cutting through complexity

BYOD – Secure Zoning Between Enterprise and Personal Data on Mobile Devices

14 November 2013

Rozana Rusli

Meling Mudin

Contents

1.0

BYOD - *Trend or Necessity?*

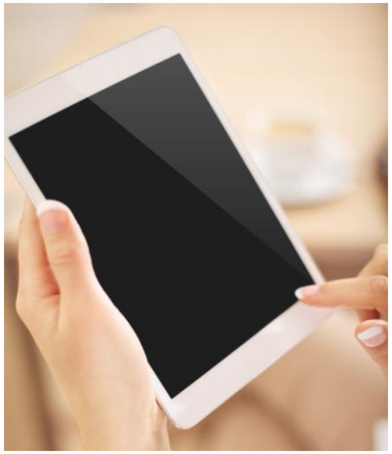
Meeting the Demands of Changing Business Models

- A mobile workforce who access data using the internet reduces costs, improve collaboration and raise productivity.
- Meeting the need for “any user, any content, any location, any time” has led to information being shared between individuals as well as organizations and the interlinking of systems to improve accessibility.

The mobile workforce…

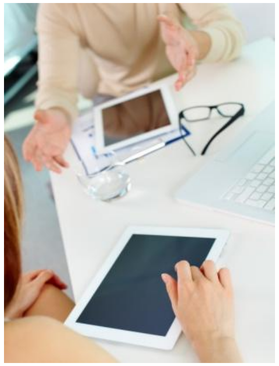
•In 2011 Mobile Workers carried on average 2.7 devices. In 2012 that jumped to 3.5 devices. For the Q1 2013 report that dropped to 3 devices (2.95).*

•In 2012, 74% of tablets were personally owned (yet used for work and personal purposes) and in 2013 that number increased to 79%.*



*Source: iPass (2013) - http://www.ipass.com/blog/mobile-worker-byod-costs-impact-productivity/

… meets the consumerization of IT



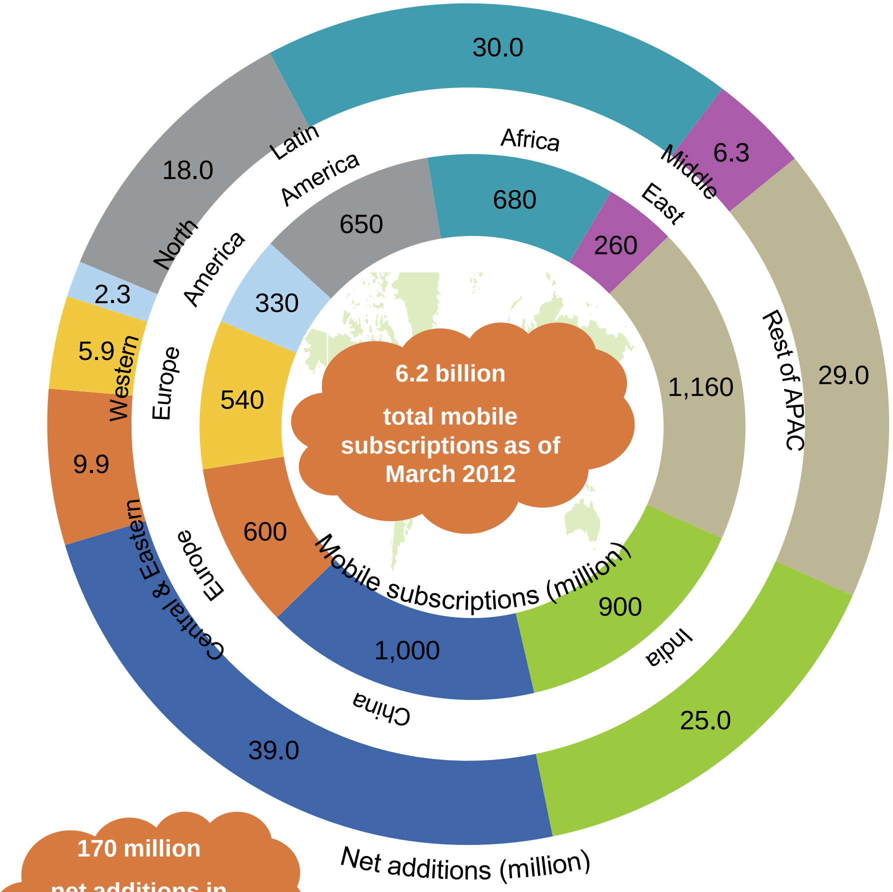
Consumers use their own devices for business purposes – a trend widely known as ‘consumerization’ or ‘bring your own device’ (BYOD).

BYOD trend creates a number of risks, but it also offers an opportunity to enhance security.

A poll of 10,000 employees revealed that employees wanted to keep company data on personal devices and did not want the company to control them. – *The e-Crime Report 2011*

Global telecom sector: An overview

Global wireless subscriber base and net additions (Q1 2012)



6.2 billion

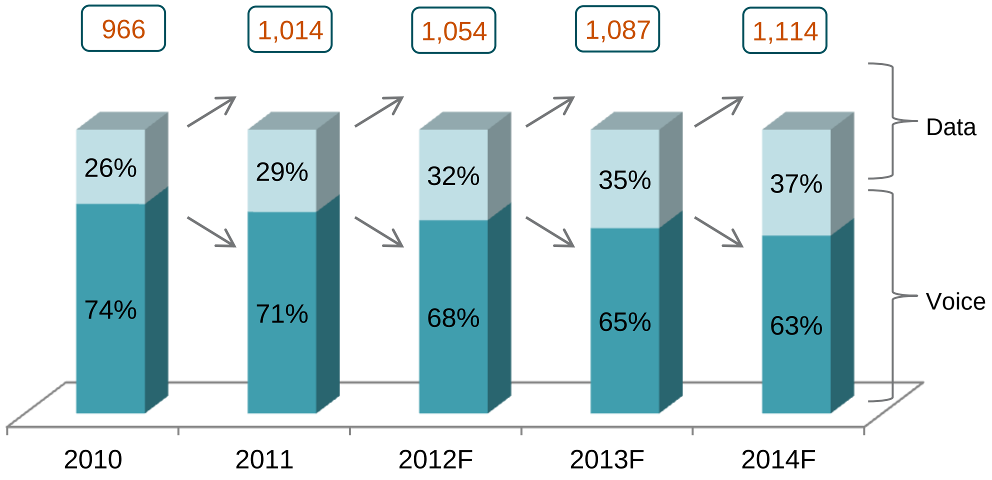
total mobile subscriptions as of March 2012

170 million

net additions in the first quarter ending March 2012

hSource: Ericsson; Informa Research

Global Mobile Services Revenues
(US$ billion)



- ❑ **Growing subscriber base:** Mobile subscriptions at 6.2 billion in Q1 2012, (**~87 percent** penetration). Adjusted active subscriptions 4.2 billion
- ❑ **Sharp decline in revenue growth for voice**– down from double-digit increases between 2005 and 2008 to just **5 percent in 2011**
  - ■ **Mobile service revenue** to grow at **CAGR 3.2 percent** during 2011-14
  - ■ **Data to drive revenue growth – CAGR 12.3 percent** during 2011-14, only partly offsetting the decline of voice revenues

What's the buzz?

