Movilidad y Seguridad

Impacto en la privacidad y los costos de la empresas

Mateo Martínez, CISSP
Foundstone Professional Services Consultant
McAfee, an Intel Company

PRIVACIDAD MODO: PARANOICO

- PRISM
- XKeyscore: NSA tool
- GMAIL
- FACEBOOK
- MAPS
- XBOX 360 KINECT

…

…

¿Foursquare?

¿Twitter?

¿Facebook?

El costo de PRISM para la “nube” en USA

	2014	2015	2016
Global market	$148.8	$160.0	$207.0
U.S. market	$72.9	$75.2	$93.2
Non-U.S. market	$75.9	$84.8	$113.9
U.S. share of non-U.S. market (Pre-PRISM)	85%	80%	75%
U.S. share of non-U.S. market (Post-PRISM)	80%	70%	55%
U.S. revenue from non-U.S. (Pre-PRISM)	$64.5	$67.8	$85.4
U.S. revenue from non-U.S. market (Post-PRISM)	$60.7	$59.4	$62.6
Annual loss	$3.8	$8.5	$22.8
Total three-year loss	**$35.0**		

Table 2: High estimate of losses from NSA revelations, in $ billions.

Fuente: http://www2.itif.org/2013-cloud-computing-costs.pdf

PRIVACIDAD MODO: SOLUCIONES

¿Tiene un iPhone?

¿Desea que los anunciantes de Apple sepan donde se encuentra?

Se puede deshabilitar accediendo a**: http://oo.apple.com/**

¿Tiene una cuenta de Google?

¿Desea que google recuerde los lugares que ha visitado?

Se puede deshabilitar accediendo a:
https://maps.google.com/locationhistory/b/0/settings

¿Consumerización IT? ¿BYOD?

