Tablets and Smartphones in the Enterprise

The BYOD craze provides IT the opportunity to deliver new applications, improve efficiency and even save money. Still, there are important management and security challenges to consider.
Controlling the Craze

What makes the BYOD movement so unlike other significant technology shifts in the workplace is that it’s being brought to work—quite literally—by employees. Bring your own device is the rare trend in which workers are the impetus for a change, rather than the ones adapting to a change presented to them by their employers.

This dynamic puts an organization’s IT staffers in a reactive mode. They’re the ones trying to keep up with changes being foisted on them; they’re the ones trying to keep pace with developments that sometimes feel beyond their control. Policies are instituted and adapted on the fly, often one or two steps behind the latest changes in devices, applications and user behavior.

Indeed, managing smartphones and tablets in the enterprise is no small challenge. For IT administrators, the trick is to understand BYOD, take advantage of the efficiencies it allows, and effectively manage the applications and data being put to work on all those devices.

To make the task less burdensome, this handbook offers some strategic and practical advice. Contributor Dan Sullivan discusses tools that can help minimize BYOD’s risks and offers guidance on formalizing use policies. He also takes a look at specific applications that can help workers with collaboration, productivity, security and remote access. And since all those applications running on employees’ tablets and smartphones need managing, IT consultant Lisa Phifer looks at systems that allow an enterprise to control and automate app usage.

Phil Sweeney
Managing editor
The BYOD Trend

The combination of easy-to-use applications, ready access to the Internet and large numbers of Web- and cloud-based applications make smartphones and tablets logical choices for many employees. Unlike other elements of IT infrastructure, however, end-user adoption has largely driven the use of mobile devices, not centralized IT planning. To compound the challenge, many of the infrastructure management tools that enterprises have in place were not designed to accommodate mobile devices.

An enterprise supporting mobile devices needs to consider several risks and management concerns, including deployment, application testing, security and governance issues, particularly with bring your own device (BYOD) policies.

Deployment. In cases where businesses provide mobile devices to employees, IT departments have to activate, configure and install applications on each device. Since many of these devices were designed for consumer use, they may have apps for a single person to configure a single device. This is more akin to setting up iTunes on an iPad than to an enterprise provisioning application.

At one time, Research In Motion Ltd.’s BlackBerry devices were unusual in their level of enterprise support, but that has changed. Apple, for example, now offers the Apple Configurator for basic iOS device management, while Exchange Active Sync offers some mobile device management features for Windows 8 phones.

If you plan to support a large number of devices, consider using a mobile device management (MDM) application, which enables large-scale
provisioning, configuring and monitoring of mobile devices. When selecting an MDM system, remember that you may need to support multiple mobile device platforms, such as Android, BlackBerry, iOS and Windows.

A mobile device deployment may also require changes to enterprise applications. You may need to update Microsoft Exchange ActiveSync policies or add an MDM app that works with ActiveSync. For example, ActiveSync can be used to remotely wipe a device, which resets the device to factory-default settings. Add-on MDM apps can enable selective wiping of data while leaving other data intact.

- **Application testing.** Web applications that work well on desktop computers are not necessarily suited for mobile device use. In addition to testing for browser compatibility, you’ll want to evaluate usability on mobile devices’ smaller screens.

  Look for new features prompted by mobile devices. Microsoft Office 365, for instance, includes cloud sync so changes on one device are pushed to versions of the document on other devices.

  Test the performance of apps over Wi-Fi and cellular networks, which may be significantly slower. The results from such testing can help support a decision to revise service-level agreements.

- **Security.** With large-scale use of mobile devices, security is one of the most important concerns. If a mobile device is lost or stolen, it can result in the loss of private or confidential information. It’s easy to block employees who have been terminated from using enterprise-controlled devices, but what about the data on their smartphones? Security measures you can use include Secure Sockets Layer (SSL) certificates, full-disk encryption, desktop virtualization and remote wiping of devices.

  SSL certificates should be installed on mobile devices when your organization needs to authenticate client devices accessing its applications. In the past, SSL certificates authenticated servers so that end users had some assurance they were using legitimate websites. Today, it is just as important for
businesses to ensure that mobile devices have been authenticated to mitigate the risk of access from unauthorized devices.

