HR, personnel details, login codes, administrator passwords, emails and more

Public Exposure & Impact

Recent CNN Moments

BANK OF AMERICA LOSES 1.2 MILLION CUSTOMER INFORMATION

CHOICEPOINT IS FINED 15.6 MILLION DOLLARS BY THE FTC FOR PERSONAL DATA LOSS

VA LOSES 26.2 MILLION VETERAN'S IDENTITIES

FIDELITY INVESTMENTS LOSES 254K HP EMPLOYEE'S DATA

AMERIPRISE FINANCIAL LOSES 226K CUSTOMER AND EMPLOYEE'S DATA

Compliance & Legislation

Examples of legislation that address the protection of sensitive data. Other laws and regulations exist and new ones are being defined by governments around the world.

Compliance & Legislation

95/46/EC (Europe)

European Union Directive 95/46/EC

Compliance & Legislation

DPA (UK)

Data Protection Act

Compliance & Legislation

Georgia Senate Bill 245 & HB 1368 (US)

Health Insurance Portability Act

Compliance & Legislation

Japanese Law (Japan)

Personal Information Protection Law

Compliance & Legislation

PIPEDA (Canada)

The Personal Information Protection & Electronic Documents Act

Compliance & Legislation

Privacy Act 1988 (Australia)

Mobile Data Platforms

PC & Linux laptops

Complete Data Protection

Full Disk Encryption

FDE Technology

- Hardware
  - Seagate
  - Stonewood FlagStone
- Software
  - Pointsec (acquired by Checkpoint)
  - Utimaco
  - Safeboot
  - GuardianEdge
- Operating System
  - Windows Vista BitLocker

Hardware

- Built-in Application Specific Integrated Circuit (ASIC) that performs the bulk encryption and decryption of the data on the drive platters
- Pre-boot authentication
- Keys stored on part of drive only accessible by user
- OS independent
- Key is stored using the TPM

However

- Key Management / Recovery
- Hard disk recovery
- Hardware Investment

Software

- Kernel level drivers for encryption/decryption
- Pre-boot authentication
- Central Management
- Password recovery
- Directory Integration

However

- Interoperability
- Platform dependant
- Performance

Operating System

- No third party software needed
- Can be controlled by Active directory
- Pre-boot authentication (option of using USB key)

However

- Large investment in new software and hardware
- Encrypts only boot partition
- Requires Enterprise version of Vista and Service Agreement
- Could be extended to DRM functionality

Must have features

- **Initial Encryption Rate not more than 8 hours**
  - Regardless of info amount on the hard drive
  - Only 3-5% system performance degradation after disk is fully encrypted (Invisible to the end user)
  - Configurable algorithm – AES, CAST, Blowfish, 3DES
- **Throttled Background Encryption Service**
  - Low priority process
  - Allows other applications priority to access processor
  - Continued end user productivity
- **Fault Tolerant**
  - User may shut down during encryption process
  - Power outage does not effect encryption process
- **Highly Scalable, Easy To Deploy & Manage And Enforceable**
  - User may not un-install without administrator approval
  - Lowers total cost of ownership (Configure and forget)
- **Suspend, Hibernation, Mouse Support**

Recovery

- Unique key for each device
- No master key vulnerability
- Created automatically at installation
- Updated automatically when changes occur
- Requires 2 authorized administrators to recover
- Enterprise can always recover a workstation

More Must have features

- **4 Methods of Recovery**
  - User forgot password?
  - User left company?
  - Operating system died?
  - Catastrophic Failure?
- **Slave Hard Drive After Authentication**
  - Login from another Pointsec encrypted machine
- **Enterprise Access**
  - Works with forensics tools
- **Imaging**
  - Re-image Boot Volume with Windows
  - Create new "Gold" images w/ Ghost
- **Multifactor Authentication**
  - Authentication at preboot with USB tokens and/or smart cards

Centralized & Automatic Logging

- Automatic transfer of logs to central location
- Central viewing of encrypted log files
- Integrates with Windows Event Viewer and/or syslog
- Counting of active clients
- Ability to export logs

Product Portfolio – Encryption Solutions

Protecting Removable Media

How to protect

- Pour glue ?
- Procure PCs without any data ports
- Active Directory group policy
- Third party software
  - Centennial Software Device Wall
  - Pointsec Device Protector (f.k.a Reflex Disknet Pro)
  - Securewave Sanctuary
- On device encryption chip
  - LaCie SAFE
  - Kingston
  - Safeboot for USB
  - SECUREDISK
  - … many other hardware vendors

Protection of Data on Removable Media

- Runs automatically and transparently to user
- Central policy management
- Gives ability to block, filter or give read only access to ports
- Whitelist and/or blacklist ability
- Option to Encrypt data as well as access it when offline or on another machine
- Remote help available for media and encrypted packages if password is forgotten

Other Avenues of Data leakage

- Infrared
- Bluetooth
- WiFi networks
- PCMCIA
- Serial

* *Removable media detected as such by operating system*

Mobile Data Platforms

Protecting PDA Platforms

Mobile Devices – Key Features

- **Real-Time Encryption**
  - Automatic on-the-fly encryption of all data stored on a device, including encrypting Microsoft Outlook® data (E-mail, Calendar & Contacts)
  - Persistent storage encryption
- **Removable Media Encryption**
  - Entire disk encrypted
  - Cards can be shared
- **Unencrypted Media Policy**
  - Enable organizations to allow / disallow use of unencrypted removable media
- **Enforceable Mandatory Access Control**
  - Prevents unauthorized use of the device and prevents the authorized user from uninstalling security software