IBM Global Technology Services
Thought Leadership White Paper

December 2011

The New Workplace: Supporting "Bring your own"

IBM

Contents

Sales of smartphones and media tablets like the Apple iPad are exploding in the consumer marketplace. While some companies issuing smartphones and tablets for employees, the majority of employees are bringing personally-owned devices to the workplace and using the business purposes—often without explicit company approval. In this paper, we will explore how you can derive business value from "Bring your own device" (BYOD), while still providing a security-rich IT infrastructure and consistent service levels.

Consumerization takes hold in the enterprise

Back in 2005, researchers at Gartner, Inc. first tagged the "consumerization of IT" as "the most significant trend affecting information technology (IT) during the next 10 years" Today, few would argue with the industry analyst's projections that, "As a result, the majority of new technologies enterprises adopt for their information systems between 2007 and 2012 will have roots in consumer applications."[1]

Although consumer technology advances are nothing new, what has changed is the push to leverage smartphones and tablets to conduct business. There may be a number of reasons for this trend:

- Many of these smartphones and tablets, along with the growing number of enterprise-class mobile applications, have powerful capabilities. They now far exceed those of the "standard issue" device from the IT department, making them much more desirable.
- Consumer mobile devices have become so pervasive in daily life due to improvements in technology (for example, small size, instant on, wireless Internet connectivity and so on.), and comfort level exists that did not with "corporate" devices. In fact, this probably reflects a cultural shift as much as a technological one.
- Companies are demanding their employees to do more with less. Today's employee is increasingly empowered and technology-savvy workers. Employees are turning to whatever helps them achieve that goal—and in many cases, that is not the PC chained to the office desk.
- Many enterprises issue corporate-liable devices to a small subset of the company, such as sales. Although mobility requirements are increasing, most enterprises are not expanding their corporate-liable programs due to cost pressures. Instead, they are exploring the employee-liable model to deliver mobile services to a larger population of users at reduced cost.

The risks of not embracing BYOD

It may be tempting to ban the use of personally owned devices in the enterprise, but corporate policies that take a hard line may simply not be enforceable. Corporate smartphone and tablet users may circumvent corporate policy, putting the enterprise at greater risk. For example, users may forward corporate email, documents and presentations to consumer services like Google Mail or Dropbox so they can be accessed from their smartphones and tablets, creating a kind of "shadow infrastructure" over which enterprises have little control and increases the risk of data leakage. In addition, not embracing BYOD can also lead to lower employee satisfaction and difficulty attracting and retaining top talent.

Strategy

So how do you say "yes" to personal devices without having the mess of governance, security, integration and support issues? By taking a methodical approach, rather than a reactive one. The following are a few key questions to consider:

- Business objectives and end user scenarios: What applications do your employees and customers need to access on mobile devices and what devices are they using?
- Corporate culture and corporate policy: Does your company have a policy for the use of personally owned devices? Is the policy voluntary? What corporate data can be accessed? What's the security policy? What's the re-imbursement policy for mobile expenses? (E.g. device, voice, data) What's the corporate culture with regards to mobile workers and does it align with my strategy? Do I need to separate work and personal data on mobile devices? How do I handle lost or stolen devices and employee separation?
- Information Technology: What IT solutions do I need to delivery the strategy? How do I manage mobile devices? What's my mobile application strategy? How do I support a wide range of mobile devices? How do I monitor compliance with corporate policy?