History

- Blackberry served the corporate world
- As of 2007 major growth market share of smartphones (iPhone, Android)

Recent years

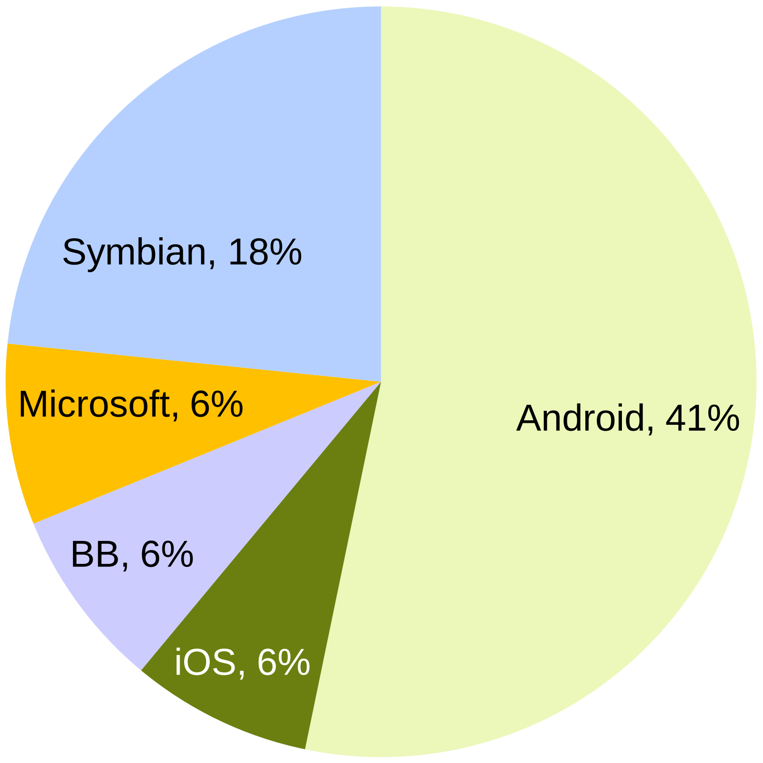
- Explosion of smartphone penetration
- Emergence of tablets
- Corporate and private phones get mixed:

"Bring your own device"

Main Drivers

- Intuitive/Usable interface
- Internet/cloud integration
- Affordable pricing

Malaysia Mobile Subscriber Market Share



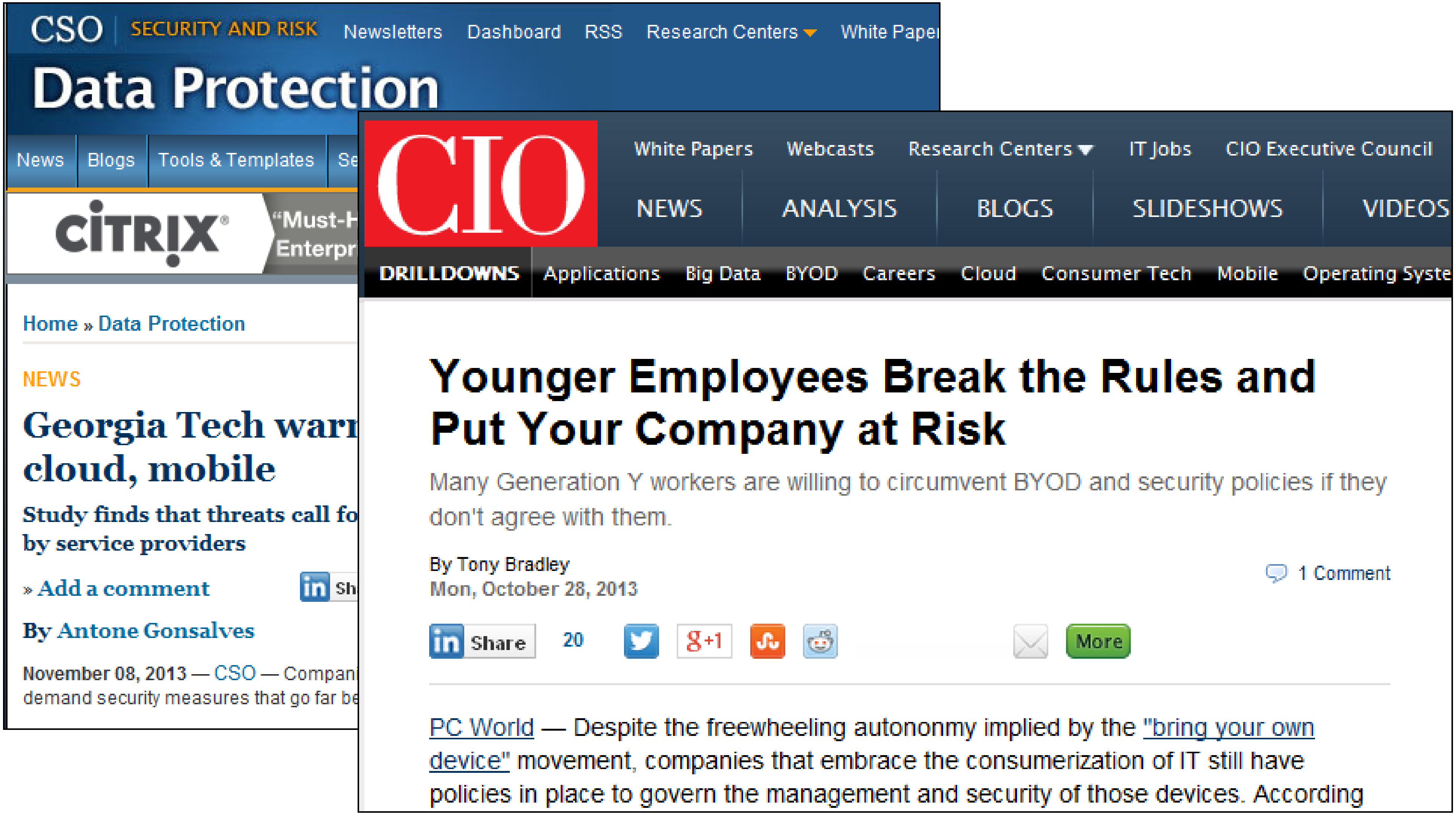
*Source: Lukman, E. (2013, September 3). Android Triumphs Against iOS in Southeast Asia Market. Retrieved November 11, 2013, from TECHINASIA: http://www.techinasia.com/os-report/