McAfee
An Intel Company

Algunos números

1200 millones: Población de la India

570 millones: Usuarios de móviles

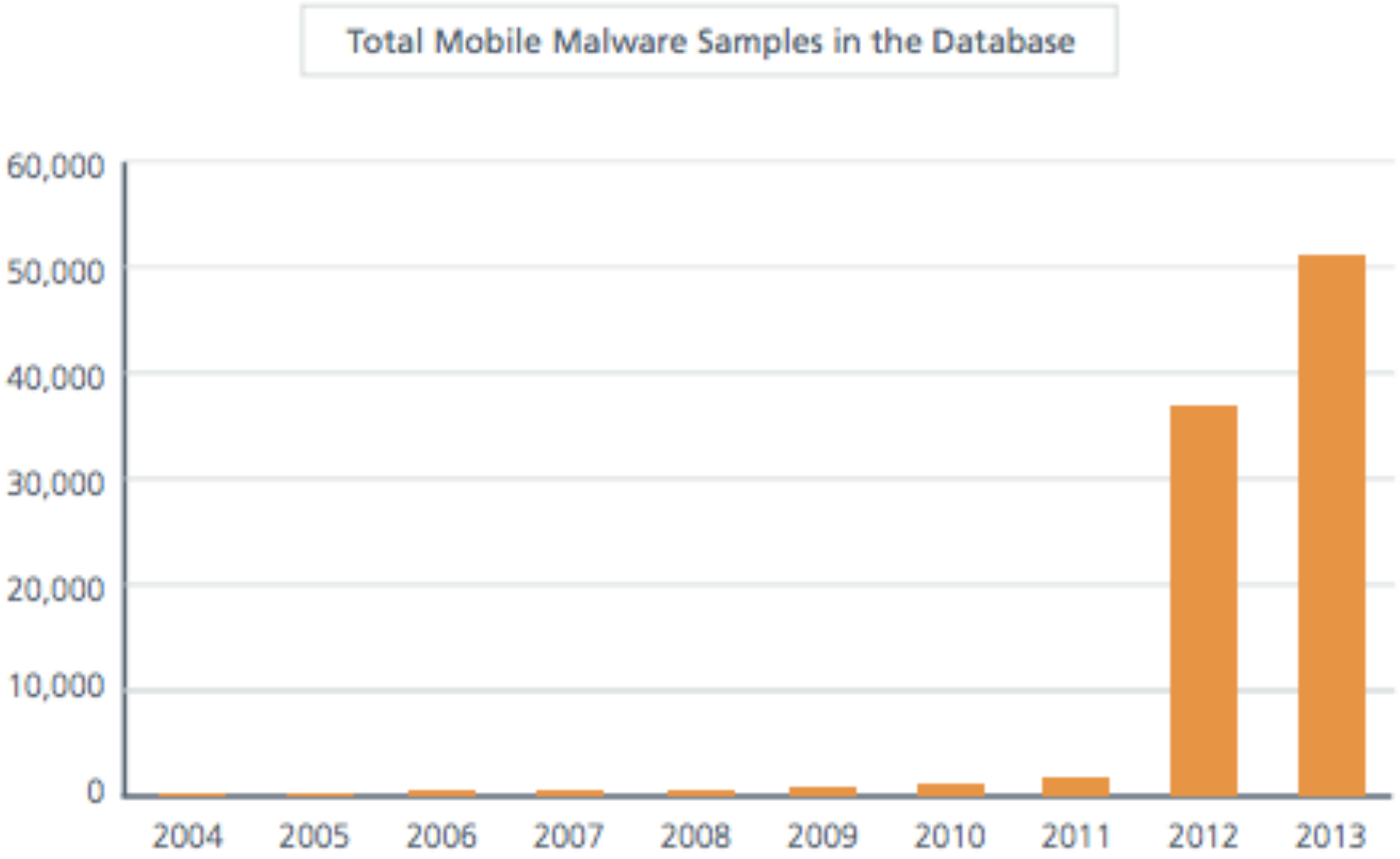
366 millones: Acceso a un baño

1000 millones: Descargas de Angry Birds

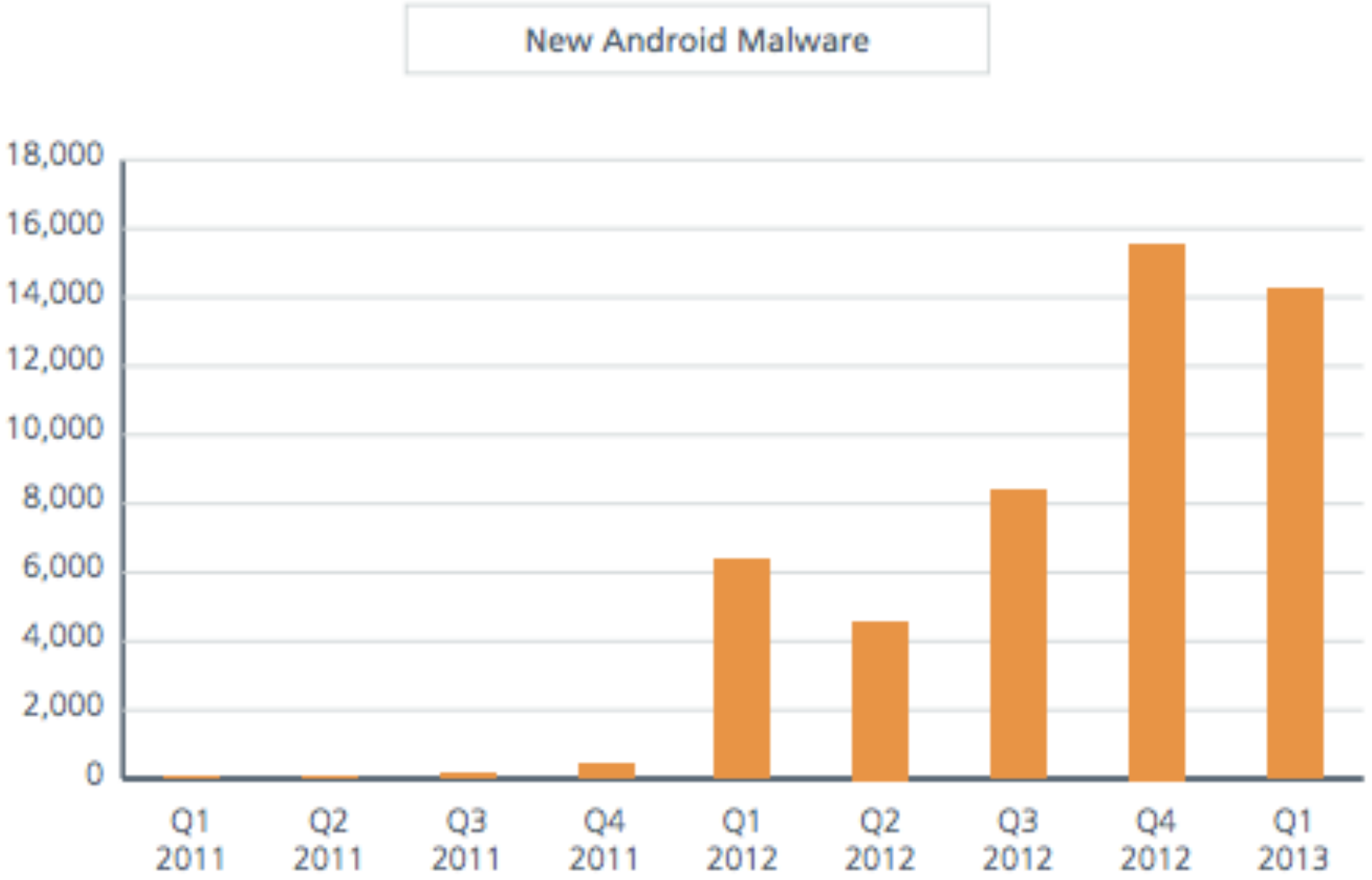
Tráfico de internet móvil > PC

2 Billones de dispositivos conectados,
En el 2020 habrá más de 50 Billones

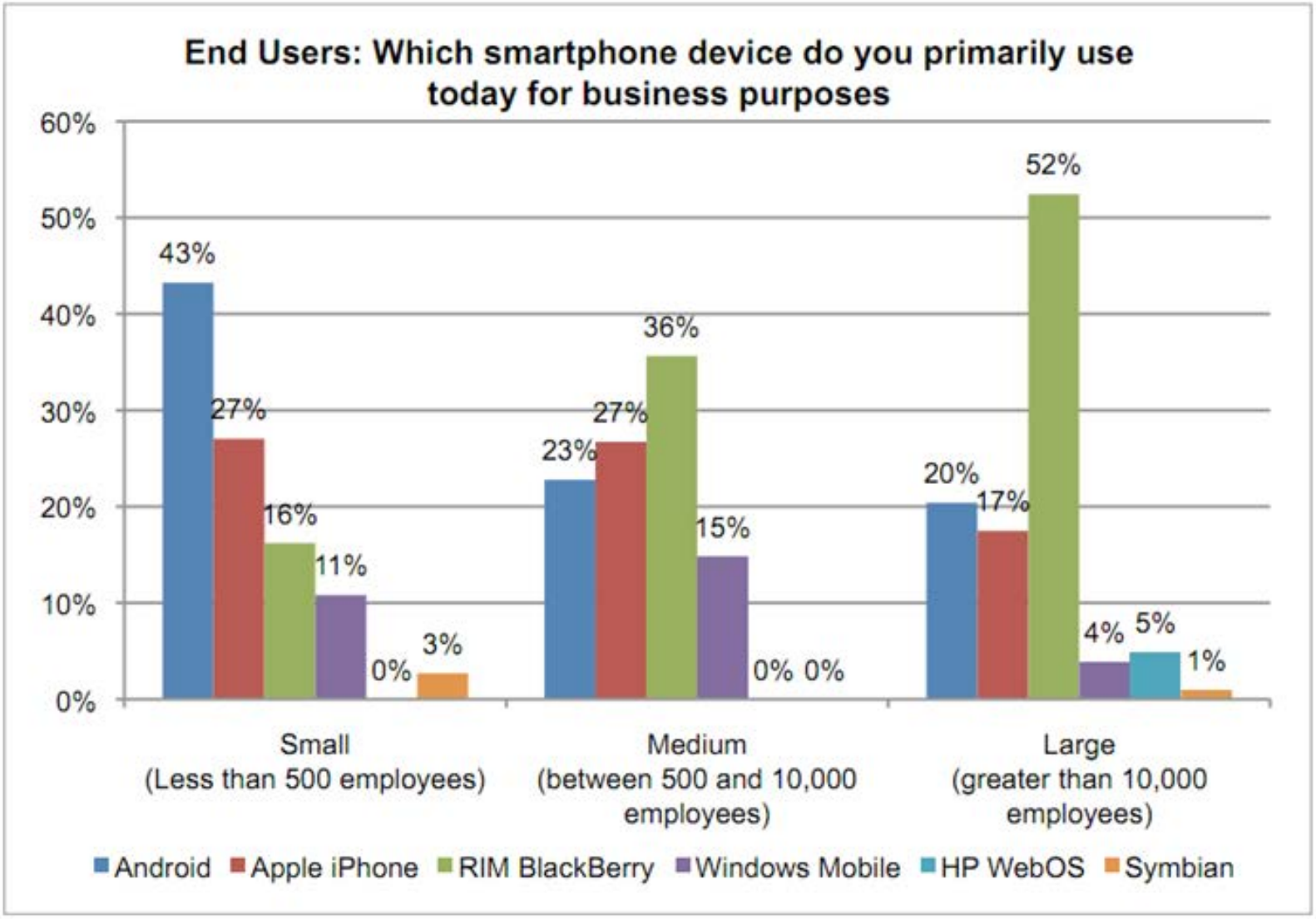
Mobile Malware



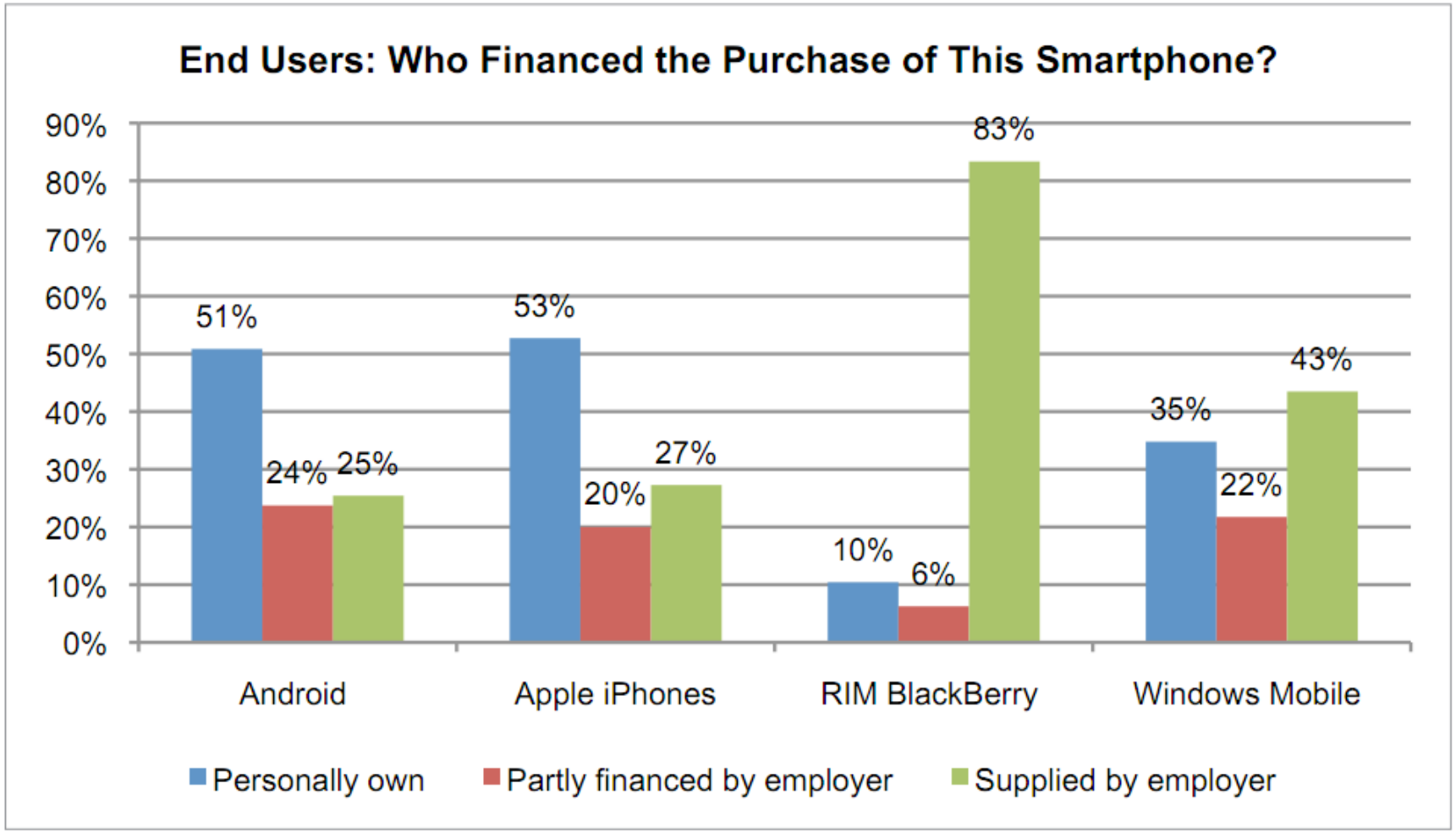
Android Malware



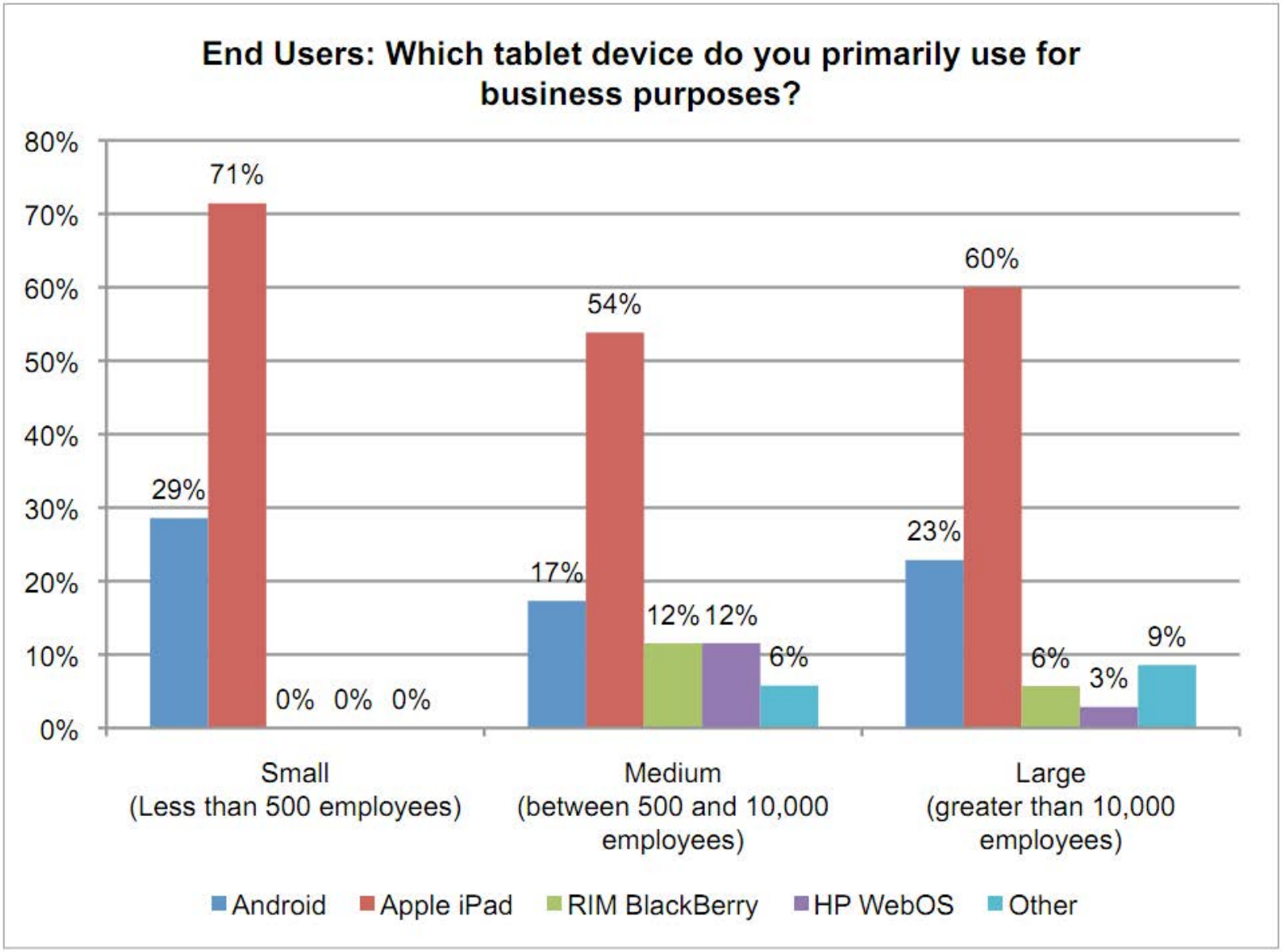
Tendencias #1



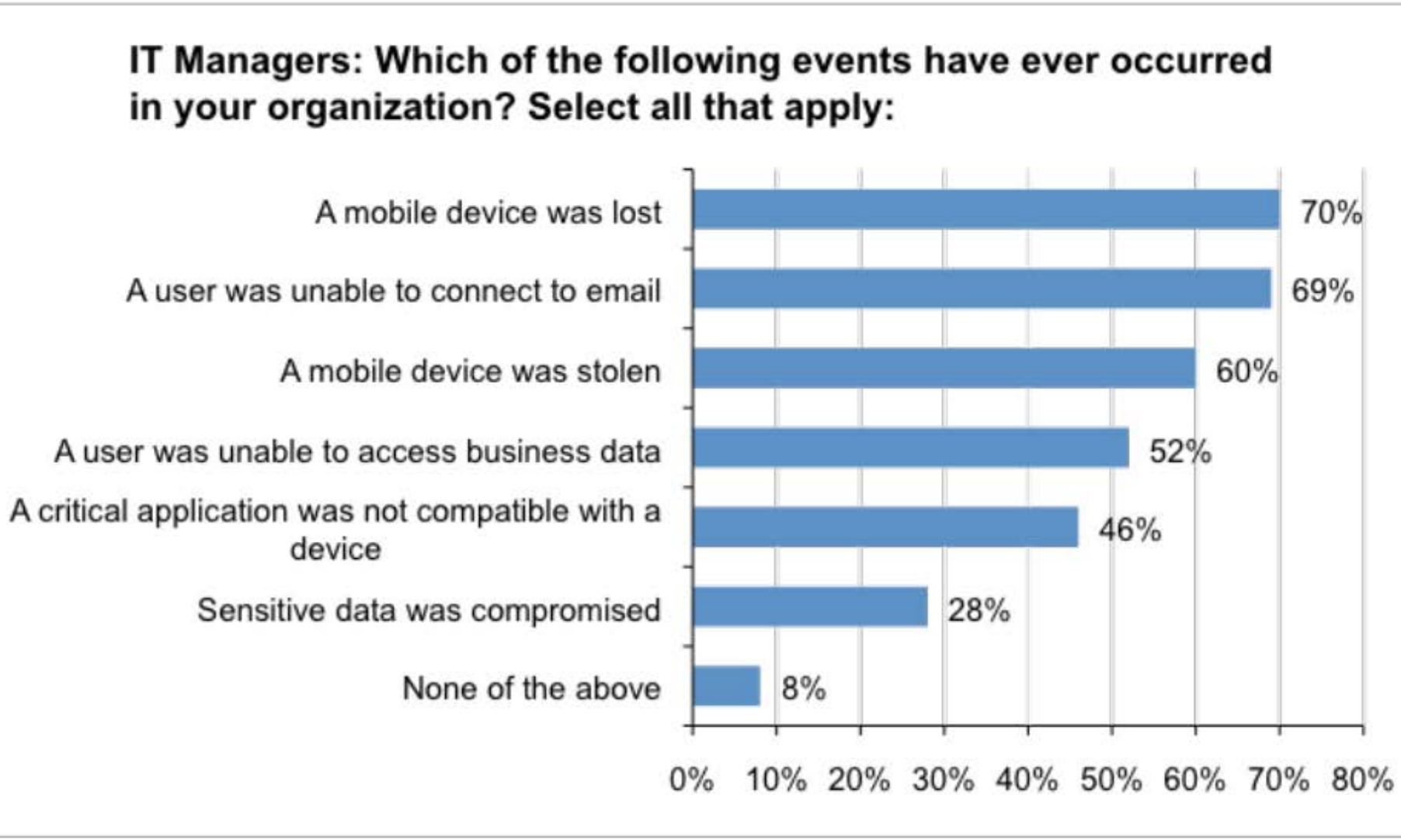
Tendencias #2



Tendencias #3

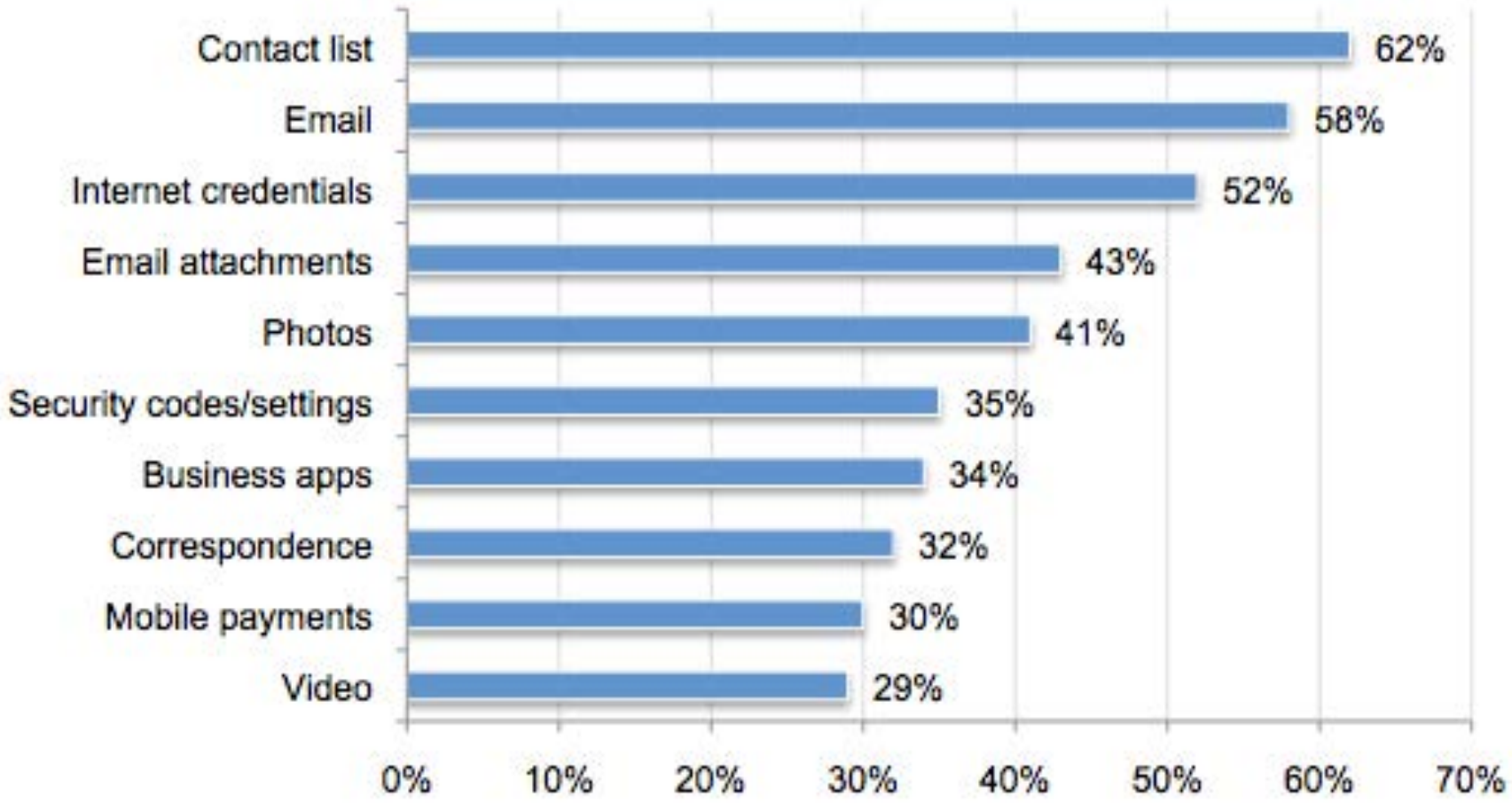


Tendencias #4



Tendencias #5

Bar Chart 8. What business information is at risk because of smartphone loss?



Resumen de Tendencias

- **Consumerization of IT**
  - Dispositivos del usuario en la red corporativa
- **Diversidad de Dispositivos**
  - iOS, Android, Windows, etc.
