BYOD Governance

Sumari Botha, Manager
KPMG LLP

10/31/2013

kpmg.com

Contents

- Introduction
- Where we are
- The Challenges of Mobile Computing
- Taking control of Mobile Security and Privacy
- Technology – The Good, The Bad and the Ugly
- Governance
- Key assessment issues
- Key Considerations
- Policy
- Enabling
- Legal
- Impact
- Q&A

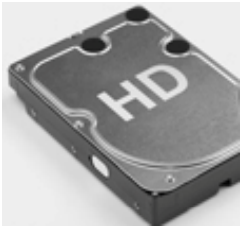
Email

Social Media

Removable Disks

PDAs & Cell Phones

CD's & DVD's



Solid State Storage & Tapes

Portable Scanners

PCs & Workstations

Ipods/Mp3 players

Where are we?

First corporate shift since 1960s

1. It's not "Bring Your Own Device", it is "Brought Your Own Device".
2. It's about personal productivity and ease of use… and "ease of use is what you know".
3. The corporate IT organization no longer dictates what technology will be used to access corporate data, the consumer marketplace does.
4. Consumer technology is improving every 3 months, not every 3 years when a laptop would end its depreciation… and user and corporate executives which IT reports to are not waiting.
5. A phone has for a long time already not been just something you use to make a phone call with…it's seen as a mini handheld computer now with limitless possibilities.
6. The issue is the 12 hour window… on Sunday night employees have instant on access to everything globally on the web with a literal touch of their finger, no wires, new applications in seconds, high resolution with Bluetooth high fidelity audio. Not, less than 12 hours later on Monday morning they are waiting for a 30 minute boot up time with slow response, can't find items with an internal intranet corporate search and green screen emulation has applications that don't match how their existing process and IT saying they will deliver applications in 6 months if at all.

Where we are (cont.)

Latest research from Gartner suggests that by 2017, half of employers may impose a mandatory BYOD policy — requiring staff to bring their own laptop, tablet and smartphone to work[1].

1. 38 percent of companies expect to stop providing workplace devices to staff by 2016. (PCs, such as desktops and laptops, are included in the definition of BYOD).

2. BYOD is most prevalent in midsize and larger enterprises, often generating between $500m-$5bn in revenue per year, with 2,500-5,000 employees on the roster.

3. BRIC nations, such as India, China, and Brazil, will most likely already be using a personal device — typically a "standard mobile phone" — at work.

4. Meanwhile, companies in the U.S. are more likely to allow BYOD than those in Europe (likely due to stronger data protection rules, see below).

5. Around half of all BYOD programs provide a partial reimbursement, while full reimbursement costs "will become rare."

1. “Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes”, May 1, 2013, http://www.gartner.com/newsroom/id/2466615

Where we are (cont.)

1. Of 1100 Senior Executives and Managers*

- 67% do not have any polices, procedures or IT systems in place to manage the use of personal devices
- 54% are not aware of all the devices their staff are using for business purposes
- 90% of organizations will support corporate applications on personal devices by 2014 according to Gartner

Technically “savvy” individuals in your company are supporting their friends and non approved devices to access the network and corporate records to improve their personal productivity because corporate IT has left them behind

* Source: YouGov, Research Now and Citrix survey conducted between May and August 2011.

Where are you?

Your company. How would you categorize your BYOD status?

1. Do your employees use any personal devices?... What about for business?
2. Does your company dictate what device or devices can be used?
3. Does your company have a Brought Your Own Device policy? What does it say?
4. Does everyone know what it is and where to get it?
5. If there is no policy, is there an advocate within your company or a compliance group?

How did you get here?