A Quick Survey – *Who has some form of BYOD in their organization?*

2.0

BYOD - *Opening Pandora's Box*

BYOD – *In the News*



Georgia Tech warn cloud, mobile

Study finds that threats call fo by service providers

By Antone Gonsalves

November 08, 2013 — CSO — Compan demand security measures that go far be

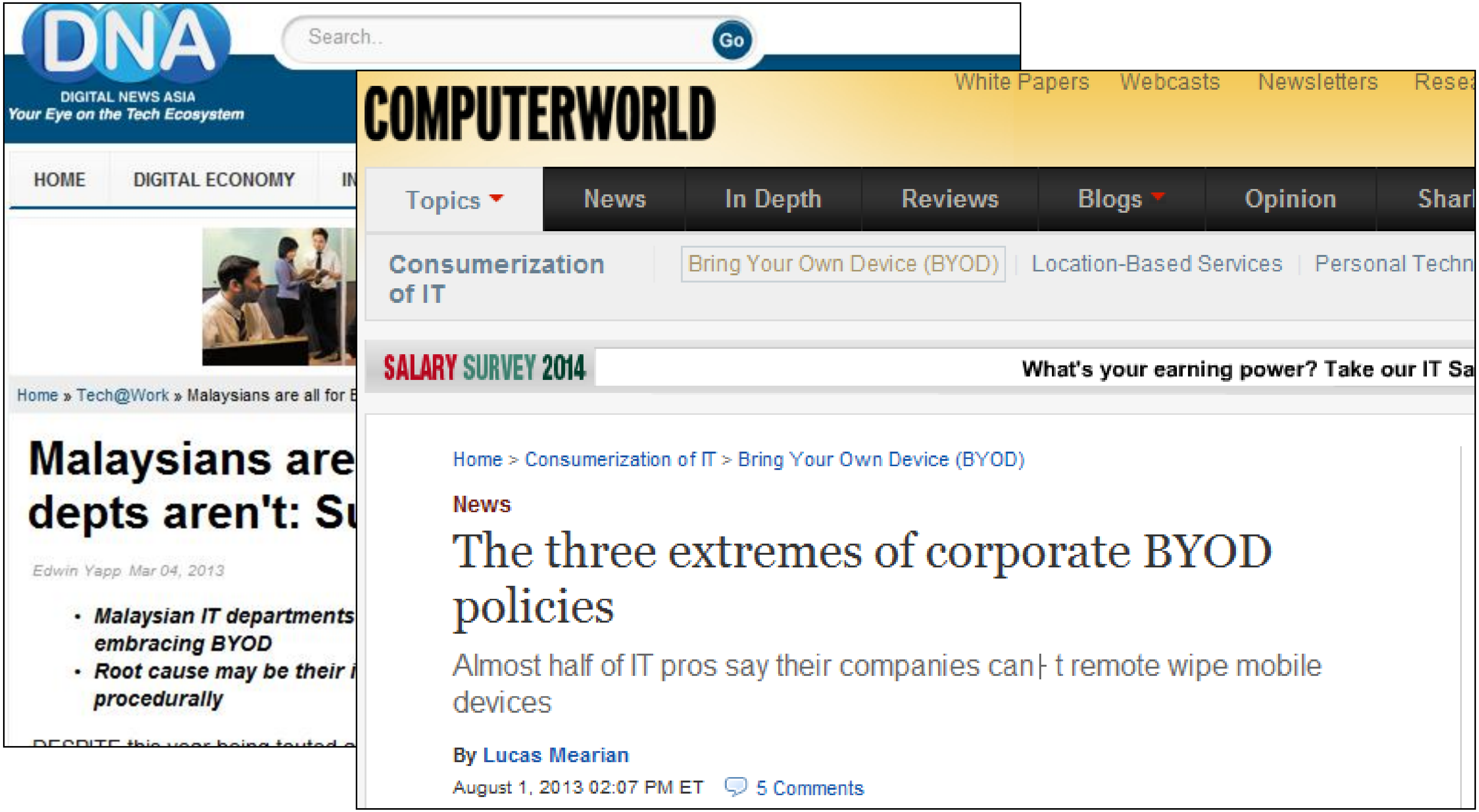
Younger Employees Break the Rules and Put Your Company at Risk

Many Generation Y workers are willing to circumvent BYOD and security policies if they don't agree with them.

By Tony Bradley
Mon, October 28, 2013

PC World — Despite the freewheeling autononmy implied by the "bring your own device" movement, companies that embrace the consumerization of IT still have policies in place to govern the management and security of those devices. According

BYOD – *In the News*



Home » Tech@Work » Malaysians are all for B

Malaysians are
depts aren't: Su

Edwin Yapp Mar 04, 2013

- *Malaysian IT departments*
  embracing BYOD
- *Root cause may be their i*
  procedurally

DESPITE this year being touted a

Home > Consumerization of IT > Bring Your Own Device (BYOD)

News

The three extremes of corporate BYOD policies

Almost half of IT pros say their companies can├ t remote wipe mobile devices

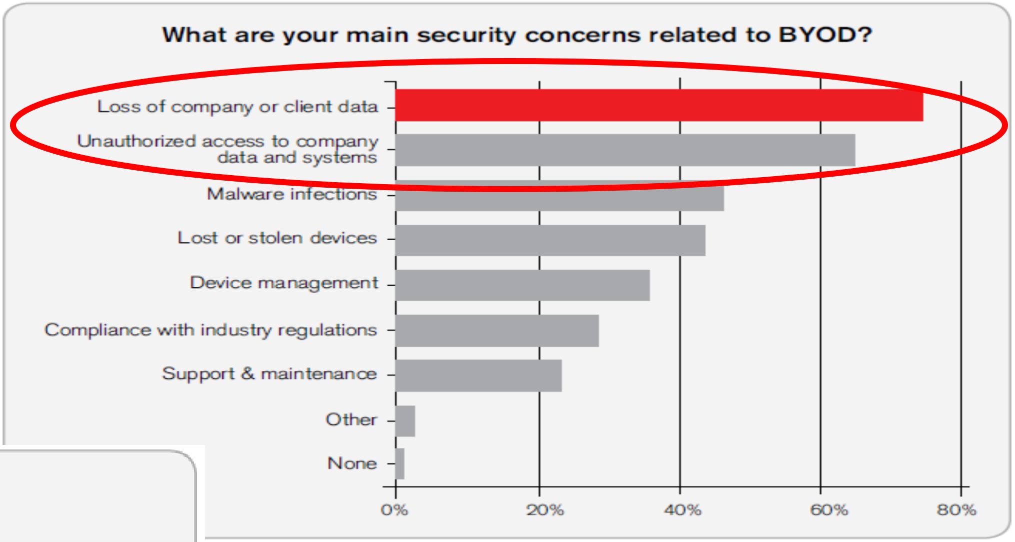
By Lucas Mearian

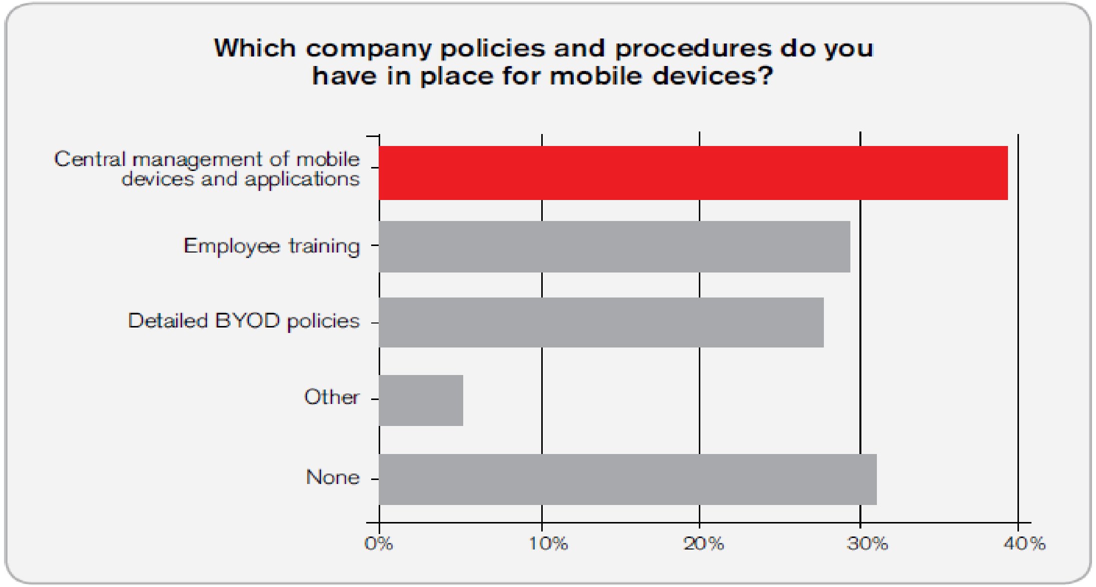
August 1, 2013 02:07 PM ET 5 Comments

What is everybody saying about BYOD?

BYOD causes significant security concerns:

Loss of company or client data (75 percent), unauthorized access to company data & systems (65 percent) and fear of malware infections (47 percent) top the list.


What are your main security concerns related to BYOD?


Which company policies and procedures do you have in place for mobile devices?