Full-disk encryption is one way to reduce the risk of data loss. A potential drawback is that some mobile applications may not work on fully encrypted devices. This can be especially problematic when employees use their personal devices for business.

Remote wiping can make device data inaccessible. Employees should understand what remote wiping does to a device and under what circumstances it would be used. As with full-disk encryption, this can become a particularly difficult issue when employee-owned devices are involved. When evaluating mobile device management applications, consider if they allow you to perform selective wipes that erase confidential information without the collateral damage of a full device wipe.

Desktop virtualization systems provide access to centrally managed and stored desktop applications and data. Users can run virtual desktops on mobile devices without the risks associated with downloading confidential data to these devices or having to install applications locally, except for the virtual desktop client.

Mobile devices are an increasingly important component of IT infrastructure. MDM systems complement existing IT management systems and support a range of operations, including deployment, monitoring and remote wiping. Web applications should be tested on mobile devices to identify which apps can be supported on mobile device browsers and which ones can be better supported using a virtualized desktop.

Allowing employees to use their personal mobile devices for work-related tasks can provide plenty of advantages: less laptop lugging, easier connectivity and potentially better interfaces. It can also help a company’s bottom line if the company doesn’t have to pay for smartphones, tablets and data plans. But there are risks with bring your own device practices, including security vulnerabilities, support costs and potential liability issues. Businesses that allow for BYOD should have well-defined policies and mechanisms to enforce them.
Defining BYOD policies. The first step in developing a set of BYOD policies is to define the scope of control the business expects to maintain over employee-owned devices.

At one end of the spectrum, a business could treat devices as if they were corporate assets in return for allowing employees access to IT resources from their personal devices.

The other extreme is to assume no control over the devices themselves and instead focus on access controls and limiting risks such as leaving corporate data on BYOD devices. The optimal policy may lie somewhere between these two poles.

BYOD policies should address acceptable use of corporate IT resources on mobile devices; minimal security controls on the device; the need for company-provided components, such as SSL certificates for device authentication; and the rights of the business to alter the device, such as to remotely wipe a lost or stolen device.

Acceptable-use policies could require the use of a virtual private network when accessing corporate systems and prohibit the storage of passwords to business applications. Security controls might also require encryption of stored data, protection of device passwords and registration of devices with an MDM system. Employees should be informed of all BYOD policies and agree to them.

Written policies and employee consent are not enough to protect a company’s information assets. Even well-intentioned employees can make mistakes, such as forgetting to set a device password or downloading confidential information over an unencrypted session. Mobile device policies should have an enforcement mechanism to ensure that they are applied consistently.

Enforcing BYOD policies. Chances are that some of your company’s existing applications can enforce BYOD policies. But before you try to use these apps, consider two key questions: “Are these applications sufficient to meet all enforcement requirements?” and “How difficult is it to manage mobile devices with these applications?”
Consider the widely used ActiveSync. It provides for policy enforcement, but mobile device manufacturers have not always supported all ActiveSync enforcement mechanisms.

Microsoft has established an ActiveSync logo program to encourage standard criteria for a minimum level of policy enforcement. Qualified devices must support automatic discovery, remote wipe, required password, minimum password length, timeout without user input and a maximum number of failed attempts, among other things. If enforcement mechanisms are sufficient and your employees are using supported devices, ActiveSync could address your needs.

Third-party mobile device management applications can support a wide array of policy enforcement operations, including full lifecycle management, app inventory control, data protection, certificate distribution, device configuration and lockdown.

Policy enforcement begins with provisioning. MDM apps can help ensure consistent configuration of devices, install applications and create accounts on self-service management portals. If your policies limit the apps that can be deployed on a BYOD device, use an MDM system that can detect unauthorized apps.

Most MDM applications support remote wiping, but completely wiping a device is drastic and, in many cases, may not be necessary. MDMs can selectively wipe data, allowing device administrators to delete corporate data while leaving personal data intact.

Your policy may require all devices accessing corporate systems to be registered with your IT department and configured with an SSL certificate for authentication. MDM apps that support certificate distribution can minimize management headaches for this operation. MDM systems can further ease the burden by reporting on expired certificates, revoked certificates and other certificate management concerns.

