IBM Software
Thought Leadership White Paper

December 2011

Mobility is moving fast. To stay in control, you have to prepare for change

Are you ready for BYOD? Here are seven questions you should answer as you roll out new mobile capabilities

IBM

Contents

Introduction

When it comes to employee-owned smartphones, tablets and other mobile devices in the workplace, the numbers do the talking. A recent survey by The Aberdeen Group found that 72 percent of responding companies allowed the practice known as BYOD—bring your own device.[1] And Information Week, in its own study, found that 65 percent of organizations expect BYOD adoption to increase.[2]

The business use of personal devices has surged dramatically. Between 2008 and 2010, the number of companies allowing phones based on the Google Android platform went from zero to 43 percent. And the use of Apple iPhones accelerated from 28 percent to 66 percent.[1]

The reason? While smartphone vendors have begun to more actively pursue corporate markets and design their products to meet business needs.[3] It is the consumerization of IT—users' desire for the same functionality in their business devices that they have in their personal ones—that usually gets the credit. For 61 percent of The Aberdeen Group's respondents, the principal reason for allowing BYOD smartphones and tablets was employee demands for mobile functionality beyond simple email and calendaring.[1]

Interestingly, employee enthusiasm for BYOD comes even when employers don't support their devices. While 43 percent of organizations both allowed and provided formal corporate support for iPhones, 34 percent more allowed use but provided no support. For Android phones, 30 percent provided support, but another 31 percent allowed use without support.[1]

It is clear that smartphones, tablet computers and other mobile devices are in the enterprise to stay. In the 2011 *Information Week* survey, 82 percent of respondents looking ahead two years said they expected smartphones to play a "critical role" in business productivity. Tablets weren't far behind, with 79 percent of respondents calling them critical to productivity—a significant increase over the 36 percent of the previous year. By contrast, only 36 percent deemed laptops critical to productivity, down from the previous year's 53 percent. [2]

These numbers tell a compelling story—but to most effectively respond, the enterprise has to do more than listen. The time has come to act.

This white paper notes that it is not enough simply to give users permission to use their personal devices for work. For successful BYOD operations, organizations must address issues they may not have considered yet, but that can have significant consequences for business and IT operations.

BYOD raises questions you may not have considered

It is common for discussions of BYOD to begin with concerns about security, or to focus on managing the vast amounts of data that these additional devices generate. But the BYOD

discussion reaches beyond security to encompass a wide range of endpoint management issues. And it reaches beyond data loads to encompass a broader impact the devices have on infrastructure and operations. The BYOD discussion is still relatively new, but it is pointing the way to change—and it is raising key issues that organizations must be ready to address.

From an organizational perspective, the rapid adoption of smartphones and tablets already is eroding cultures in which IT managed technology and controlled access to resources by selecting, purchasing, deploying and supporting employees' mobile devices. Those practices and those devices, most often the BlackBerry platform with a focus on voice, email and calendaring, are not gone. But BYOD scenarios and the more robust, application-based focus of smartphones and tablets are taking over.

In only one year, from 2010 to 2011, *Information Week* charted a drop in the number of organizations standardizing on a mobile device platform from 73 percent to 58 percent.[2] And in the two year period from 2008 to 2010, The Aberdeen Group saw the use of BlackBerry platform decline from 81 percent of organizations to 73 percent[1] —still a healthy number, but a change that indicates a coming era of more complex heterogeneous environments for IT and more productive functionality for business users.

Whether they are collecting global positioning data, supporting business transactions or interfacing with the network to ensure optimal performance for technology functions, mobile devices are at the heart of today's services and operations. On today's smarter planet, data gathering, information sharing and decision making must continue regardless of the user's location in order to support highly competitive businesses.

The explosion in the numbers and types of mobile devices, as a result, spawns questions that organizations must address if they are to gain the most benefits possible from employees, their devices and the business network.

Is your network ready for more complexity?

It is true that an increase in the number of devices does not increase the amount of data by the same rate. After all, each employee uses only one device at a time. But more devices does mean more opportunities for gathering data and more opportunities for connecting with the network. The network, as a result, has to grow and evolve to meet those increased demands.