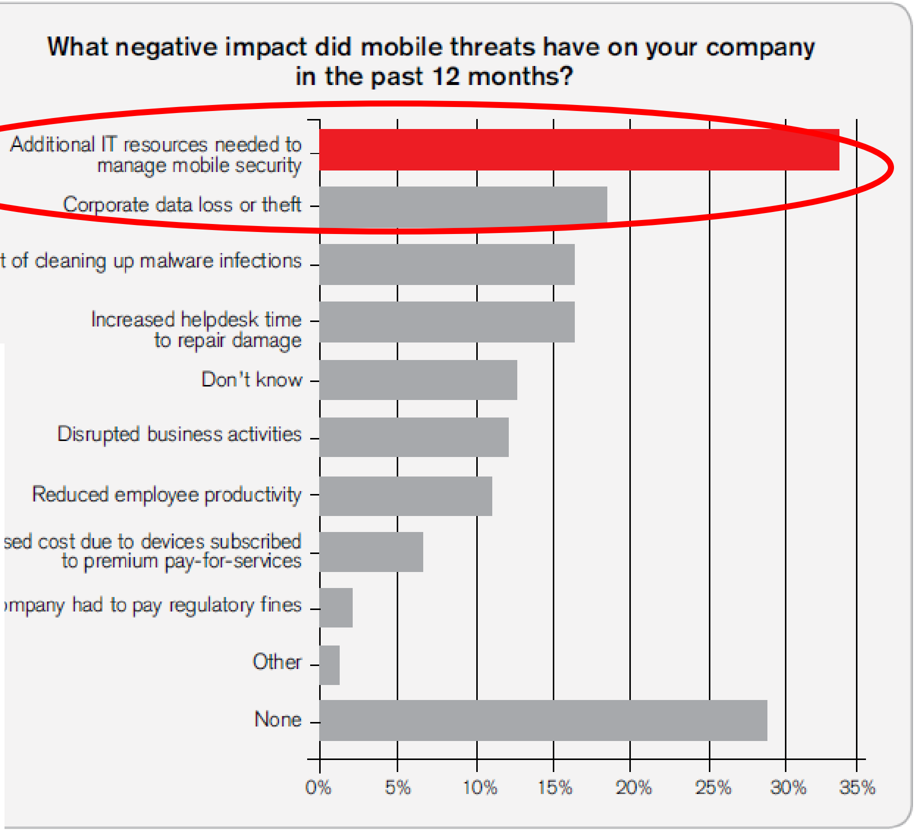
Central management of mobile devices and applications: (39 percent) tops the list of BYOD policies and procedures

32 percent of organizations say they do not have any policies or procedures in place.

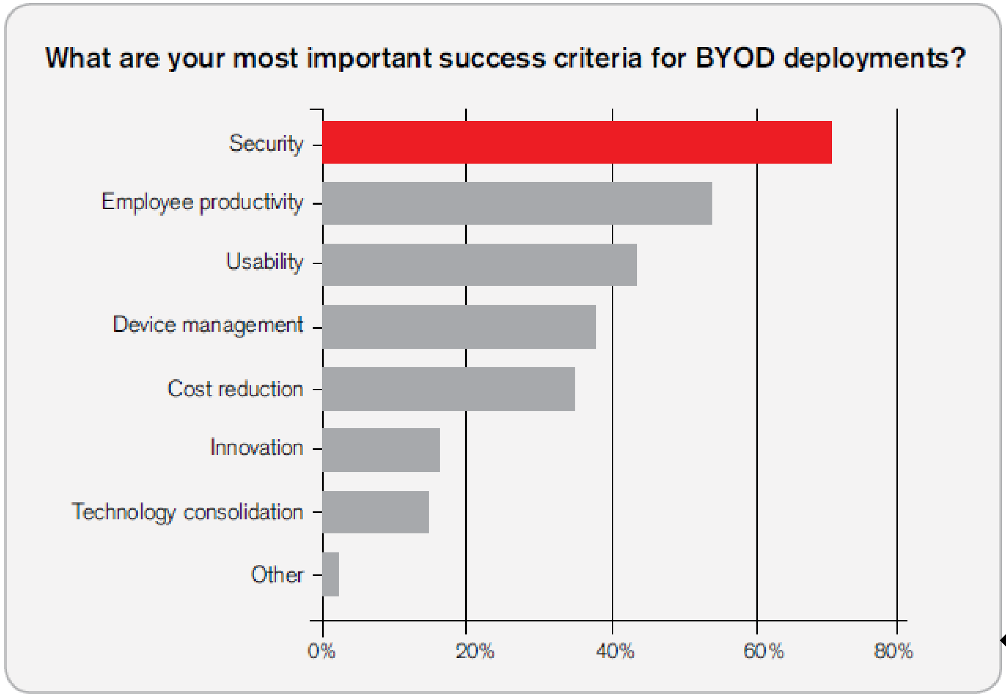
Source: 2013 Survey Results – BYOD & Mobile Security

What is everybody saying about BYOD?

The biggest impact of mobile security threats is the need for **additional IT resources** to manage them (33 percent). And 28 percent of respondents report no negative impact from mobile threats in the past 12 months.



What negative impact did mobile threats have on your company in the past 12 months?