1. Explosion of smartphones and affordable personal data assistants (pda)
2. Cloud computing common marketing and cloud delivery of the pda application
3. Tablet affordability, speed of use and the reality of reduced touch interface
4. Two holsters and the quick draw
5. When is the last time you ordered something from your corporate equipment from IT

The challenges of mobile computing (or BYOD)

- Is not only what devices will be support but what operating systems and applications. Will you support multiple operating systems?
- As enterprises and individuals embrace cloud computing, their most trusted data is migrating to systems that are continuously accessible via mobile devices.
- Google and Facebook has 37 pages terms and conditions of use… will take your data, not agree to delete it and sell it to “their partners”. Do your employees have corporate records on their mobile devices?
- Proliferation of mobile applications makes it difficult for users to track and understand the danger of their security or privacy being breached by third-party code.
  - In 2009, just one year after the first mobile apps were put onto smartphones, users downloaded more than 9 billion of them; two years later that number had more than tripled to 29 billion. Pundits suggest that 2015 will see the number soar to 183 billion.
  - Android has nearly a million applications developed. Trend Micro claimed that roughly one in ten apps on the Google Play app store was outright malicious.
  - The Apple store regularly rejects up to 7% of submitted applications because they violate Apple’s mobile application guidelines.

6B people use mobile phones, 1B are smartphones

Taking control of mobile security and privacy

- Mobile devices are it's own worst enemy
  - small size and compact design, while a key feature for consumers, also means that mobiles frequently end up lost in the back of cabs and other public places.
  - small user interfaces and tiny keypads – central to their convenience – also tends to lead users to use shorter and often less secure passwords.
- However, the potential security and privacy attributes of mobile may, in the long-term, far outweigh the risks.
- Take a balanced approach
  - Ease of use: Mobile security processes must be straightforward and convenient.
  - Customer Awareness: Education will be a key component of overcoming consumer's security concerns.
  - Technology planning: Ensure that developers and IT leaders are thinking about the deeper tactical implications of mobile and how these impact the risk profile for the company .

Technology – The Good

Ranking the devices:

- iOS6 – Can be configured to be the most secure of the current set of mobile OS/devices
- Samsung SAFE with Android 4.2 – Can be configured to be very secure via MDM, probably the same as iOS6
- Android 4.2 - Can be configured to be quite secure via MDM
- Android 3.x and below has security risks that need to be understood and accepted

The Enterprise Software:

- Good Technology – Some prefer the concept of Good's fully containerized solution, but the choice comes down to understanding where they want to go with "Consumerization" and how much the company will want to spend.
- MobileIron – Many perceive the MobileIron interface as better.
- AirWatch – Mobile Device Management
- Citrix – Application and Data containerization

Technology – The Good

Criteria for selecting Mobile Device Management solutions:

- Internal resources for management and support
- Complexity of data
- Cross-platform needs
- Delivery – on premise or cloud based

If you just want to have email and perhaps edit some simple documents: Good Dynamics is probably the most secure for Android and WP7 and also the most expensive.

If you want to develop corporate applications then, AirWatch or MobileIron gives you marginally more flexibility, and if you limit devices to iOS6 and Android 4.2, you can get close to the security levels of a Good Implementation.

Technology – The Bad

Windows Phone 7 lacks a few fundamental features… it's not suitable for BYOD use when accessing Enterprise data.

- WP7 doesn't support certificate based authentication for Email to Exchange Active sync.
- WP7 remote wipe on the device only deletes the email profile not the email on the device if you're using the native email client. This prevents any further email being downloaded but the user walks off with all the email they already had.

Earlier versions of Android encryption and application store vulnerabilities

- Approximate 40% of the Android devices in the wild are still running 2.3.x which does not support device encryption by default.
- Android is plagued with the weak security in the Play store compared with Apples App Store.