Solutions

Once the strategy has been developed, you'll need to explore IT solutions. The following are a few you may want to consider

- **Mobile Device Management (MDM):** If your requirements call for the ability to manage devices and compliance, you'll probably want to look at one or more Mobile Device Management solutions to enforce corporate security policy and monitor compliance
- **Applications:** What applications will my users use? Are they available out of the box? Are they web, native, hybrid or virtual? Do they meet my security requirements? Do I need to create custom applications? Do I need to explore Mobile Enterprise Application Platforms? (MEAP). How do I deploy and manage application? Do I need an enterprise application store to manage and distribute applications? Do I need to prohibit the applications that users can use on their mobile devices? Are there applications that employees must run on their mobile devices? (E.g. anti-malware)
- **Network:** How will users connect their devices to the corporate network via Wi-Fi and cellular. If my employees are connecting to the corporate Wi-Fi network, do I have adequate Wi-Fi coverage and capacity? If employees are connecting from offsite, do I need one or more VPN solutions?
- **Support:** How will I provide support for a variety of devices? Can I automate common tasks such as device registration to reduce administration overhead? How do I educate employees on how to use mobile devices effectively?

Lessons Learned from IBM's internal deployment

In 2009, IBM undertook an aggressive campaign to support enterprise mobility and smartphones and tablets in particular. By the end of 2011, is it estimated that IBM will have in excess of 100,000 smartphone and tablet users with access to the IBM corporate network. The most popular platforms include Google Android smartphones and tablets, Apple iPhone and iPad and BlackBerry.

The following are a few of the key lessons learned:

- Employees are supportive of personally owned (and funded) smartphones and tablets
- Employees want to use a single smartphone for personal and business use. Most users don't want to use two smartphones—one for work and one for personal use
- The majority of employees were supportive of the devices and platforms that IBM elected to support (E.g. Android 2.2+, iPhone 3GS+, BlackBerry, etc.). However, there were additional devices and platforms that employees asked for that could not be supported due to security requirements
- Generally, employees appreciated the need to enforce security policies on the device. However, this was a deal-breaker for some users. The biggest customer dissatisfier is the eight-character alphanumeric password to unlock the device. Employees are requesting better separation between work and personal data and the ability to secure just the "work" data
- Remote wipe of an entire device is unpopular with employees. Employees applauded the recent enhancements to Lotus Traveler which allows remote wipe of just corporate data (E.g. email)
- Browser-based cloud solutions like Lotus® iNotes® ultra-light mode provides flexibility, reduces device dependencies and addresses data at rest security concerns
- With multiple smartphone and tablet options, we needed to provide guidance to employees so they could make informed choices on what the best device(s) were for their particular needs
- Enterprise capabilities continue to lag in a consumer-driven market
- Leveraging Lotus Mobile Connect clientless SSL proxy provided the best end-user experience on Apple iOS and Google Android. However, this necessitated the use of a separate, VPN client solution for general access to the corporate network. Employees were receptive of self-service support options including automated onboarding and diagnostics

IBM Mobility Chronology

2004-2007: BlackBerry smartphone is the sole option, with limited employee access

2008: Limited proof of concept for Windows Mobile leveraging Lotus Traveler

2009: Launch pilot and expand to include Nokia and Apple iOS and embrace personally owned model with expanded access via Lotus Traveler

2010: Complete pilot and begin production deployment. Expand platform support to include Apple iPad and Google Android

2011: Wide-scale production deployments, with mobility as a core infrastructure service instead of an add-on. Native mobile clients for Sametime Instant Messaging, IBM Connections and Symphony Viewers on Apple iOS and Android

End-User Support for BYOD

With a wide range of smartphones and platforms to support, the help desk can quickly become overwhelmed. To address this concern, we advocate self-service support and automation. Specifically:

- Up-to-date online documentation with device, platforms, services provided and employee responsibilities
- The ability to activate a new device online without administrative interaction
- Heavy use of social media inside the company to leverage "wisdom of the crowds." This is critical as new devices and OS versions are released weekly
- The ability to perform common tasks online including device reset and wipe

For more information

To learn more about IBM Enterprise Services—managed mobility services, contact your IBM marketing representative, IBM Business Partner, or visit the following website: **ibm.com**/services/mobility

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
December 2011

[1] Gartner, Inc. (October 20, 2005)."Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years". Press release. Retrieved from http://www.gartner.com/press_releases/asset_138285_11.html

Please Recycle

ENW03010-USEN-01