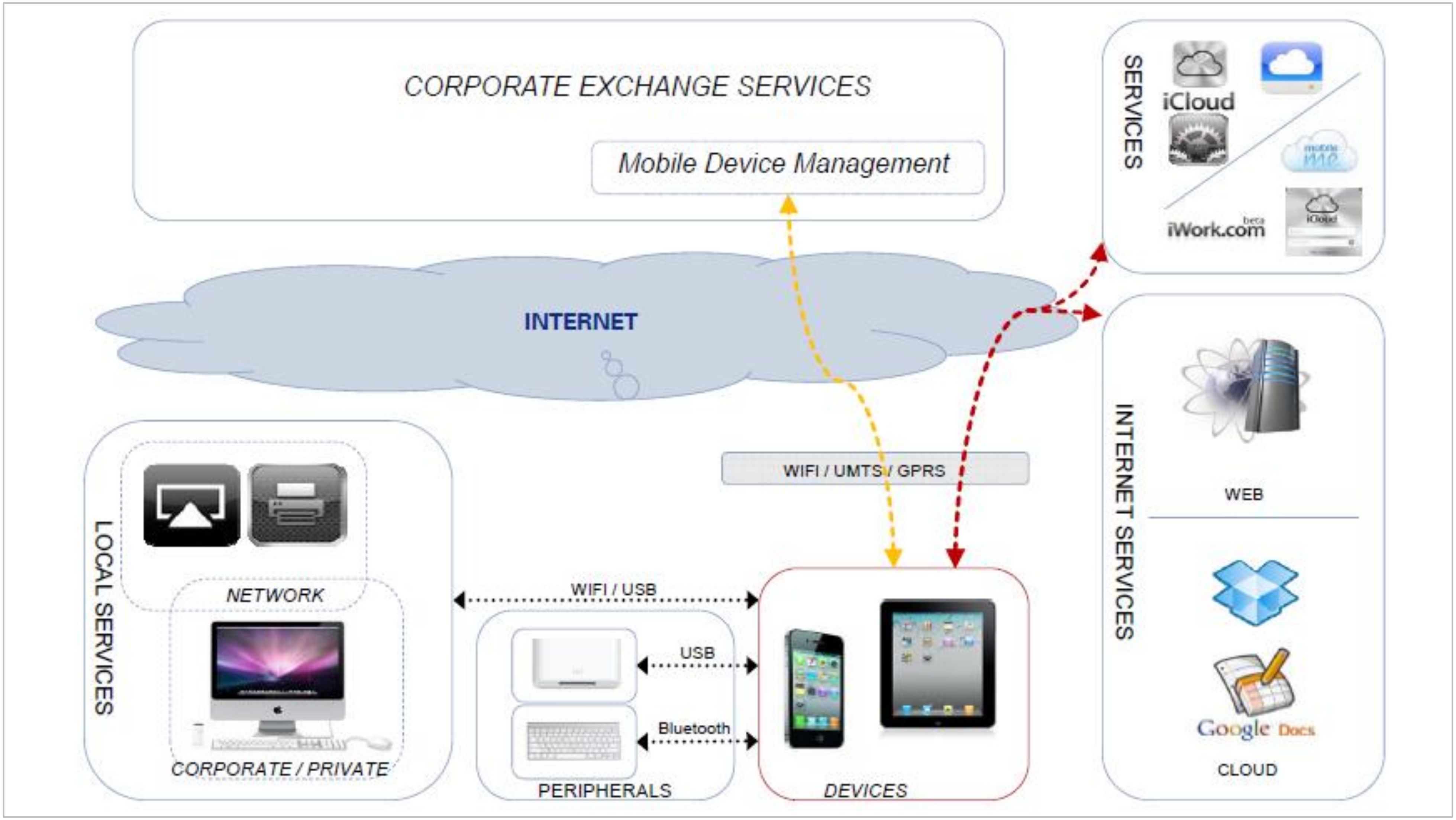


What are your most important success criteria for BYOD deployments?

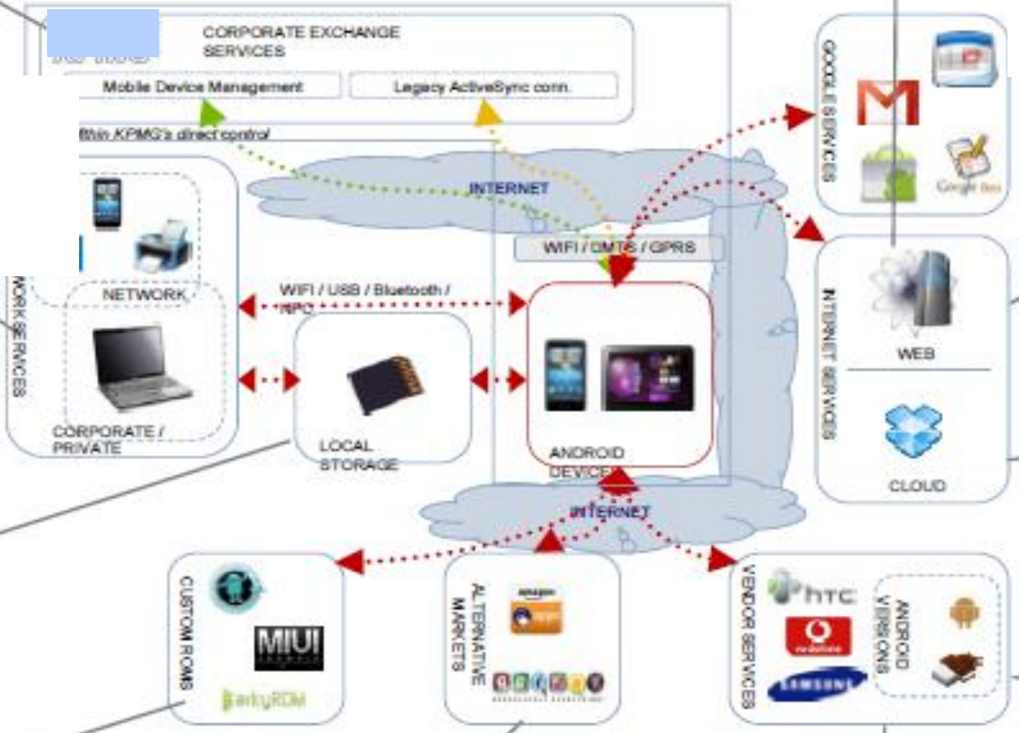
The most important success criterion of BYOD deployments is **maintaining security** for 70 percent of organizations. Employee productivity ranks second with 54 percent.

Source: 2013 Survey Results – BYOD & Mobile Security

User Bad Habit: I don’t know where my data is



Threat Analysis



Unauthorised devices connect with ActiveSync

Cloud Services

Corporate data compromised through corporate network connection

Website with malicious content

Third party provider compromised

Unauthorised access of SD card

Updates

Android custom ROMs

Android alternative market

Android device rooting

A Quick Survey – *Has any one suffered a Security breach as a result of BYOD?*

3.0

BYOD – *The Business Case, Implications and Strategies*

The Business Case

Cost

- If structured correctly, a BYOD strategy can **pay for itself**.
- A large Australian/International Corporate had demonstrated they could change their cost base for mobility by -40% to +300% by considering a BYOD strategy.

Staff productivity & engagement

- Employees want simple solutions that offer **more choice** and **flexibility** and improve their productivity. Employees don't want to carry work and personal devices.
- In a recent survey of users who BYOD, 94% of reported **productivity gains** of 6 minutes per day. An astonishing 53% reported productivity gains of greater than 30 minutes per day.

Risk Management

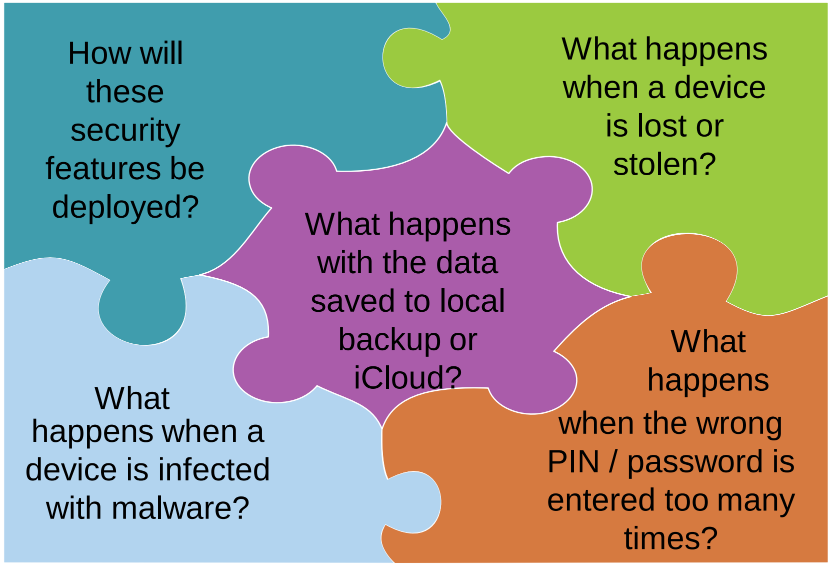
- Many organizations have **"uncontrolled"** BYOD incident.
- Organizations are not likely to have effective systems, policies and procedures to deal with corporate data on non company issued devices.
- Organizations also need to consider how to support and fund BYOD.
- If not done properly, this leaves unmitigated risk, which could result in unplanned cost, data exposure/loss or breach of intellectual property rights.

Cost benefits are just one factor. Make mistakes on some of the other factors, and it will cost the organization even more.

Implications – Enterprise Standards, Technology and Security

Main concerns

Ensure the necessary security features to protect corporate data and prevent data loss as well comply with Corporate Standards – Security Requirements for Mobile Devices.



How will these security features be deployed?

What happens when a device is lost or stolen?

What happens with the data saved to local backup or iCloud?

What happens when a device is infected with malware?

What happens when the wrong PIN / password is entered too many times?

KPMG Approach

KPMG limited the BYOD program to main OS on the market and implemented dedicated MDM solutions

Implications - Legal and Data Privacy

Main concerns

- MDM features may include activity monitoring, tracking, and remote lock & wipe.
- Employees must give explicit and fully-informed consent for any organization to access and process their personal data.
- Employee consent is also required should a business wish to install a MDM application on their device.