Technology – The Ugly

Top issues faced by mobile devices:

- Physical Security
- Secure Data Storage (on disk)
- Strong authentication and multi factor authentication with Poor Keyboards
- Multiple-User Support with Security
- Secure Operating Systems
- Application Isolation
- Virus, Worms, Trojans, Spyware and Malware
- Strict use and enforcement of SSL
- Phishing
- Location Privacy/Security

Governance Strategy

1. User
2. Risk and Security
3. Privacy
4. Financial
5. Support
6. Applications

Assessment

1. Who is eligible to bring and use devices?
2. Will the company support any device or only a specific list of devices?
3. Do your employees care? Is your support worth using a specific device?
4. BYOD processes in place for requesting access to IT services, data and mobile applications?
5. BYOD processes in place for granting and fulfilling access
6. How will the company protect data privacy and what are the security requirements?
7. Will the company reimburse employees and track usage?
8. How will the devices be managed, data wiped and monitored?
9. Do you have security requirements?
10. Do you use mobile device management software?
11. Is there a governance strategy in place?

You need a policy as soon as possible.

Consider

1. What services
2. Survey and assess what employees are actually doing
3. Review each governance item per service
4. Establish roles and requirements on how devices are used
5. Policy must match processes, procedures within your culture behaviors
6. Benefits
7. Risks
8. Possession, custody, and control
9. Preservation and retention
10. Litigation
11. Set expectations with service level agreements
12. Realize what is happening, don’t ignore it and trust your employees
13. Employees will want to do the right thing
14. Ease of device registration
15. Improved productivity to the workforce

Policy

- Risks of key-logging on personal devices
- Meeting requirement of encrypted VPN connection
- Geo-location tracking
- Filter bubble, six characteristics of an individual, PDA user profiling
- Access to personal email, chat, and social activity
- Handling of personal music, movies, and financial information
- Risks of data transmission from personal devices
- Benefits of setting up a “sandbox” for corporate information on a personal device
- Options for handling and accessing personal device passwords
- Wireless access policies
- Acceptable use policies, such as securing devices and closing down devices if unattended
- Incident reporting practices and cooperation with corporate requirements
- Lost device process incident
- Device recycling/disposal at end of lifecycle

Enable

Define Needs, Roles, Rules and Policy:

- Activities and business unit needs that truly require corporate data access
- Data access requirements and privacy requirements
- Sharing requirements and collaboration
- Roles and rules requirements

Define Levels of Support for Personal Devices. Policy should include clear definitions for support including:

- User roles and needs that qualify for personal device usage and support
- Geographic area that qualifies for support and access
- Expense policies
- Devices, versions, and operating systems that will be supported
- Minimum system requirements and configurations

Enable

Obtain OGC approval before implementing your BYOD policy. Legal and training requirement should minimally include:

- Liability clause for damage, corruption, and data deletion
- Consent and waiver agreement
- Training on privacy trade-offs and expectations
- Training on support and update requirements

Legal

- Demonstrate consistency in security software and applications installed on all personal and corporate devices
- Obtain and retain personal devices for audits — Clearly stated requirements for turnaround times and longevity
- Demonstrate consistency in policy and applications security on all personal or corporate devices — Anti-virus, anti-malware installations, encryption installation, updates and patches
- Monitor device use to detect misuse, hacking, or malware
- Determine how the device connects to the company's network
- Obtain rights to access the device for purposes of an investigation
- Integrate, terminate, or limit existing activities accordingly
- Wipe, brick, lock, or disable lost or stolen personal devices to secure corporate data
- Send notifications to wipe data if devices are sold, retired, or reassigned

Impact

- Nobody ever grew their business by maintaining the status-quo. So it is with mobile: those organizations willing to innovate their business and operating models are achieving results in the new mobile era, while those standing on the sidelines are quickly falling behind.
- It is happening. Address it and reduce risk.
- Develop a digital strategy that not only reflects the business objectives, but also customer and employee needs and expectations.
- Enhance efficiency, increase productivity
- Allow them to make the choice to use tools they will use
- Align your organization with the roles to meet the actual need and not perceived IT need
- Reduce IT asset expenditures to meet actual usage
- Put the right tools in the right hands at the right time

Thank you

Sumari Botha

sumaribotha@kpmg.com

858-230-1571