INFORMATION SECURITY SearchSecurity.com INFORMATION SECURITY DECISIONS

Five Steps To Securing Mobile Devices

Joel Snyder

Senior Partner, Opus One

jms@opus1.com

OPUS one

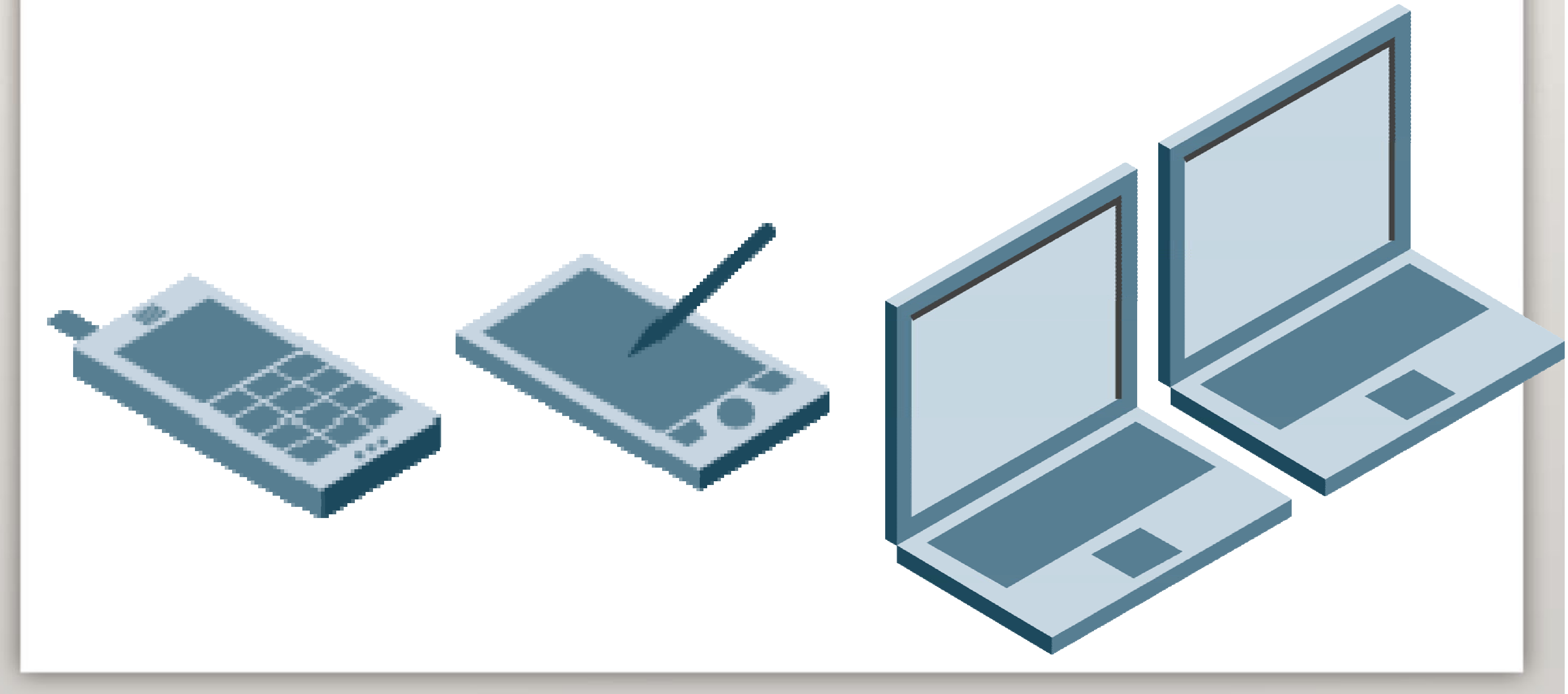
Agenda

- **Overview: stating the obvious**
- **Plan A**
- **Plan B**
  - Policy
  - Technologies for Data Protection
  - Malware Protection
  - Authentication

Thanks to Andy Briney and Craig Mathias for helping prepare this!

Mobile Devices Means…

- Smart Phones & Laptops
- But mostly Smart Phones



Insert Statistics Here

47% of corporate data resides on mobile devices

350,000

Mobile devices lost or stolen over a 2 year period

(stolen from: Dean Ocampo)

Insert More Statistics Here

Data Loss Impact

Averages $140 Per Customer

Direct costs - $50 per customer
(Legal, notification, etc.)
Indirect costs - $15 per customer
(Lost employee productivity)
Opportunity costs - $75 per customer
(Loss of customer and recruiting new one
Government Fines; Regulatory Actions
Exposure to legal action
Shareholder value loss
Diminished Goodwill
33 States with Legislation

(stolen from: Dean Ocampo)

Plan A

Solve Mobility Security by Forbidding Use of Mobile Devices

Plan B

Use Policy and Technology to Provide Mobility … Securely!

Five Pieces of Mobility Security

- Policy for Mobile Devices
- Technology to Protect Data in Motion
- Technology to Protect Data at Rest
- Protection From Malware
- Authentication