- **Crecimiento de Apps**
  - Mayor que e-mail y web
- **Amenazas para móviles**
  - Android es el favorito

Seguridad PC vs Móvil

	PC	Móvil	= + similar ≠ divergent
AMENAZAS	• Malware, Virus, Phishing, Stolen Data, Trojans, DoS, Social Engineering	• Similar al PC + • Pérdida de dispositivo, eavesdropping, fraude SMS	= +
VECTORES	• Browser, Bluetooth, Wi-Fi, Cellular Network, Cross Channel, Email	• Similar al PC + • SMS, MMS, App downloads	= +
ENTORNO	• Homogenous OS environment • Largely local computing centric	• Fragmented OS environment • Cloud-centric, tethered to OS provider	≠

Los desafíos en los ambientes móviles motivan a un cambio en el enfoque

Source: McAfee, inCode

Apple iOS Security

Apple iOS is a slimmed down version of Apple's OS X and leverages security pillars

Traditional Access control.

The iOS access control features provide a similar level of security as for traditional Windows-based desktops.

Application Provenance

- Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications have not been tampered with or altered.
- The primary security goal of Apple's provenance approach is to limit malware and Apple has been reasonably effective.

Note that Apple's provenance approach only applies to devices that have not been "jailbroken". Jailbroken devices have their provenance system disabled and may run apps from any source.

Encryption

- Effective HW Encryption from iPhone 3GS onwards.
- Additional Data Protection features
- Allows rapid device wiping
- However decryption key available for background apps without passcode

Application Sandboxing

- A high degree of separation between apps, and between apps and the operating system
- Provides a great deal of protection against network-based attacks.
- However, attacks against specific apps like the Web browser, while being self-contained and blocked from affecting other apps, can still cause significant harm to a device.

Android Security

Based on Linux and takes advantage of native security provided by Linux kernel
Two major drawbacks; application provenance and its permission system

Traditional Access control.

- The Android access control features provide a similar level of security as for traditional Windows-based desktops and the iOS systems.

Application Provenance

- Ensures that only digitally signed applications may be installed on Android devices.
- Attackers can easily inject malicious code into legitimate applications and then easily redistribute them across the Internet, signing them with an anonymous digital certificate. Without any certification by Google.
- Google does require application authors wishing to distribute their apps via the official Android Google Play Store register with Google. As with Apple's registration approach, this should act as a deterrent to less organized attackers.