KPMG Approach

•KPMG implemented a BYOD policy:

•addresses the above concerns

•formally communicated and acknowledged by all participants.

- Policies configurations enforced using the MDM were carefully reviewed to ensure compliance with legal and Data Privacy requirements.

What needs to be considered in a BYOD Strategy?

☑ Funding arrangements related to whether to provide a stipend, allowance, reimbursement or no compensation

☑ Staff engagement considerations and expectations

☑ Taxation implications for the organization subject to how the organization decides to fund the arrangement

☑ Legal implications associated with Corporate data on a private device

☑ Commercial considerations in the context of existing telecom and hardware contracts that may run for many years in the future, and the deployment of software licenses

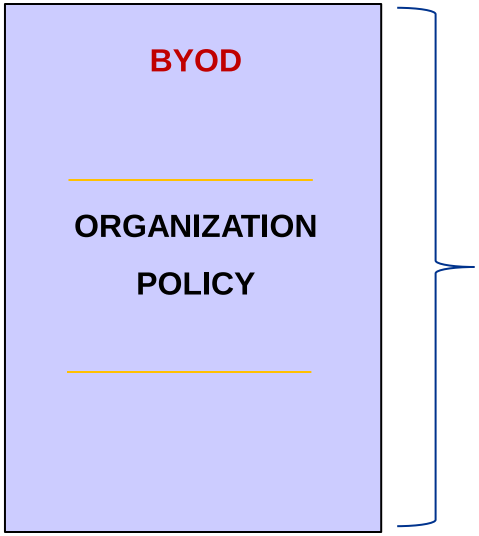
☑ Support considerations with respect to dealing with BYOD

BYOD Policy

Policy

Getting the policy right protects the business from the risks associated with BYOD

- What devices makes and models will be allowed
- How will Antivirus be handled
- What actions does the company reserve the right to carry out on an employees personal device (e.g. remote wipe on loss)
- How will leavers be handled
- What access controls will be used (Certificate based authentication, Pin Number lengths)



Contents

Mobile Messaging Policies and Procedures

1. Technology Standard
2. Service Level and Support
3. Device Loss and Damage Procedures
4. Business Data Protection
5. Data Ownership
6. Device Ownership and Replacement
7. Mobile Device Security Features

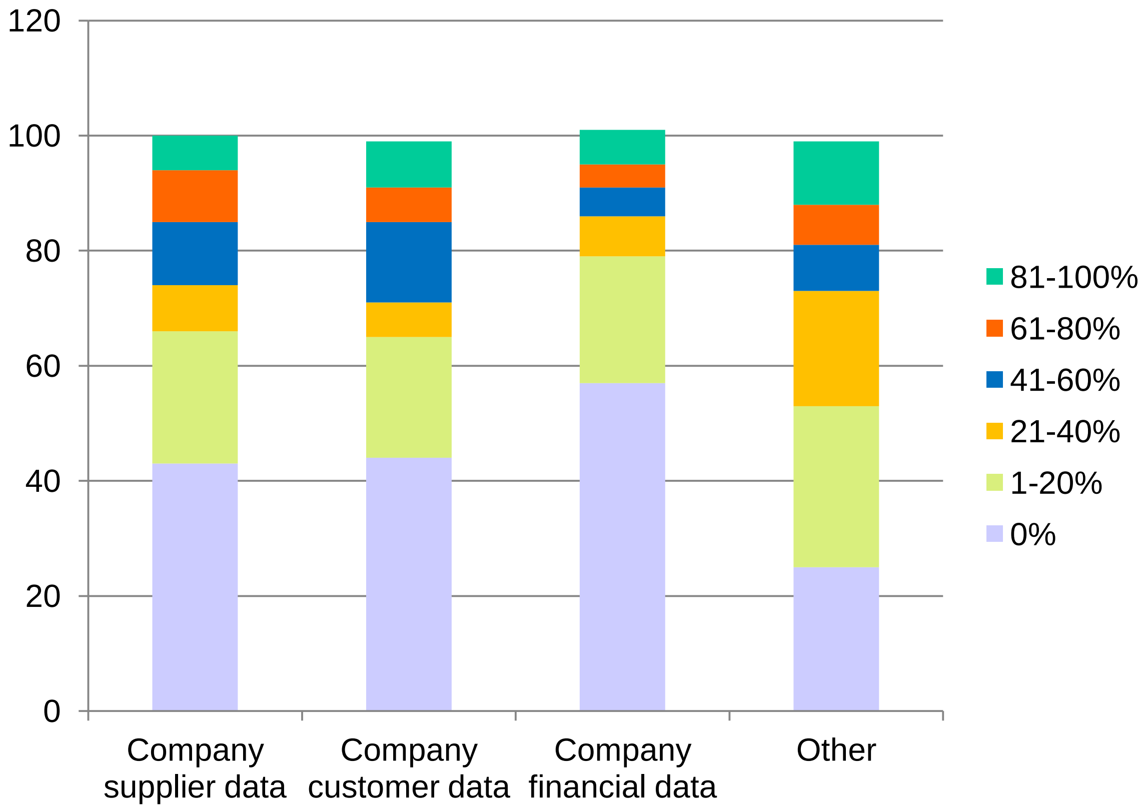
4.0

BYOD – *Secure Zoning*

What corporate data is being accessed?

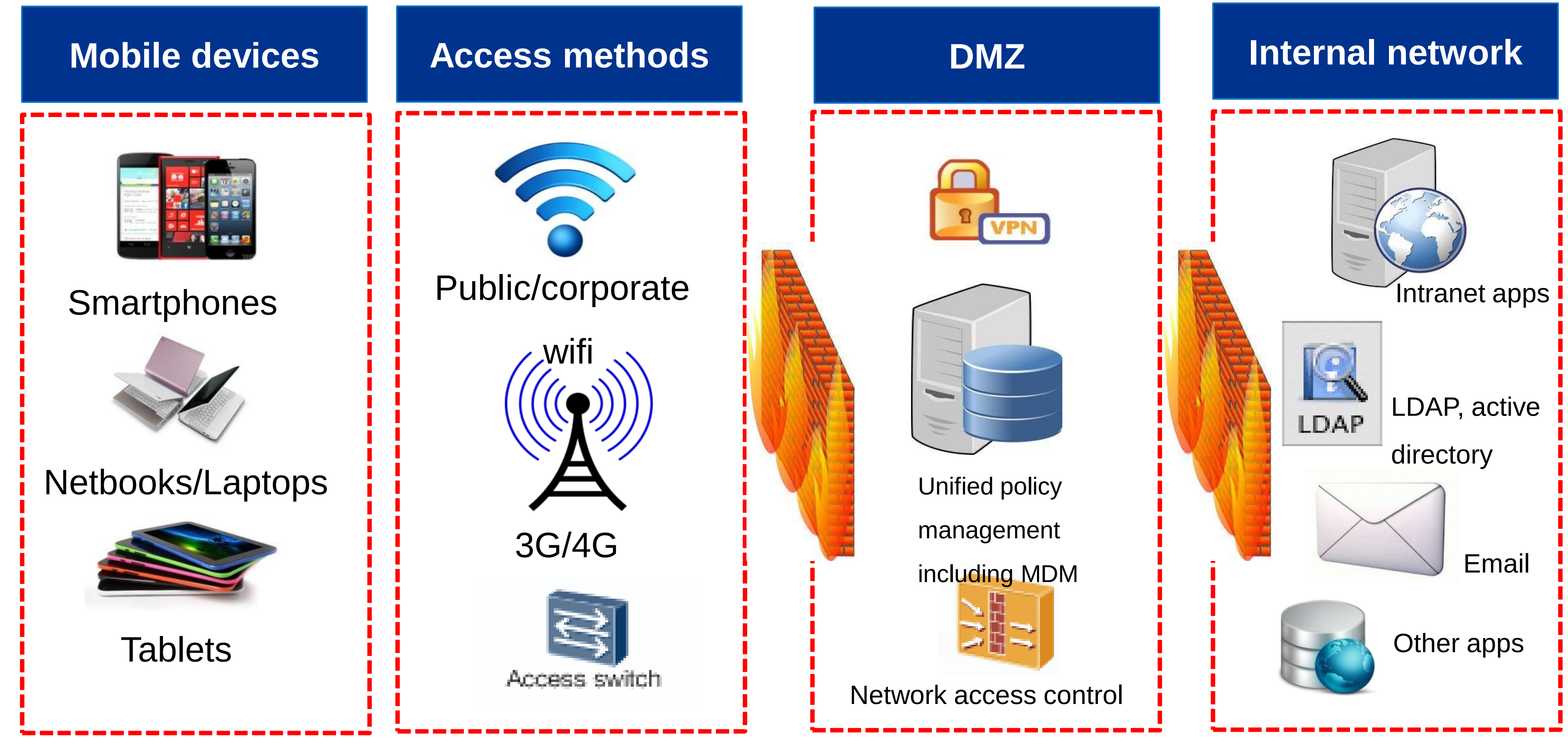
1. Email
2. Intranet application
   a) HR
   b) Financial
   c) … and other application
3. Work related documents
   a) Proposals
   b) Marketing documents
   c) Sales and pipeline information
   d) Client information