FIRST: Start By Building Policy

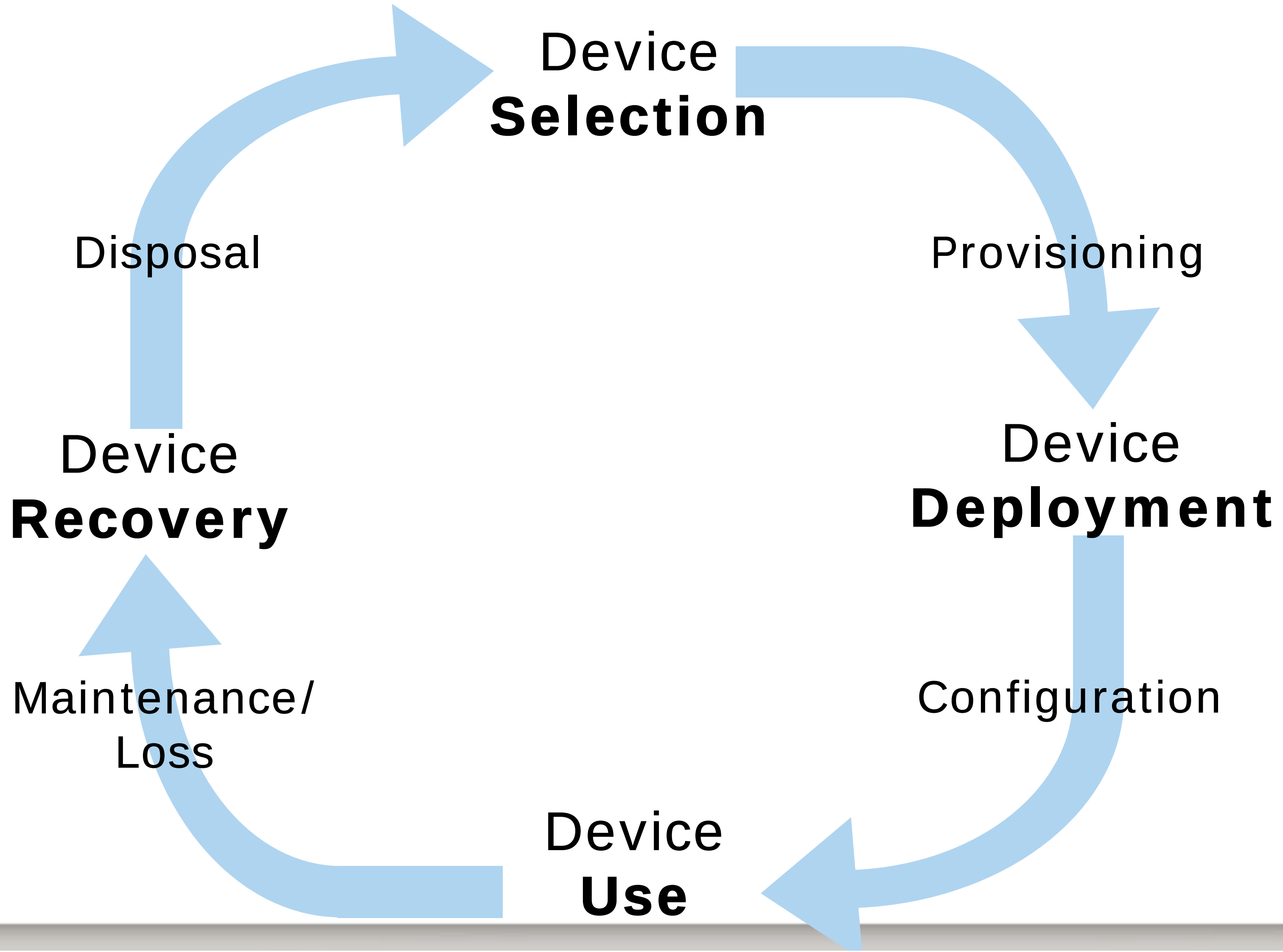
- **Without a policy…**

No Advice: “Employee IT” inefficient

Liability for Loss: Negligence? PCI 1.1?

No Boundaries: Anything Goes!