Encryption

- Available in Android 3.0, enhanced with 4.0
- Software encryption only

Application Sandboxing

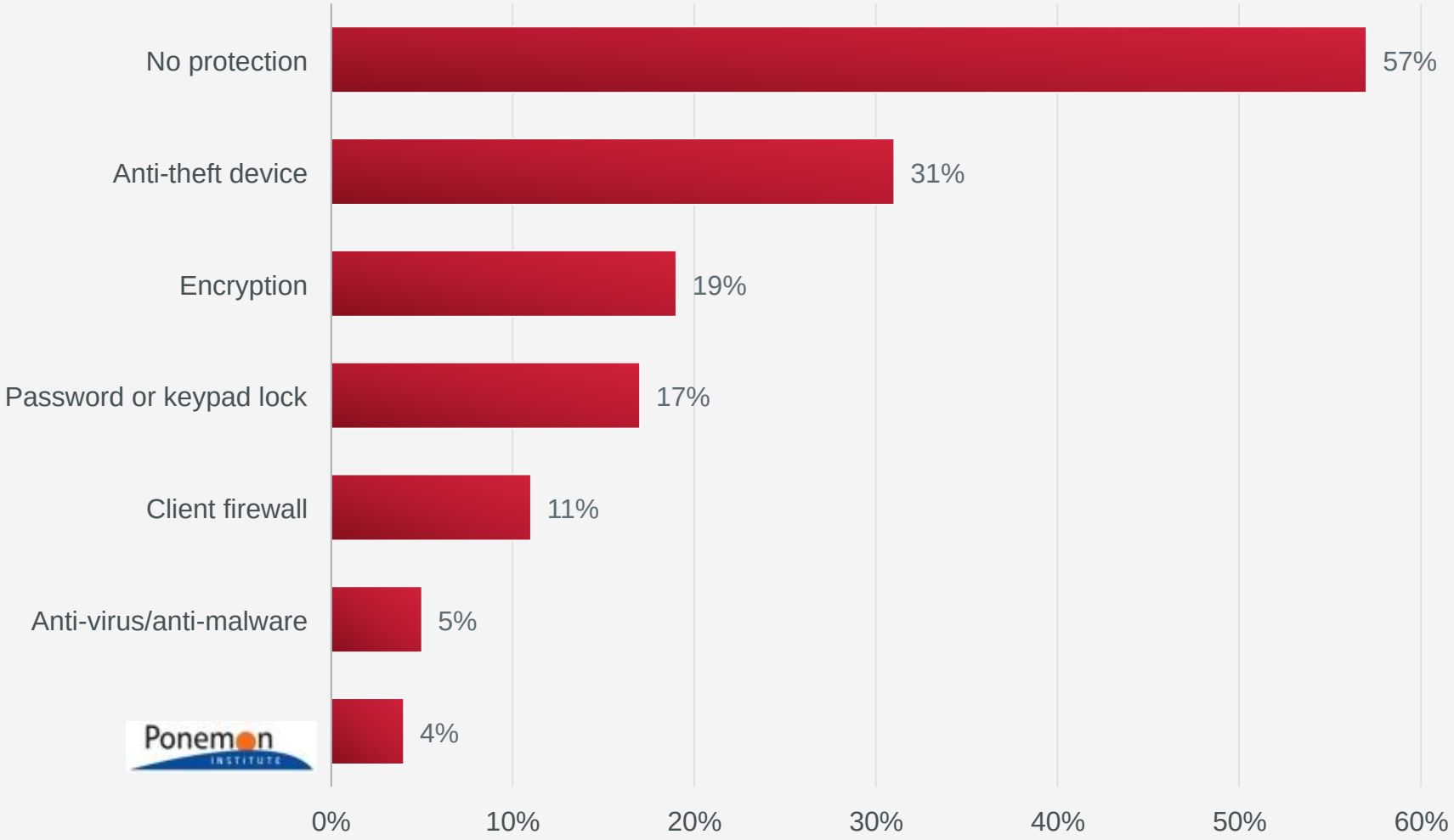
- Android's permission model ensures that apps are isolated from virtually every major device system unless they explicitly request access to those systems.
- Unfortunately, Android relies on the user to decide whether to grant permissions to an app, leaving Android open to social engineering attacks. Most users cannot be relied upon to make such security decisions, leaving them open to malware attacks.

Rooting Android Devices

- Por defecto, el kernel y alguna aplicaciones de core, corren con privilegios de root
- Android no controla si un usuario con privilegios de root modifica el SO, Kernel o aplicaciones.
- Root tiene acceso full a las aplicaciones y a los datos
- El cifrado con la clave en el dispositivo no protege los datos del acceso del usuario root.