In a BYOD scenario, the organization can achieve significant cost savings because it is not purchasing devices. But the resulting need to manage multiple operating systems and hardware platforms can cause its own expense—and significant IT headaches. For while applications on smartphones and tablets move mobile business connectivity beyond voice and email, they increase the need for more bandwidth and larger infrastructures. And the organization faces a growing need for more effective network management.

Virtualization is one solution. The enhanced resource utilization and streamlined management it makes possible helps accommodate more users, more devices and increased movement of data. But any environment will need capabilities such as event management and root cause analysis to ensure device performance, as well as discovery and centralized management to keep tabs on far flung mobile assets.

2 Can your help desk handle the coming flood?

When users bring their own devices, they bring a wide range of personal abilities—or lack of abilities—to device use. Even employees who are proficient with their devices or who rely on their vendor to resolve device problems likely will need help with internal procedures such as device configurations or network connections. What's more, the demand grows all at once. A company initiating a BYOD policy typically finds that large numbers of employees want to join the program immediately. The sudden need for additional bandwidth and infrastructure can cause performance problems, and the help desk can be swamped with calls for aid.

A larger help desk staff may be necessary, at least in the beginning. But there are other steps that the organization can take. Just as organizations manage the customer experience, managing the employee user experience can help improve employee productivity and morale, and reduce the cost of help desk support. The process involves monitoring data such as connection times or frequency, and ensuring adequate bandwidth is available to meet the need.

3 Are your BYOD mobile devices secure?

Smartphones are small, and they are easily lost or stolen. It's no wonder, then, that 93 percent of organizations rank the security of mobile devices at least equal to other security concerns. Nearly 60 percent rank it as high or among the highest priorities—with "among the top priorities" the fastest growing level of concern.[2]

The BYOD scenario, however, raises the security risk still higher. Because employees also use their smartphones and tablets for personal reasons, they typically carry the devices with them constantly, smartphones are always connected to the network, and users frequently connect to the business from casual, less secure environments such as coffee shops. Also because the equipment is personal, employees often resist security measures that place management agents or software on the device. In these cases, IT must find other ways to keep both the mobile devices and the business environment secure.

The challenge, then, is to effectively limit network access to authorized—and verified—users without hurting employee productivity. Encryption must be managed to keep data secure during transmission. Change, especially to device configurations, must be managed to support compliance with regulatory requirements. And if a device becomes compromised, IT must be able to remotely wipe it clean before sensitive business data falls into the wrong hands.

Is your app store open for business?

Allowing employee-owned devices that provide functions beyond simple email, calendaring and voice functions can be an important step toward greater business efficiency. But it is only the first step. As in consumer electronics, where users can download applications from Internet sites known as "app stores," business organizations increasingly support BYOD functionality by developing and distributing applications of their own.

Organizations now typically develop light, thin applications that focus on specific tasks. But an organization that develops its own applications and distributes them through an internal application store can achieve big results. Companies taking take this step report increases in employee productivity as great as 45 percent and in operational efficiency as high as 44 percent.[1]

Next steps include extending existing business applications to mobile devices, and deploying mobile versions of third-party software for functions such as customer relationship management, enabling still greater functionality that is more widely and easily available than ever before.

Are new services ready to roll out?

By definition, customers, business partners and other external stakeholders bring their own devices when they interact with the organization and its infrastructure. Extending existing business services and creating new services for the world outside the organization, as a result, can dovetail nicely with an internal BYOD initiative.

Service providers already face the issues and opportunities that come with a large and heterogeneous base of user devices. They need to provide more than a data pipe. They need to put into place an infrastructure that increases bandwidth, then manage it with tools that improve the customer experience. Service providers need to carefully control and balance capital investments with operating costs to support a sustainable revenue stream.

Increasingly, enterprise organizations need to do the same. As the world becomes more instrumented, interconnected and intelligent and as it expands into new markets, organizations need to provide increasingly valuable services both internally and externally, regardless of the device the end user chooses.