Policy Covers Lifecycle of Devices



Device **Selection**

Provisioning

Device **Deployment**

Configuration

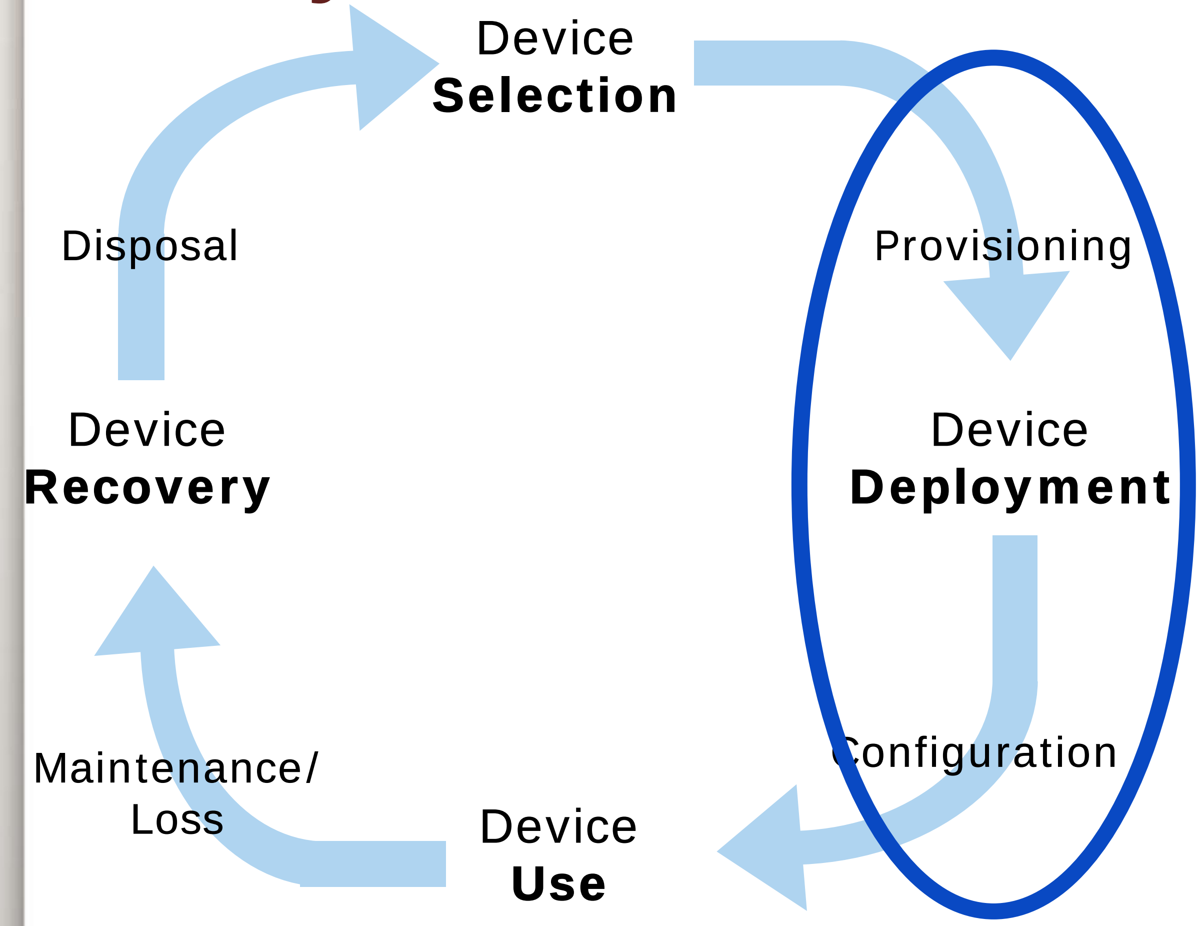
Device **Use**

Maintenance/ Loss

Device **Recovery**

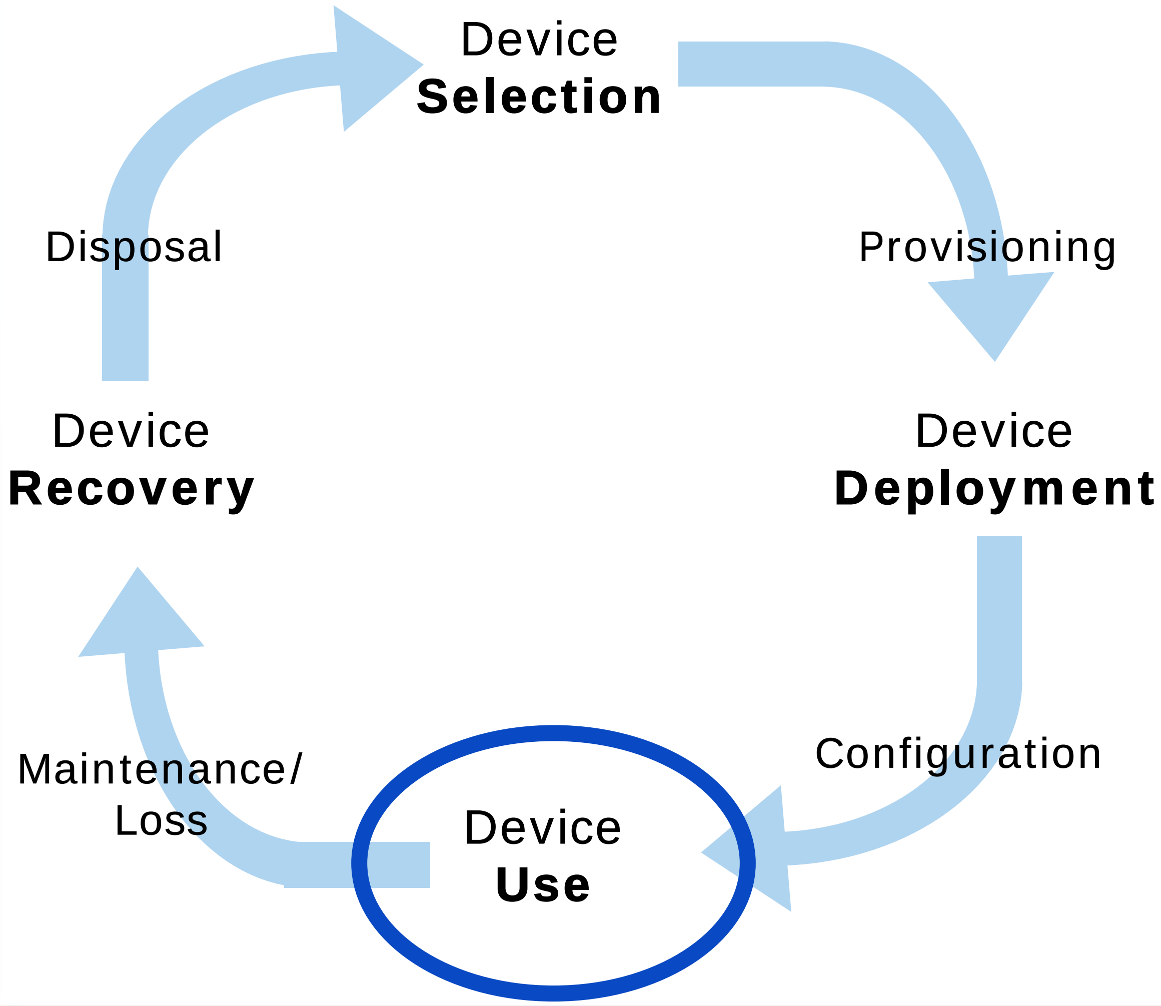
Disposal

Technology Can Support Your Policy



This is Mostly <u>Technology</u>

Users Must Support Your Policy



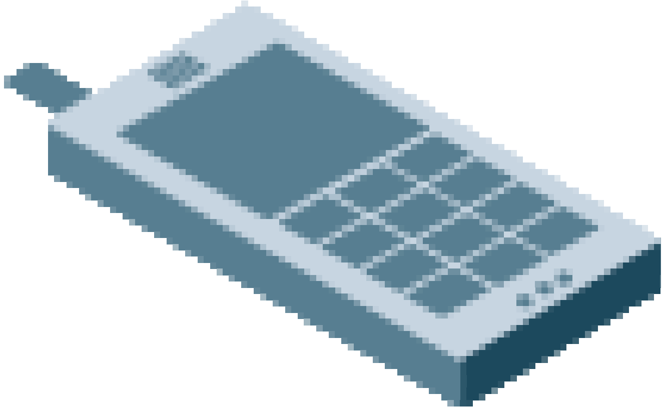
Device Use includes:

User signing an Acceptable Use Policy (AUP)