http://source.android.com/tech/security/

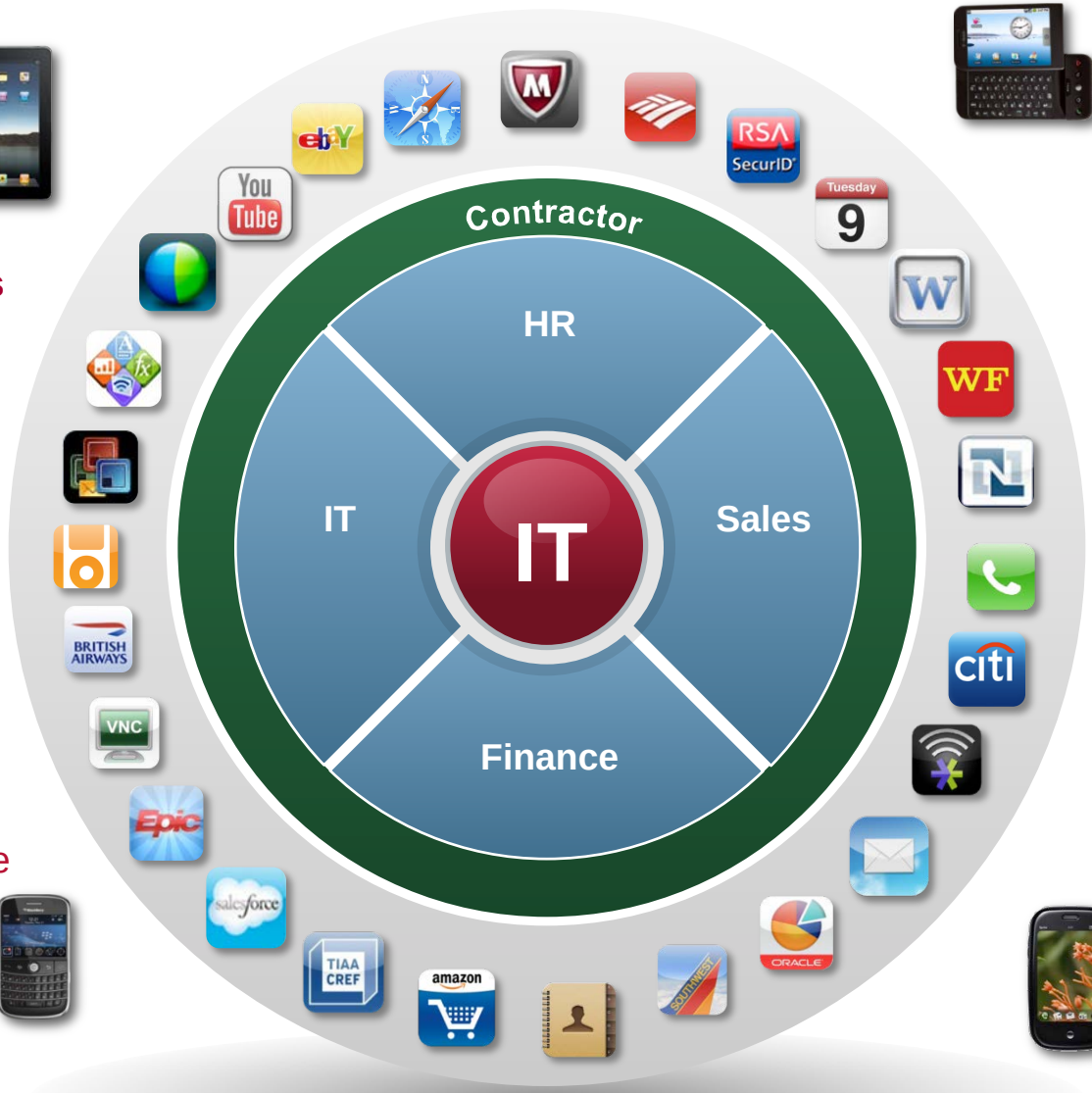
Protección en dispositivos perdidos



La mobilidad nos trae nuevos riesgos

Políticas diferentes entre usuarios IT y móviles

Los dispositivos móviles la nueva frontera del malware



Más de la mitad de los usuario **NO** bloquean los equipos

1 de cada 5 equipos móviles se **pierde** por año

Herramientas de consumo en la organización
Web 2.0, Apps 2.0, Mobility 2.0…Enterprise 2.0

McAfee

60,000 Nuevas piezas de **Malware/día**

Costo de la pérdida de un laptop: $25-50K

Zeus Malware apunta a mobile phones **via SMS**

80% de los usuarios concientes de la pérdida de Información

Entendiendo las menazas en dispositivos móviles

En la mira de los atacantes

Mobile app & content download flood has captured hacker interest in mobile technology

Las plataformas móviles son vulnerables

The fragility of mobile device security is proven, and exploitation of vulnerabilities is accelerating

Ninguna marca o SO es inmune

Malicious activity follows platform viability – consumers and businesses everywhere are targets – Android, iOS, J2ME, BlackBerry and the mobile web are known vehicles

Activos estratégicos bajo amenaza

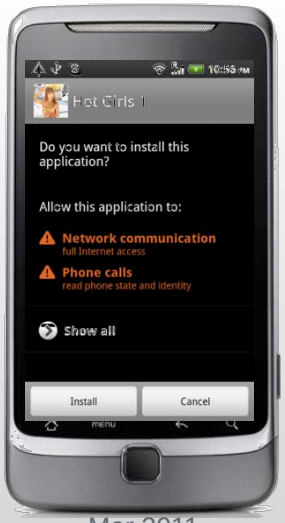
Customer data, location data, billing interface, network, and brand are expected to be the most targeted & affected assets

La protección de la fuentes confiables de Android es deshabilitada muy fácilmente

Algunos ejemplos

DrdDream

- El troyano #1 embebido en apps
- 50+ apps eliminadas del Android Market
- Roba información y espera ordenes del servidor C&C



Mar 2011

GoldDream.A

- Troyano: logs de SMS y llamadas y los sube a un servidor externo
- Se pueden ejecutar comandos desde el servidor
- Herramientas firmadas

Jul 2011

NickiSpy

- Troyano: Graba las conversaciones telefónicas en la tarjeta SD
- Monitora la posición del usuario y envia SMS Premium

Aug 2011

Requerimientos para Seguridad en Móviles

Movilidad y Seguridad

Proteger dispositivos

Dispositivos

- Device Management (MDM)
- Anti-Malware
- Web Protection

Proteger datos

Datos

- Data Protection (Locate, Lock, Wipe, Delete)
- Jailbroken and Rooted Device Exclusion
- Encryption

Proteger Apps

Apps

- Enterprise App Store
- Seguridad en App Stores
- Listas Blancas / Negras de Apps