***The type of information that staff members have access to based on a general survey**



**Source: ZDNet. (2013, August 6). Nine out of 10 senior staffers have BYOD access to corporate data. Retrieved November 11, 2013, from ZDNet: http://www.zdnet.com/nine-out-of-10-senior-staffers-have-byod-access-to-corporate-data-7000019016/*

Typical security zoning for BYOD and how corporate data is accessed



Mobile devices

Smartphones

Netbooks/Laptops

Tablets

Access methods

Public/corporate wifi

3G/4G

DMZ

Unified policy management including MDM

Network access control

Internal network

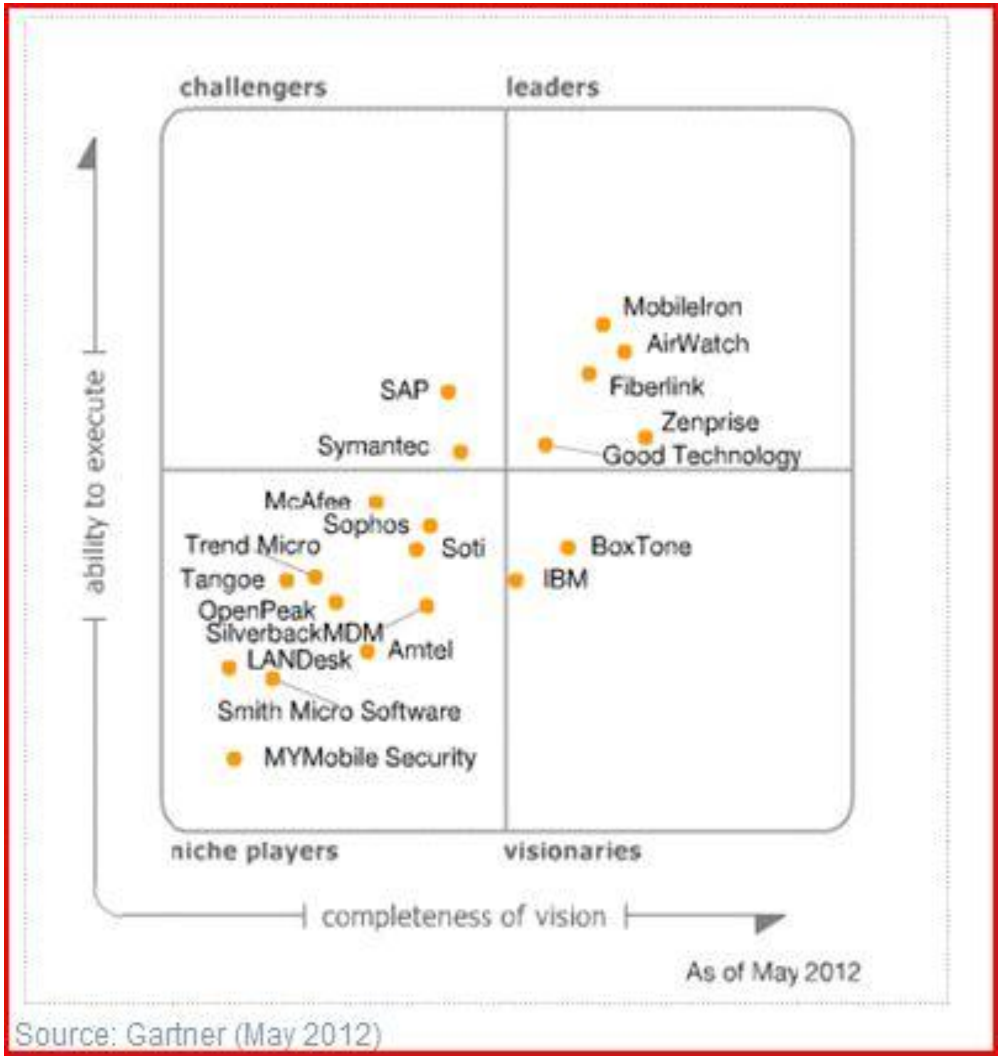
Intranet apps

LDAP, active directory

Email

Other apps

Security zoning on mobile devices



Source: Gartner (May 2012)

Mobile "containerization"

1. Separating corporate mobile applications and data into a secure, encrypted "containers" on the mobile devices
2. Provides clear division as to what is corporate data and personal data
3. Allows IT to control what applications can access what type of data
4. Provides ability to enforce policies on the mobile devices:
   a) Remote wiping
   b) Check for "rooted", "jailbroken" or insecure device configurations

Examples of containerization technologies

1. Good
2. Samsung's KNOX
3. MobileIron

Challenges to Containerization

Challenges

1. Resistance from employees due to ability to remotely wipe the device
2. Remote wipe requires that the device is connected to the Internet
3. Corporate data remains on the phone if device is stolen or lost
4. Ability to support multiple hardware and mobile operating systems
   a) Android represents a challenge due to “fragmentation” – i.e. multiple version of Android operating systems and multiple versions of applications for each operating system
   b) Security – issues of increasing number of malwares for Android

Security zones at the network level

Mobile device management (MDM)

1. MDM software secures, monitors, manages and supports mobile devices deployed across the enterprise, mobile operators and service providers
2. The main functions are typically to distribute applications, data, configurations and policies settings for all types of mobile devices including company-issued and personal devices
3. Optimizes security by controlling and protecting data and configuration settings while reducing support costs and security risks

Network Access Control (NAC)

1. NAC can be combined with MDM to enforce policies in a BYOD environment
   a) For example, personal devices that are not managed by MDM agents should be limited to Internet access only, or placed in limited access zones where they can access a subset of applications and network resources as per user or group role
2. Policies should be able to protect wired and wireless access
   a) For example, policies for smartphones and tablets that requires access through wireless and laptops/desktops that require access through wired network