User being educated about and buying into security issues

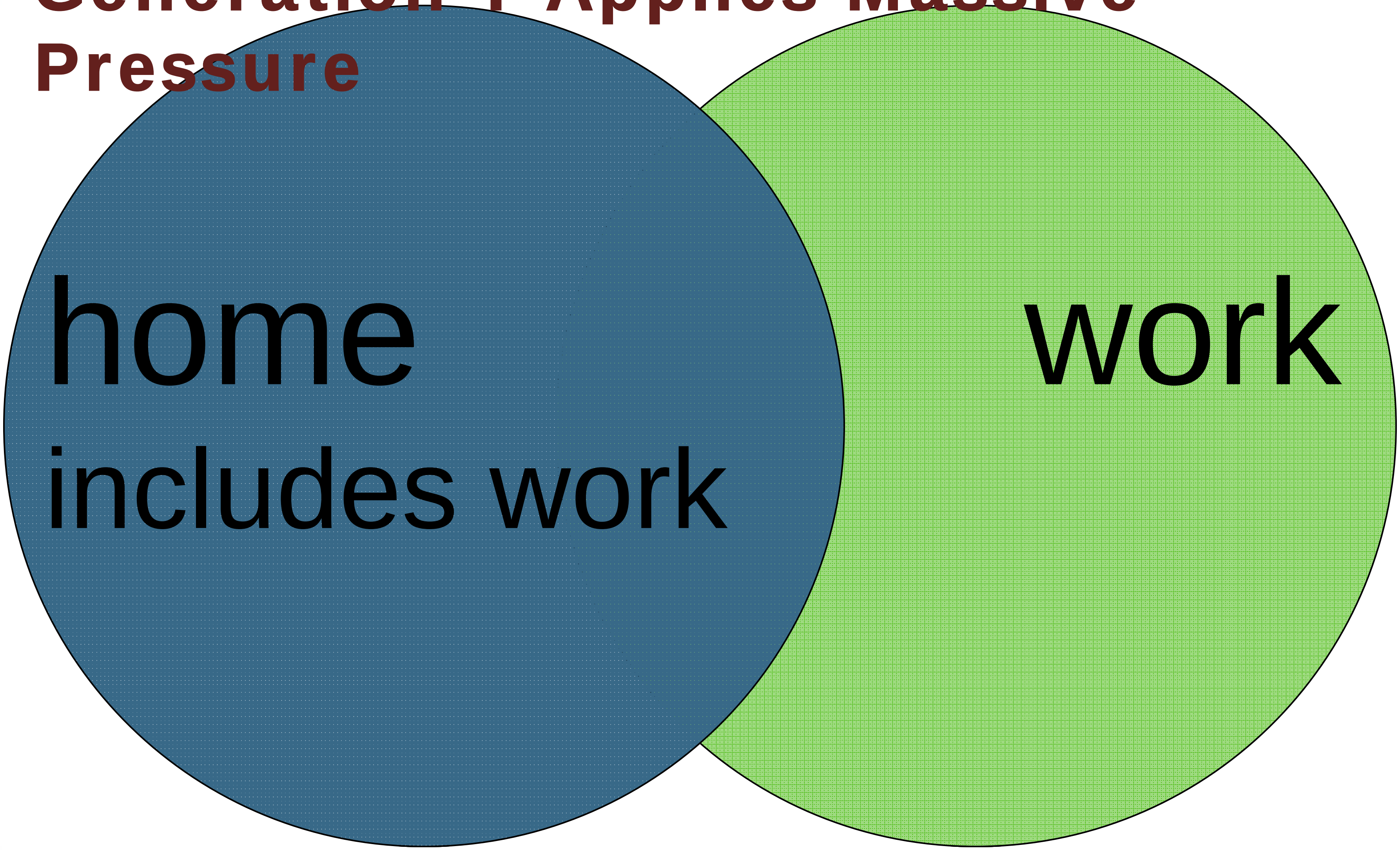
The Most Fundamental Policy Decision Is

Who "Owns" This Phone?



Don't screw up for the sake of having the coolest device!

Generation Y Applies Massive Pressure



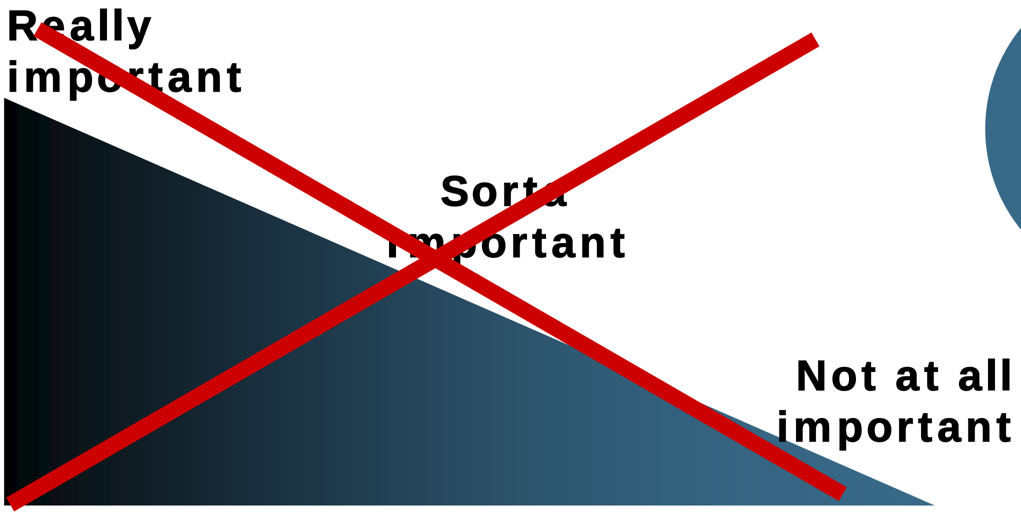
home

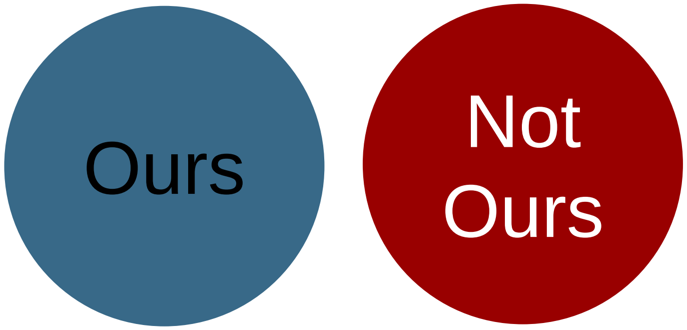
includes work

work

SECOND: Nothing Important Moves Unencrypted

- There is no spectrum of “important” to “unimportant”
- If you originated the data, we define it as “important”





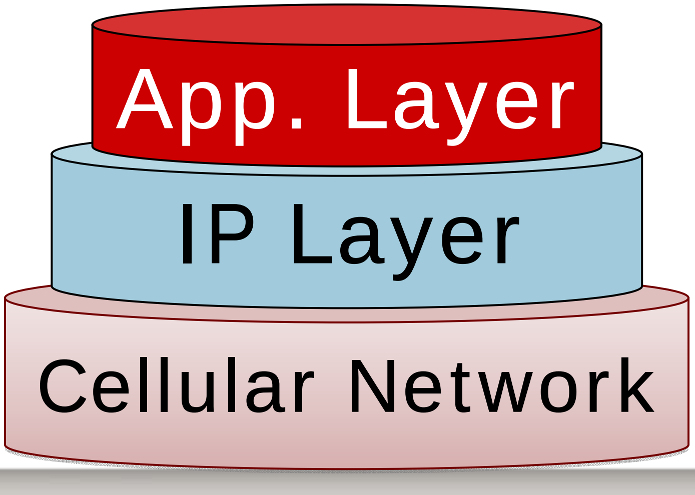
“Moving” Means Any Wireless Communication

- Mobile Data Services have a relatively lower risk, but must be protected
- 802.11 (WiFi) services have huge risk, and must be protected
- Bluetooth is not generally used for data transfer… and should not be, due to design issues

I don’t have to list the threats here, do I?