Alcance de las soluciones necesarias

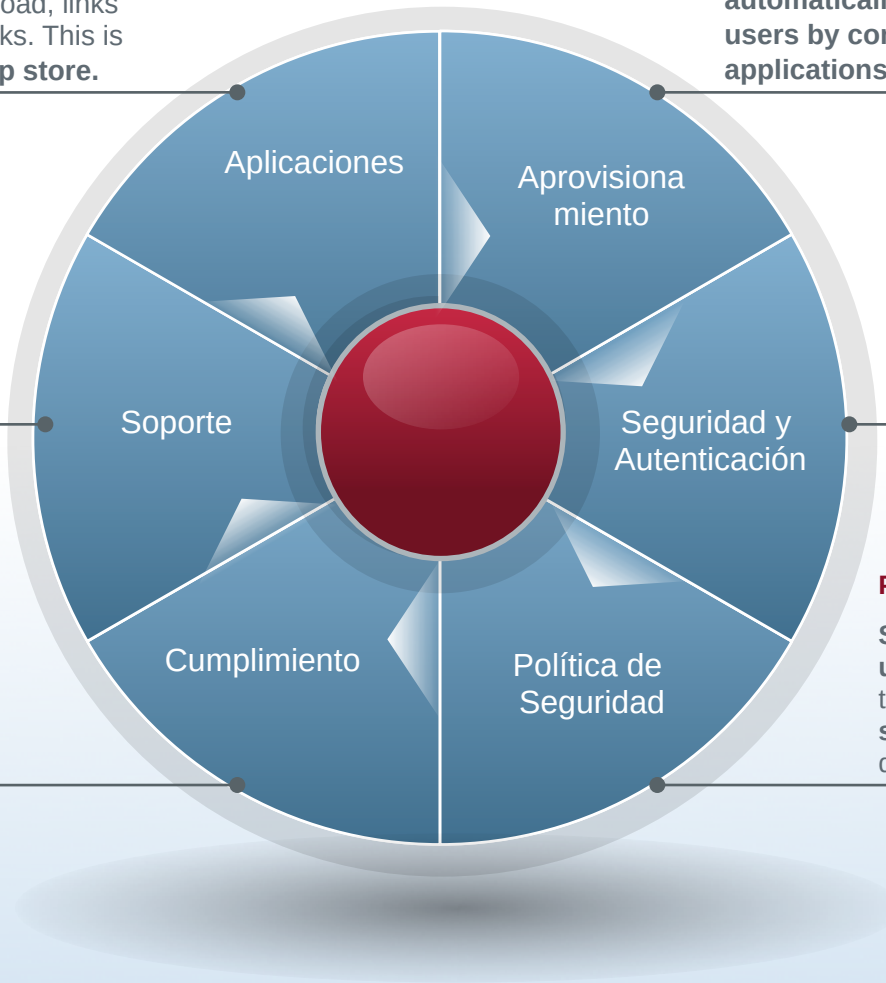
Ciclo de vida

Aplicaciones Corporativas

Make applications available in a **secure, role-based way**. Offer software for download, links to third-party app stores, and web links. This is accomplished via the **Enterprise App store.**

Aprovisionamiento

Self-service provisioning sets security policies, configures network connectivity, **automatically personalizes devices for users by configuring email and other applications**.



Soporte IT

Manage policies and devices and get reports through their web browsers. Consoles access is **role based leveraging, directory authentication and groups.**

Seguridad y Autenticación

Each device is issued a **unique digital certificate** to strongly authenticate it to the enterprise network.

Cumplimiento

Devices are automatically checked prior to network access **to ensure that only authorized, managed, and secured devices access enterprise applications and services.**

Políticas de Seguridad

Security policies and configuration updates are pushed in real-time to the device over-the-air, including **selective and remote wipe**, if the device is lost or stolen.

Laptops y Desktops
Conéctelo a la red corporativa

McAfee

Segmentar el acceso de acuerdo a la identificación y el rol

2

3

Chequeo de antivirus y SO antes de conectarse

Segmentar el acceso a la red en el momento de la conexión

1

4

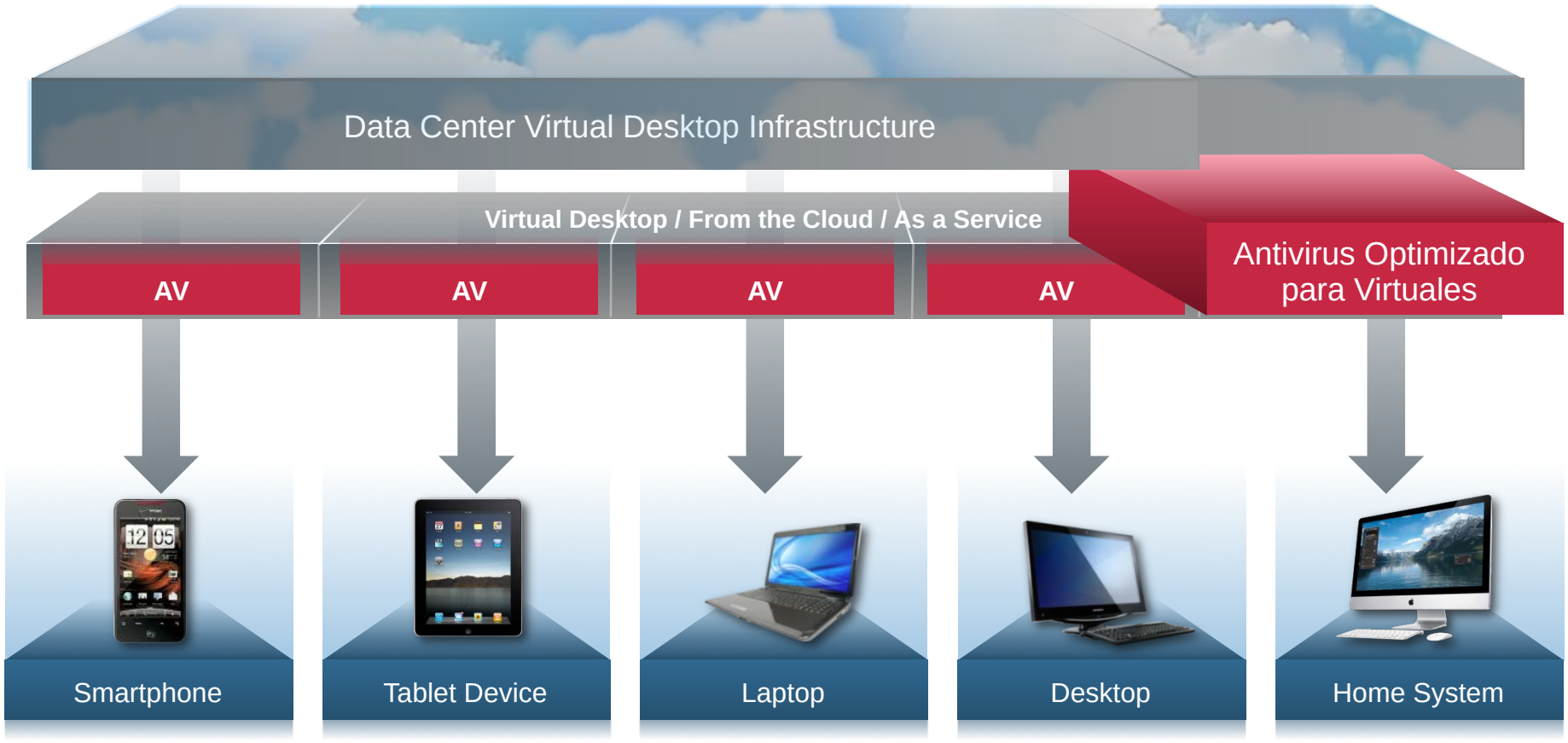
Chequeo full

Chequeo de cumplimiento antes de poder conectarse

Dispositivos NO-Gestionados

Dispositivos Gestionados

Virtualized Desktop



- Evitar tormentas de antivirus
- Escaneo de equipos apagados
- Mejor ROI

Conclusiones

- Gran crecimiento de amenazas para móviles
- Oportunidades en la nube
- Ser Paranoico vs Ser Cuidadoso
- BYOD: Es una realidad que hay que afrontar
- Definir políticas, procesos y procedimientos
- Los costos por no aplicar controles son altos
- Hay soluciones en el mercado (ver McAfee ☺)

Mateo Martínez, CISSP
Foundstone Professional Services
McAfee, an Intel Company

mateo_martinez@mcafee.com

http://mcaf.ee/0bshf (cero, b, s, h, f)