Finally, look for MDM apps to provide device configuration and lockdown functions. For some users, you may wish to lock down cameras, Bluetooth, GPS and Wi-Fi. If you specify an encryption policy, investigate an MDM that
can enforce this policy on both fixed storage and Secure Digital cards.

Good BYOD policies share two characteristics: They are clearly defined, and they are enforced. BYOD policies should address acceptable use, security controls and the rights of the business to alter the device. Existing enterprise applications, such as Microsoft Exchange ActiveSync and certificate management systems, may be sufficient for enforcing policies. If you require more control over devices and the ability to generate management reports about BYOD use, an MDM system may be a better option.

BYOD is a change for the way many enterprises operate. It requires businesses and employees to accommodate one another’s needs and expectations. When this accommodation is done well, both parties benefit. Let’s look at BYOD in terms of the changing nature of IT control, as well as tips on adopting BYOD policies and practices.

The changing nature of IT control. A common scenario has been for the business to own the infrastructure, the end-user devices and the applications used for business operations. These systems were used almost exclusively for business purposes, with occasional and generally insignificant personal use. An organization set acceptable-use and security policies focused on its best interests.

Today, these same organizations face an emerging management model that must account for more contracted resources, such as public clouds and other service providers, as well as more use of employee-owned devices. The result is a mixture of business-owned, business-contracted and employee-owned devices that requires more consensus on policies and practices than in the past.

At first, it might seem as though businesses are losing control, but that’s hardly the case. Businesses may have less direct control over devices, but they have not lost control over what matters most: data and applications. If a server were stolen, it might cost a business several thousand dollars; if a server with confidential data or intellectual property were stolen, it might cost the same company hundreds of thousands or even millions of dollars.
The advent of cloud computing and BYOD highlights the fact that the most valuable IT assets are not devices but the data and applications that are stored and run on them. Businesses should implement BYOD policies and practices that protect those valued assets.

**Benefits and risks of BYOD.** Both employees and businesses can benefit from BYOD. Employees can consolidate hardware, have improved connectivity, and work with more user-friendly and functional interfaces than were available with some corporate applications. Enterprises can benefit from potentially lower hardware and support costs as well as improved employee productivity.

Risks include security breaches, unanticipated legal liabilities arising from questions of data security and control, and higher support costs. The details of a mobile device implementation will affect these support costs.

**Tips on accommodating BYOD.** To minimize potential drawbacks and manage employee expectations, focus on three tasks prior to widespread BYOD adoption: defining policies, implementing a policy enforcement mechanism, and evaluating mobile device apps and enterprise applications that you intend to support.

Define policies, including those that address acceptable use of business applications and assets on mobile devices. You should also specify the minimum security controls that must be in place to use business systems with a mobile device and the rights of the business to alter mobile devices, such as remotely wiping them if needed.

BYOD and related security policies must be enforced. Existing IT systems may be able to support some levels of compliance; for example, some policies can be enforced through Microsoft Exchange ActiveSync.

More comprehensive policy enforcement will likely require a mobile device management system. An MDM should support provisioning, monitoring, policy enforcement and, if required, some degree of device controls such as disabling Bluetooth.
The BYOD Trend

Evaluate the enterprise applications you expect to support on mobile devices. Identify the minimal form-factor requirements, such as screen size, resolution and data transfer speeds.

Also, consider if the Web applications will be delivered to mobile devices through an existing Web interface or through a specialized app. Software vendors may have apps for their products. In the case of popular enterprise applications, such as Microsoft SharePoint, third-party software developers may be able to meet your needs.

One way to minimize risks during evaluation is to begin with testing in the IT lab, followed by small pilots. If these tests are successful, you can roll out support incrementally. This approach can reduce the risk of scalability problems affecting a large number of users.

The goal of IT support for BYOD is to integrate employee-owned mobile devices into the business in a way that complements the existing IT infrastructure and applications without compromising the security or functionality of corporate resources. —Dan Sullivan
Device-Friendly Applications

Now that your smartphone is also your camera, calendar and garage-door opener, it should be no surprise that there is a wide array of business applications for mobile devices. Mobile devices have the processing power and the storage to support productivity, collaboration and remote desktop access programs. The products mentioned here are representative of the mobile apps available on the market, but this list is by no means comprehensive.