Protecting Mobile Data Services Can Occur at Application or IP Layer

- Application Layer requires each application / URL be individually protected
- Enforces at the firewall
- Opens larger attack surface in the network
- Limits access to "what you can get over Internet"
- Less intrusive to end-user
- More device independent



App. Layer

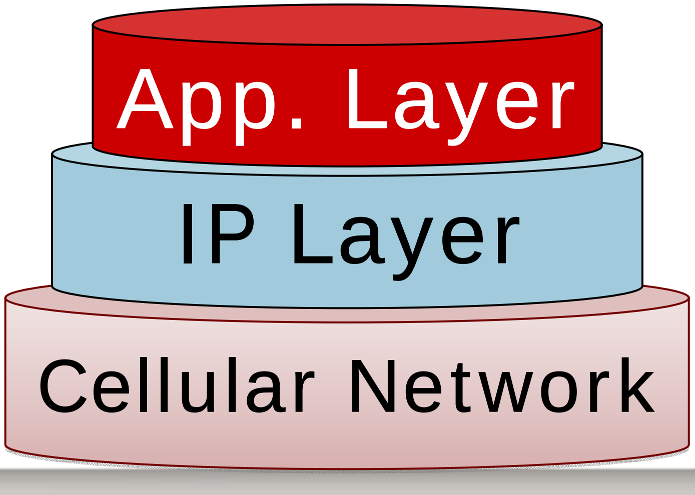
IP Layer

Cellular Network

Policy element: personal webmail to be HTTPS encrypted

IP Layer Protection Offers Greater Access, but Lower Interoperability

- IP Layer requires a compatible VPN client to be installed on each device–a potential support issue
- Enforces at the firewall and VPN concentrator
- Provides smallest attack surface and greatest access
- Can be very intrusive & annoying
- Need that VPN client!

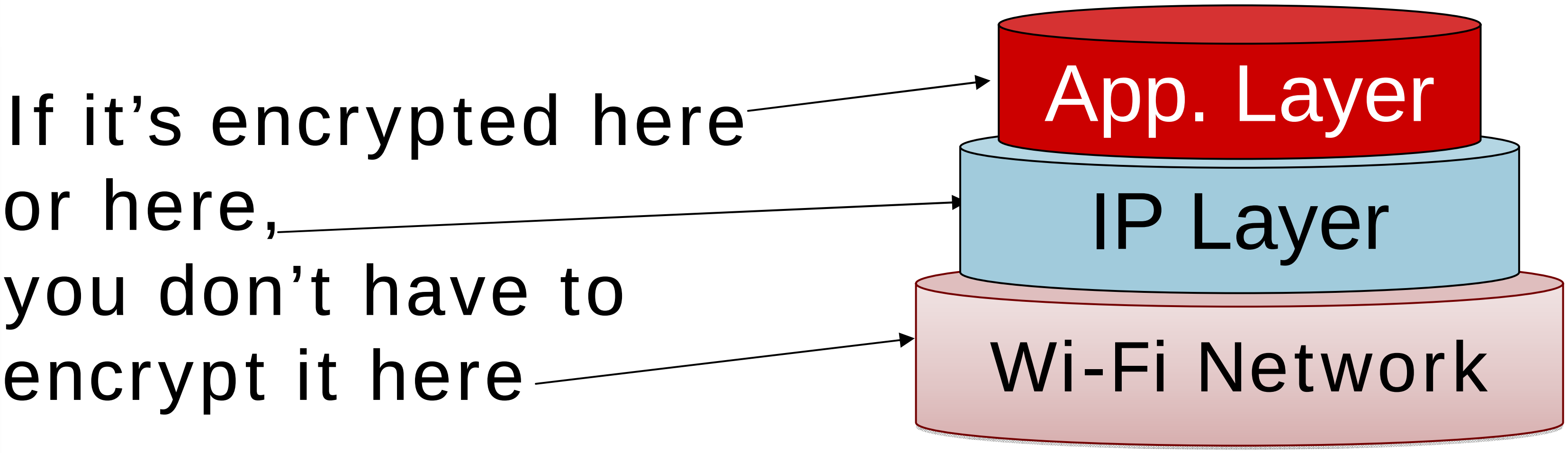


Wi-Fi is Harder To Control

- Existing corporate standards for Wi-Fi apply
- And those standards must be
  - WPA *or*
  - WPA2

- Hot-spots rarely support link encryption (T-Mobile the exception)
- Link encryption good; end-to-end encryption ~~better~~ required

Wi-Fi is Harder To Control… So We Go Back to Either IP Layer or Application Layer Encryption