Sample use cases and policies for MDM and NAC

Use case	Sample Policies
Employee-owned tablets and smartphones	1. MDM agent is required for the device to gain access to wireless corporate network 2. Employee can only use supported devices by the MDM solution **Sample Actions** *1. Non-compliant device (e.g. rooted or jailbroken) are denied access to the wired network. This is detected by the MDM agent* *2. If MDM agent is detected, the device is granted access and access to applications are based on user/role* *3. If no MDM is detected, the device is granted access to the guest network with Internet access*
Employee owned laptops	1. IT-issued NAC agent is installed 2. Up to date patches are required 3. Up to date anti virus signatures are required 4. Disk encryption is required 5. Personal firewall is turned on and some ports are blocked 6. DLP agent is required **Sample Actions** 1. Full access is granted if the laptop is compliant 2. If the laptop is non-compliant, it is granted access to guest network with Internet access

Security zones on the laptop and applications

Desktop virtualization

1. Enables separation of corporate data and applications from the employee’s personal laptops or mobile devices
   a) No data resides and no work is physically performed on the BYOD device, therefore corporate data remains secure
   b) Policies and access control are centralized which provides a manageable security control around corporate data and applications, therefore risks are easier to mitigate
2. A myriad of solutions exists such as virtual desktop infrastructure (VDI), hosted virtual desktop (HVD), desktop as a service (DaaS), and server-based computing
3. Support can be extended to tablets and smartphones

Application virtualization

1. Also know as “application streaming” or “session virtualization” – neither the application or the data is on the BYOD
2. Provides full desktop experience for employee – the OS on BYOD “thinks” the application is running locally
3. Sample technologies: Citrix Receiver, XenApp, App-V

5.0

Case Studies

Summary of BYOD in KPMG Romania

2012 BYOD program allowing employees to use their own smart phones to access relevant corporate data:

In the past...

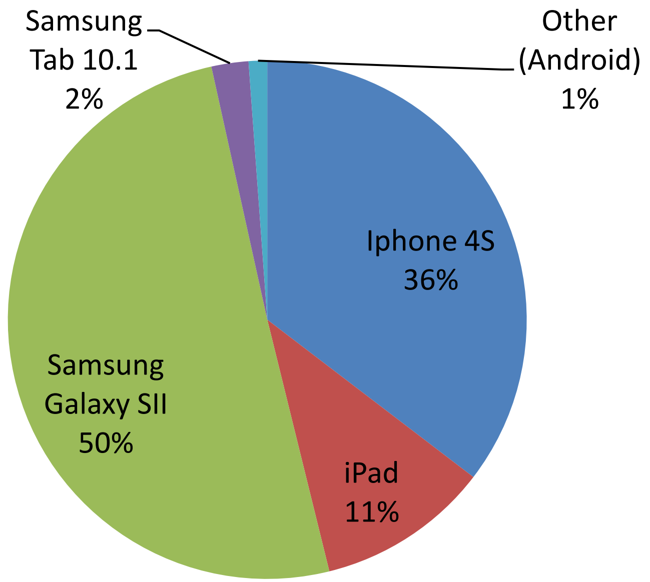
- Around 150 BB used by Managers and above
- Mainly used for corporate email access
- Cloud based services (private cloud)
- Expensive solution, especially in roaming

Drivers for change

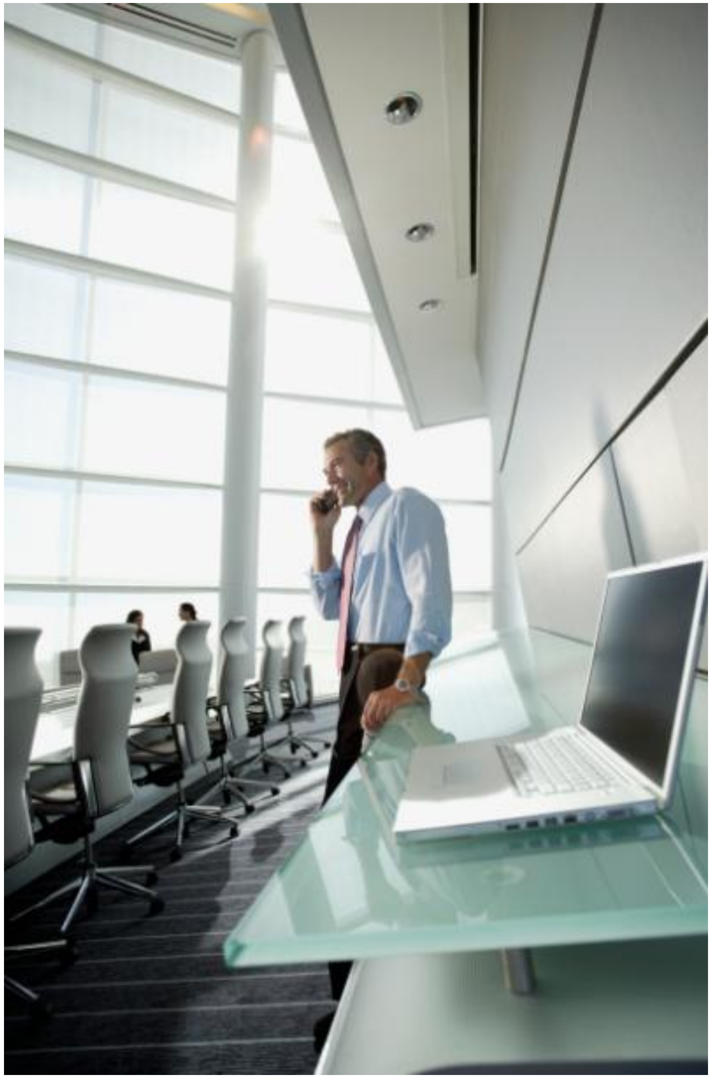
- Proliferation of smart devices
- KPMG people
- Need for mobility
- Cost management

Today

- 260 smart devices (phones and tablets) activated
- Traffic volume increased by 30%, costs reduced by 10%
- After 6 months review the business case was confirmed
- Legal and Data Privacy aspects considered and formalized in a BYOD policy
- MDM solution implemented but processes are complex and need time to stabilize
- Initiative well received by KPMG staff (user satisfaction increased)
- Behavior changed (efficiency & innovation)



BYOD in KPMG Romania – *Lessons Learnt*



Enrolling mobile devices results in new risks

- ✓ Broader then expected, e.g. legal, technology, integration, backups
- ✓ Security controls work differently on mobile devices

Technical Solutions

- ✓ Different security architectures to reduce risks of mobile devices
- ✓ No technical solution fixes it all, mitigate risks by people, processes and technology

How to continue

- ➢ Perform risk assessment before implementation
- ➢ Consult with relevant experts
- ➢ Implement security controls for people, process and technology
- ➢ Test effectiveness of security controls
- ➢ Stay up-to-date with recent developments
- ➢ Structured approach, phase by phase

Summary of BYOD in KPMG Malaysia

Highlights on KPMG Malaysia’s BYOD program:

In the past...

- 2004; started with Blackberry devices
- High investment; only 50 units were used by Partners
- Users are able to read and response to email in a more timely manner on the go

Drivers for change

- Proliferation of smart devices
- KPMG people
- Need for mobility
- Cost management

2008 - 2012

- In year 2008, deployed Activesync on Exchange for all management staff.
- Managed to deploy 250 users on Activesync on Exchange without heavy investment as the device was essentially owned by the user.
- Security and device management became an increasing challenge. The popularity of mobile devices also saw an increase of malwares/vulnerability exposures on these devices that could pose a risk to the firm.
- In 2012, Global ITS recognized the need to use mobile device management (MDM) to further strengthen the BYOD concept by enforcing Mobile Device Management.
- The cost of the device management was shared by all countries thus enabling smaller countries to embark in BYOD without expensive MDM investment.

KPMG

cutting through complexity™

Rozana Rusli

Executive Director

Tel: 603 7721 7087
rozanarusli@kpmg.com.my

Meling Mudin

Associate Director

Tel: 603 7721 7184
melingmudin@kpmg.com.my

cutting through complexity

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.