The apps are grouped into six categories: productivity, collaboration, remote access, security, social networking, and news and information.

- **Productivity.** Tablets may not replace laptops in most business-use cases, but there is plenty of overlap in what they both can do. For essential word processing, presentation and spreadsheet functionality, look to Apple’s Pages, Keynote and Numbers for iPad users. For Android users, Documents To Go by DataViz and Quickoffice Pro from Mobile Systems are two suites in this category.

  If you need a quick diagram, process flow or website wireframe, turn to apps like Omni Group’s OmniGraffle for the iPad and SillyCube’s Smart Diagram Pro for the Android platform. When you need to read and annotate PDF documents, try Yuri Selukoff’s GoodReader for the iPad and Unidocs Inc.’s ezPDF Reader for Android devices.

  If you need access to an enterprise application, there is a good chance you can find an app. For example, you can review business intelligence reports using SAP’s BusinessObjects Explorer for the iPad, MicroStrategy Inc.’s Mobile Intelligence for Android and iPad, as well as Penthao’s Mobile BI.
Collaboration. No worker is an island, so collaboration systems are essential to employees’ day-to-day activities. For example, a good file-sharing tool can let employees stop using email for sharing files. Dropbox and Box.net file-sharing services have clients for the iPad and Android. Security concerns about consumer file-sharing services are prompting some businesses to turn to more enterprise-focused file-sharing services such as Synplicity. For SharePoint users, SouthLabs SharePoint Mobile Client for iPad and SharePlus–SharePoint Client for Android bring calendars, documents and task lists to mobile devices.

Remote access. Even with the advanced functionality of today’s tablets and smartphones, sometimes you need access to a full workstation or server. Two widely used protocols are Remote Desktop Protocol (RDP) for Windows and Virtual Network Computing (VNC) for Unix and Linux.

   Wyse Technology Inc. offers PocketCloud Remote RDP/VNC for access to Windows or Mac OS from the Android and iPad/iPhone platforms. RealVNC Ltd.’s VNCViewer for Android provides remote access to Mac OS X, Windows or Linux servers running VNC-compatible server software. When you need access to a command line, Better Terminal Emulator from Magic-AndroidApps can bring a Linux terminal to your mobile device.

Security. Mobile devices need security controls, but they can also improve the security of other systems. Antivirus software is not always welcome on mobile devices because of the extra load on the processor and battery. If you decide to use antivirus protection on your mobile devices, you have several options. Major security vendors such as McAfee, Kaspersky and Norton have mobile products. Some offer features not available on desktop versions, such as functions to block unwanted calls and Short Message Service messages, remotely disable a device, and locate a device on Google Maps.

   Smartphones can eliminate the need to carry a secure token for generating one-time passwords. Products such as RSA SecurID now offer software versions of their tokens that run on Android devices and iPhones.
Smartphones might also help eliminate the unsecure practice of writing passwords down and leaving them in obvious places. Password manager apps like mSeven Software LLC’s mSecure-Password Manager, Ilium Software Inc.’s e-Wallet, and Acendo Inc.’s DataVault and Password Manager all enable phones to store passwords.

- **Social networking.** Social networking is an important business tool, and many mobile devices are designed to make the most of it. Of course, there are mobile apps for all the usual suspects: Facebook, Google+, LinkedIn and Twitter. Basic clients are available for free for the most popular services, and more feature-rich clients, such as Tweetbot by Tapbots and MyPad+ for Facebook and Twitter from Loytr Inc., are available as well.

- **News and information.** Keeping up with changes in markets and technology requires access to a variety of information sources. Zite and Flipboard are personalized magazines for the iPhone and iPad, as is Pulse, which is available on both Android and iOS platforms.

  The Kindle app for iPhone, iPad and Android provides access to Amazon.com’s selection of e-books. Audible Inc.’s free Audible app turns a device into an audiobook device. If you just want to borrow a book, try OverDrive Media’s Console to get e-books and audiobooks from your library.

  —Dan Sullivan
Those Apps Need Managing, Too

**Mobile device management** enables business use of employee-owned smartphones and tablets, but managing devices is just the start. To truly take advantage of enterprise mobility, add a mobile application management tool.