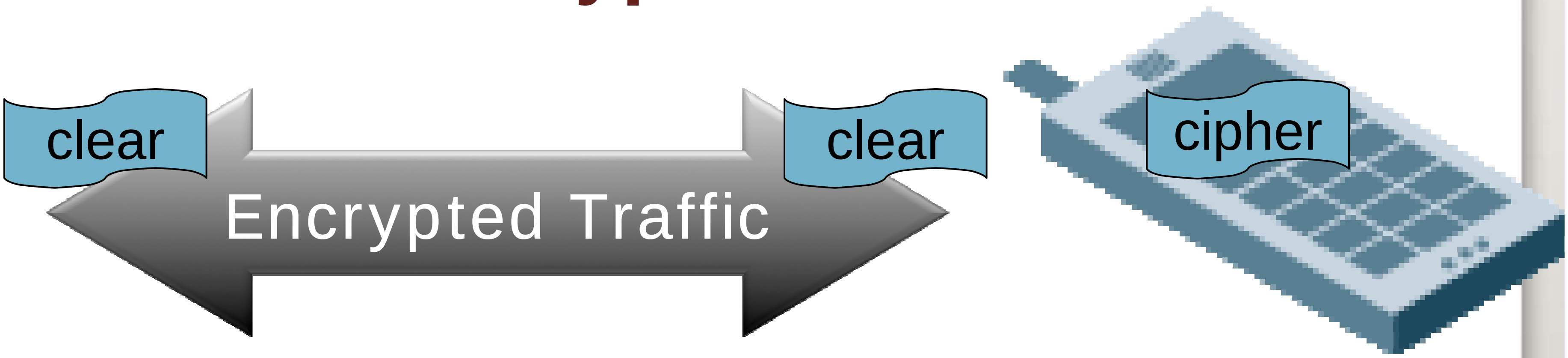


If it's encrypted here
or here,
you don't have to
encrypt it here

THIRD: Nothing Sits Around Unencrypted

- As long as no one ever loses a device, you can safely ignore this one

Start by Making Sure Your Own Data Are Encrypted

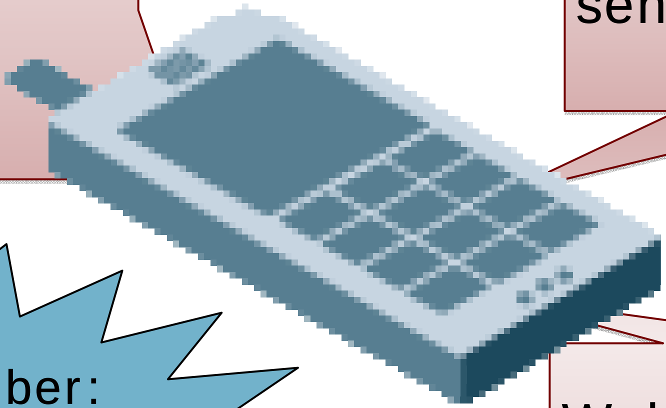


- Could encrypt individual documents
- Could encrypt partitions within the device
- Could just encrypt the whole volume

But what about devices that are just too dumb to encrypt?

Look Beyond The Obvious For Full Protection

Emails are cached;
SMS/MMS are stored
and not tracked.
All are sensitive.

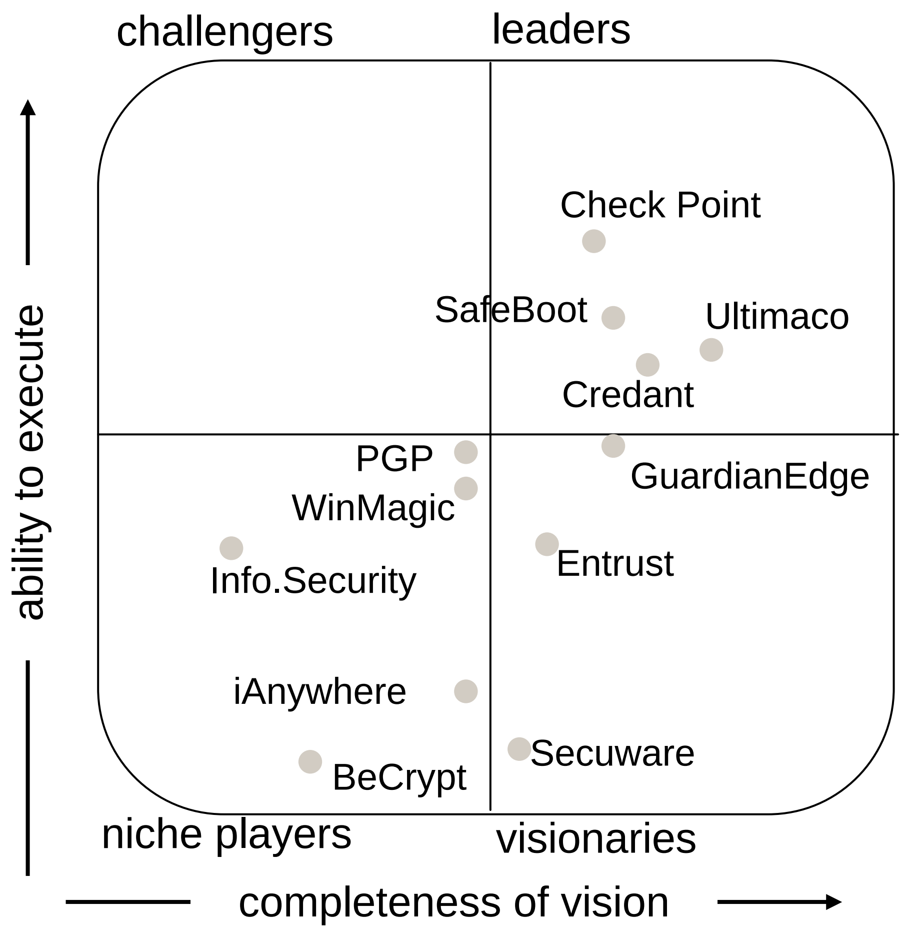


Your corporate phone directory has valuable & sensitive information.

Web browsers cache data of all sorts, whether they are sensitive or not.

Key to remember:
Just because it's not
corporate email,
doesn't mean it's
not corporate email.

Device Vendors Don't Care About This, So Use Third-Party Packages



Vendors who gave Gartner money (July/ 2007)

Mathias' Law Says We Will See Organic Growth Here:

> "It is *inevitable* that security features will roll-up into operating systems over time."

So While Device Vendors Don't Care, They Will Eventually Fix It!
Perhaps Not in Your Lifetime, Though