6 Are management policies and procedures set?

Allowing BYOD smartphones and tablet computers means more than saying "yes" to employee preferences. It means putting into place policies that govern how devices will be used and how they will be managed. Many of these policies regulate issues that are unique to portable devices—from which telecommunications carrier to use, to who pays for the service, to how data will be removed from the device if it is lost or stolen.

Most organizations recognize the importance of such policies. Compliance and policy settings, along with policy enforcement, are the control features most frequently cited as important. But as important as policies are, only half of organizations have written policies and procedures that directly address the issues surrounding the use of mobile devices.[2]

Procedures for managing devices are similarly important, ranking nearly as high as policies among organizational priorities.[2] In a heterogeneous BYOD environment, the selection of management tools can be critical. Large numbers of point solutions can create management chaos. The organization can reduce complexity, however, with mobile device management solutions that integrate with its existing management infrastructure—just as BYOB smartphones and tablet computers integrate into business processes.

7 Are all of your employees aware?

Using a smartphone or a tablet at work is not the same as using it at home—even if the user owns the device. Employees may have selected their own platforms and form factors. They may to a certain extent have selected their own applications. But an employee education program still is necessary to ensure that employees understand the policies that govern the use of their devices, to help them take advantage of the resources available to them, and to streamline device management so users and IT alike can remain as productive as possible.

Consider, for example, the fact that a sudden and large influx of BYOD mobile devices can slow performance on the organization's Wi-Fi network. But if employees are aware of alternatives, such as the ability to connect to a femtocell—a device that beams cell signals short distances and routes them to the broadband network—they can not only enhance their own connectivity but relieve heavy traffic on the organization's wireless infrastructure.

It is therefore to the organization's advantage to develop a tech savvy workforce, and not to assume that use of personal devices is entirely an individual responsibility. Default settings, configurations, compliance with policies all must be communicated. Employee awareness becomes a key building block that supports the success of the BYOD scenario.

Conclusion

Regardless of whether you are just now implementing a BYOD policy or you have one fully in place, IBM can help you meet the IT challenges of multiplatform, multivendor, employee-owned mobile devices.

When you are expanding your network to accommodate new business and technology requirements, IBM can help ensure the infrastructure and bandwidth necessary and to put into place capabilities for reducing costs, generating new revenues and achieving competitive success.

When you are faced with the management challenges inherent in the business use of smartphones, tablet computers and other mobile devices, IBM can provide the tools you need to reach beyond the traditional endpoint management paradigm. The IBM white paper Managing the growing pains in today's expanding networks describes effective management technologies for expanding environments and discusses management products that can meet your unique needs.

IBM delivers the full breadth of coverage you need for optimizing networks, securing and managing mobile devices, efficiently and securely developing mobile applications, securely controlling managing access to resources, and supporting managed services and outsourcing options. The IBM white paper **Getting a better grip on mobile devices** describes how you can handle the additional IT workload load of managing mobile devices.

For more information

To learn more about IBM solutions for supporting mobile implementations in the enterprise, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/tivoli

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet every-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce cost. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research. For more information on Tivoli software from IBM, visit: **ibm.com**/tivoli

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
December 2011

Please Recycle

[1] Borg, Andrew, "Mobility Becomes Core IT", The Aberdeen Group, SAP Mobility Insights Webcast Series, Part I, March 29, 2011 http://event.on24.com/event/29/75/81/rt/1/documents/slidepdf/mobile_latest_march_28.pdf

[2] Moerschel, Grant, "Mobile Device Management," InformationWeek Reports, November 2011 http://reports.informationweek.com/abstract/18/8484/Mobility-Wireless/research-mobile-device-management.html

[3] Wingfield, Nick, "Once Wary, Apple Warms Up to Business Market," The New York Times, November 15, 2011 http://www.nytimes.com/2011/11/16/technology/businesses-too-have-eyes-for-ipads-and-iphones.html?_r=1&hpw

TIW14132-USEN-00