Products that deliver a wide range of capabilities can blur the boundaries between device and application management. Mobile device management (MDM) is for enrolling devices, inventorying assets, configuring settings, tracking use and ensuring policy compliance. Mobile application management (MAM) is for presenting application catalogs, distributing and updating software over the air, inventorying installed applications, configuring application settings and reporting on application use.

Some products include both MDM and MAM, such as those from AirWatch, Fiberlink and MobileIron. Other vendors deliver standalone MAM tools. And some vendors sell standalone products and MDM bundles, which complicates the landscape even further. But don’t let these “you say po-TAY-to; I say po-TAH-to” arguments distract you from the fundamental difference: MDM lets IT administer an entire device, while MAM focuses on applications.

Employers that embrace BYOD by enrolling and configuring devices have addressed fundamental concerns. By taking these basic steps, employers may safely permit employee devices to access corporate email or Web portals. But employees want to do more work with their smartphones and tablets, and employers should want that, too. These powerful, well-connected computers have the CPU, storage and displays to run real business applications. Tapping this potential is where mobile application management comes in.

For starters, MAM tools can help employers manage business use of public
applications downloaded from the Apple App Store and Google Play. They can also present a list of mandatory or recommended apps to each user, inventory the apps installed on a device and identify those that are missing. (For example, any salesperson carrying an iPhone might need the iOS version of the Salesforce Mobile app.) With iOS apps, employers may purchase license keys from Apple’s Volume Purchase Program and distribute those keys via MAM.

Over time, MAM tools can alert users to new apps or to new versions of existing apps. Although they can’t remove user-installed public apps, MAM tools can work with MDM products to respond to noncompliance with policies. Together, MAM and MDM can change a device’s settings to prevent network or corporate email access.

These basic MAM capabilities can help put users’ devices to better use. Employers may insist that all devices have mandatory mobile security measures, such as virtual private network clients, anti-malware, secure browsers and virtual desktop clients. Using MAM to automate app installation and updates can reduce the costs associated with letting the help desk troubleshoot incorrectly configured or poorly written public apps. And taking advantage of Apple’s Volume Purchase Program can help you avoid the paperwork and expense of app purchase reimbursement.

Many employers will no doubt stop with public apps on users’ personal devices, at least for now. But mobile application management can also play an instrumental role in developing and deploying in-house enterprise apps.

MAM tools can push Android .apk and iOS .ipa files to smartphones and tablets. For Android devices, packages may be associated with public or private apps, and anyone can develop and sign them. For iOS devices, apps are limited to enterprise apps, developed by or for the employer and signed using an Apple-issued certificate.

MAM may also push the credential, profile and data files required for installed apps to operate properly. For example, every iOS enterprise app is paired with a provisioning profile that must be present for the app to execute.

Whenever you release an update to an enterprise app, MAM tools can
inventory all devices to identify which ones are running old software and then initiate silent over-the-air updates to those devices. Some products support policy-driven updates, such as updating only when a device is connected to Wi-Fi.

MAM technology may also be useful when it comes to monitoring enterprise apps because the software can collect usage, performance and error metrics and use them to support analytics. This kind of data can help employers refine enterprise apps to increase productivity, reduce support costs and target future app-development efforts.

Finally, MAM can help disable enterprise apps on noncompliant devices, former employees’ devices, devices that are being retired, and lost or stolen devices. For example, when a previously enrolled iOS device is removed from management control, all enterprise apps installed on that iPhone or iPad are automatically disabled.

Studies show that organizations are really just getting started with developing their own private apps. Expect MAM tools to increase in importance as enterprise app use grows. Some products are more tightly integrated with enterprise app development, providing app storage, version control and test support, for example. And while MAM tools often support multiple mobile platforms, many differences exist.

Ultimately, some employers may prefer to manage a few applications on employees’ devices, but not the entire device. If your mobility initiative hasn’t yet touched on MAM, it’s probably time to start considering how it fits into your plan. —Lisa Phifer
DAN SULLIVAN, M.S., is an author, systems architect and consultant with over 20 years of IT experience with engagements in advanced analytics, systems architecture, database design, enterprise security and business intelligence.

LISA PHIFER owns Core Competence Inc., a consulting firm specializing in business use of emerging Internet technologies. Lisa has been involved in the design, implementation and evaluation of internetworking, security and management products for 30 years.