Mobile Devices are Current, High Priority Targets for Malware

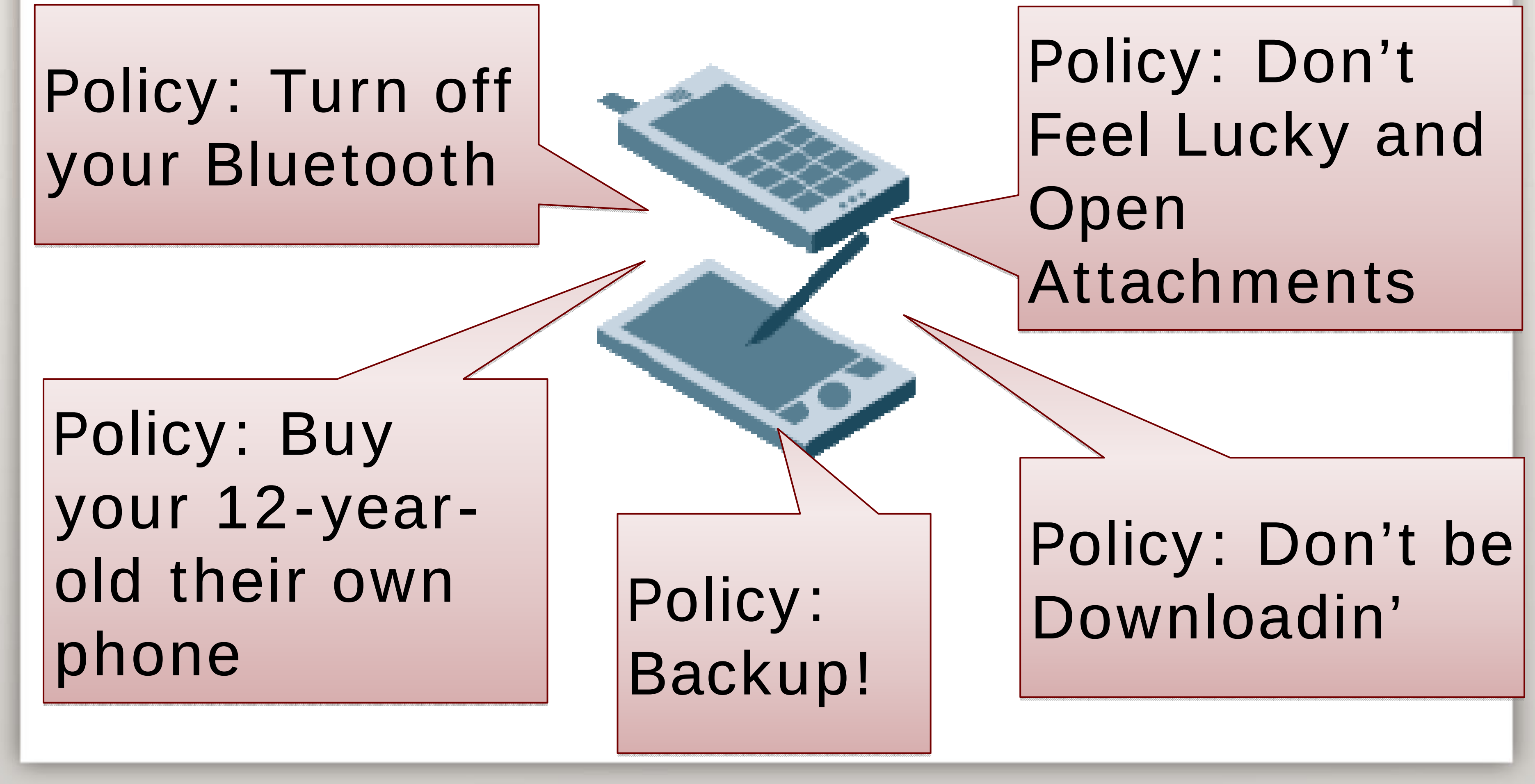
- **Threats to Device**
  - Malware/viruses/etc. spread through Bluetooth
  - … spread through email
  - … spread through ringtones
  - … spread through downloads

- **Threats To Organization**
  - Cost of "900-number" phone calls
    - Or International…
  - Lost productivity when mobile worker's device crashes
  - Stolen data by malware

Obvious Answer: Anti-Malware

Equally Obvious Problem: Each Device has a different operating system!

Malware Protection is an Opportunity for Policy to Help



Policy: Turn off your Bluetooth

Policy: Don’t Feel Lucky and Open Attachments

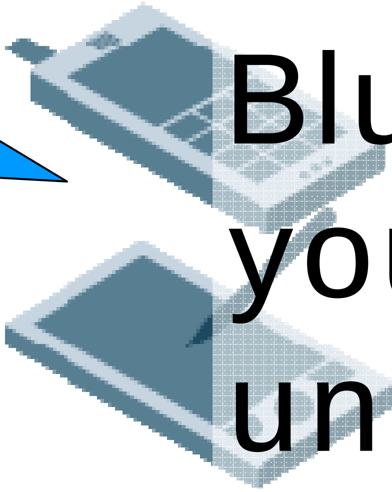
Policy: Buy your 12-year-old their own phone

Policy: Backup!

Policy: Don’t be Downloadin’

If You Only Do One Thing…

Policy: Turn off your Bluetooth



Bluetooth is your biggest unmitigated threat!

Device Management Software Can Enforce Policy and Protect You

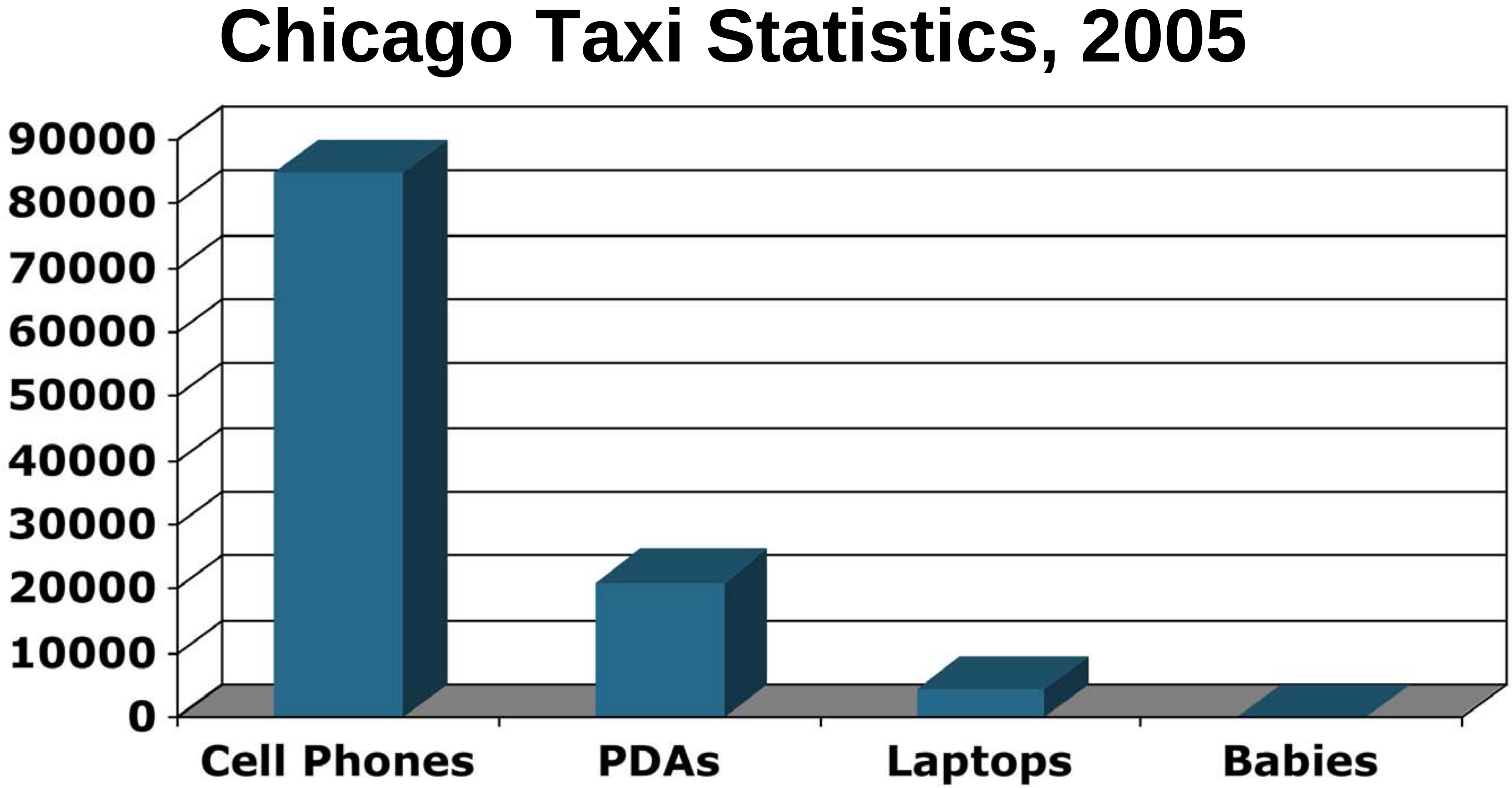
	Features To Look For
★	Device Provisioning
★	Application (Email, Usually) Configuration
★	Download Policy Enforcement; Backups
★	Remote Device Wipe
★	Remote Device Lock and Unlock
★	Password Recovery (Encryption)
★	Over The Air (OTA) Management
★	Open Mobile Alliance Device Management

Some of this can be outsourced, with the right carrier and plan.

Did I Mention That Your Device Management System Must Be Cross-Platform?

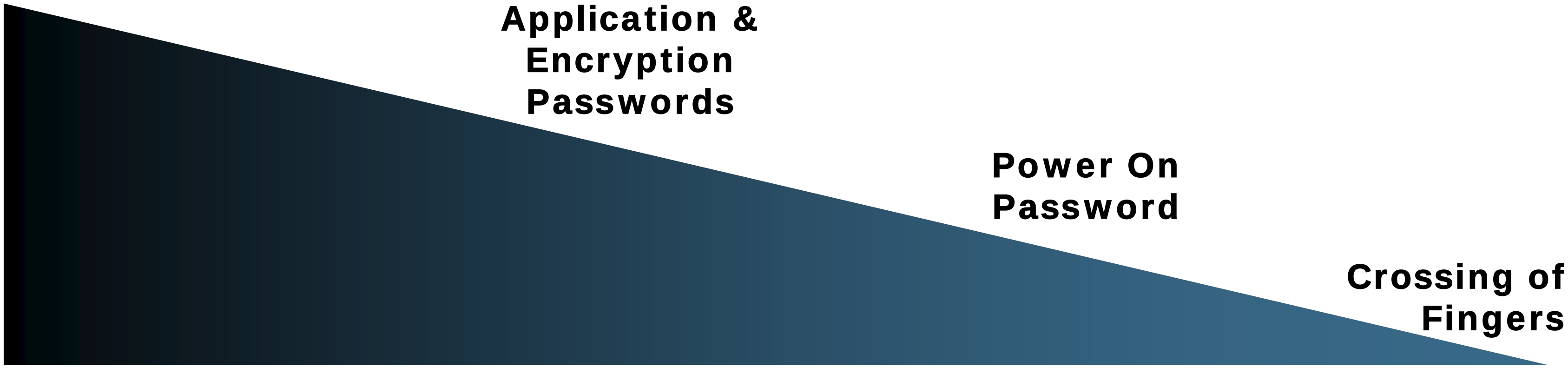
Hint: 5 out of 5 is impossible. Sorry.

Your Last Defense: Authentication



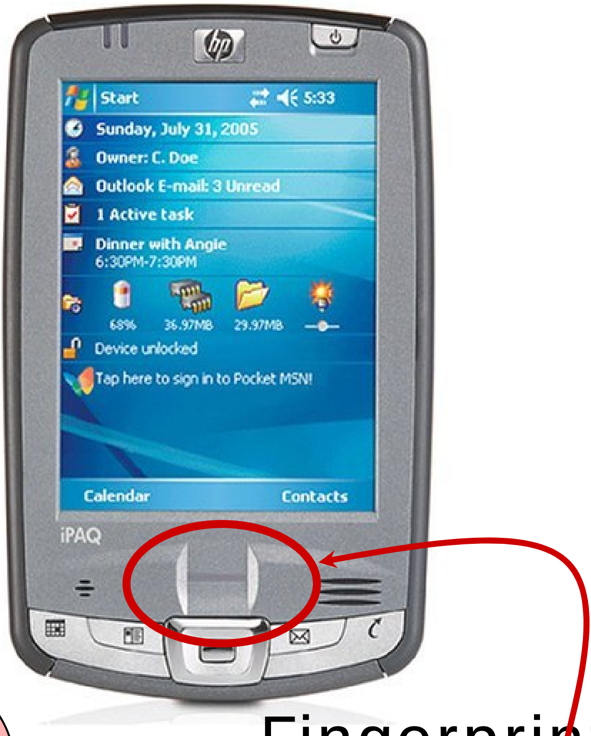
Authentication Can Occur at Multiple Points During Device Use

Authentication is often tied to encryption–the same password ***unlocks*** and ***decrypts*** data



New Technologies May Help… Or Not

Two-Factor Authentication Is Available!



Fingerprint Reader

TCG Trusted Platform Module

Pick Your Authentication Style Based On Two Key Factors

User Compliance

What will the user community put up with?

Do I need the same policy for all users?

Risk of Disclosure

How valuable are the data on this device?

What is my risk if the data are lost or disclosed?

Five Steps To Solving the Mobility Security Puzzle

Policy	Create a policy that covers the device lifecycle, from selection to recovery.
Data In Motion	Encrypt all data over cell and WiFi networks. Use VPN clients or application layer encryption.
Data at Rest	Encrypt data stored on device. Manage cached data with 3rd party software and passwords.
Malware Protection	Protect against malware with policy (Bluetooth, downloads) and technology (anti-malware SW).
Authenti-cation	Require user authentication at points required for acceptable risk/aggravation.

Thanks!

Joel Snyder
jms@opus1.com
Opus One

OPUS one