WHITE PAPER

CDW PEOPLE WHO GET IT

MASTERING MOBILITY IN A BYOD WORLD

Integrating mobile devices into today's enterprise infrastructures offers challenges and rewards.

Executive Summary

Mobility has evolved rapidly from a nice-to-have amenity to a core productivity requirement for today's information-driven organizations. The use of smartphones and tablet devices, in particular, has exploded as employees embrace anytime, anywhere access to voice, email, web content and applications.

This booming mobile device market presents both opportunities and challenges for today's IT decision-makers. On one hand, the pervasiveness of mobile devices and the increasing richness of their technical capabilities create tremendous opportunities for organizations to increase employee productivity, streamline workflows and improve collaboration. On the other hand, a number of new challenges lie ahead, particularly when it comes to IT management, security and governance.

TWEET THIS!

Table of Contents

The bring-your-own-device (BYOD) trend makes these challenges especially complex. Instead of issuing a single, standard mobile device to every worker and maintaining complete administrative control over that device, most IT departments must manage the myriad mobile devices that workers buy on their own — and use for personal purposes, as well as for work.

IT management at every organization must therefore develop sound strategies for successfully integrating mobile devices into their work processes, and also mitigate the risks associated with allowing workers to use these devices to access sensitive data and applications.

That can be a tough job, so IT leaders are likely to look for assistance from qualified partners with best-practice expertise and the contract services they need to achieve their mobility goals quickly and efficiently. More specifically, organizations that want to succeed at mobility should seek assistance in four key areas:

- Mobile devices
- Platforms
- Applications
- Operations and support

By getting the help they need in each of these areas, IT management can ensure that their organizations reap the substantial benefits offered by mobility.

Mobile Devices: Practical Procurement

The first challenge any organization confronts when crafting a mobility strategy is deciding which specific devices make the most sense for its needs. Devices vary significantly in their capabilities, costs and compatibility, and users have varying requirements when it comes to attributes such as display size, keyboard or battery life. These parameters must be factored in when deciding on an appropriate mix of mobile devices.

Onboarding

Once an organization decides which devices and carriers to use, the next step is to assign these devices and carriers to employees. At this point, the right mobility partner can offer substantial value by providing a complete, well-managed onboarding program that will perform the following tasks:

Device upgrades and number porting: An onboarding service can handle any upgrades of existing worker devices included on the mobile plan list. Upgrades may already be provided for within employees' existing carrier contracts.

Accessory selection: Depending on work requirements and personal preferences, users may also need wall and car chargers, headsets, cases, keyboards, batteries and other extras, in addition to their mobile device. A selection of appropriate accessories should accompany any device upgrade.

Configuration, delivery and activation: Once devices, carriers and accessories are specified for each mobile program participant, the onboarding service provider will execute all associated procurement orders, including appropriate device configuration, accessory packaging and confirmed delivery. The service provider also will ensure employees take any actions required for proper activation of their devices.

MDM administration: An integral component to any onboarding service is the inclusion of all new devices — along with role-appropriate security authorizations — in the organization's mobile device management (MDM) platform. In many cases, the same mobility partner that provides the onboarding service will also be responsible for MDM operations (See *Mobile Platforms* section).

Ongoing Support

As part of a managed program, a mobility partner can help organizations ensure that devices in the field are promptly and properly serviced to guarantee continued employee productivity. Key aspects of this support include the following:

Warranty management: Warranty coverage should be tracked for all devices, and extended or enhanced coverage should be purchased and tracked as appropriate.

Device replacement: Over time, mobile devices will need to be replaced, either temporarily or permanently depending on the nature of the problem. In addition to replacing devices, a service provider will perform device authentication and authorization tasks, including deauthentication and deauthorization of any devices issued temporarily.

Advanced exchange "depot" services: A service partner can further support worker productivity through depot services that allow users to exchange disabled devices for working ones more quickly and easily than through traditional carriers, which often force users to visit inconveniently located offices or wait several days for a replacement device to be shipped.

End-of-life Device Retirement

Organizations also need processes that ensure the secure retirement of mobile devices at the end of their useful life. Policies and practices must address both device deauthorization and the removal of any sensitive data housed in the device's memory.

There are several reasons why an organization would choose to engage with a service provider to assist with such tasks, which are complex and require specialized technical knowledge. Authorized service providers transact much more business with mobile carriers than most individual organizations, leading to closer working relationships.

As a result, organizations will find that the right service partner can ensure the success of their mobility program while also

driving down costs. Signing on with an experienced partner also helps organizations gain the benefits of mobility without placing an excessive burden on limited internal IT resources.

Where Does BYOD Fit In?

Does BYOD fit into the organization's mobility strategy? Ideally, that would be a good question to ask around the time that the broader mobility plan is coming together. More likely, BYOD becomes an issue that organizations are forced to address after the fact, as workers inevitably bring their personal devices into the workplace. BYOD does not mean "bring any device in the known universe, and we will support it." But BYOD offers a way to achieve a win-win for organizations and workers.

Employees win by not having to carry two devices (one for personal use, one for work) and by possibly having some of the costs of their devices subsidized by their employer. Organizations win by having their staff defray some of the costs they would typically allocate toward mobile devices and by gaining greater employee productivity. Workers are more efficient (and more likely to address work-related issues outside of traditional work hours) when they use their personal mobile device for their job.

Organizations invariably must place limits on the mobile devices they support under their BYOD programs. It is simply impractical to support every device available. Instead, it makes sense to define a set of BYOD-approved devices that balance choice for employees with technical practicality for the IT department. Approved device options can be covered in the organization's BYOD policy (see *Writing Sound BYOD Policies* sidebar).

Writing Sound BYOD Policies

BYOD success isn't just a matter of implementing the right mobile technology. It also requires smart policies and clear communication with workers. After all, the inclusion of employee-owned devices in an organization's IT environment is a very new phenomenon, and it therefore requires both parties to consider and agree upon a variety of points.

The right mobility partner can contribute a wealth of insight and experience into the formulation of an organization's BYOD policies. For example, employees store all kinds of personal content, such as phone numbers and photos, on their mobile devices. But in the event that their device is lost or stolen, an organization may need to immediately wipe all content from the device. Workers need to understand this in advance — and probably agree to it in writing.

In some cases, of course, it may be possible to segregate personal content from work-related content using techniques such as "sandboxing." However, in the event of a lawsuit, an organization might still have to seize an employee's device in order to fulfill legal discovery requirements. Again, this is something that should be made clear as part of an explicitly communicated BYOD policy.

Some organizations have even found that BYOD programs affect their collective bargaining agreements with labor unions. For example, the use of a smartphone to check email after hours can technically be considered overtime. In such circumstances, organizations need to protect themselves either by prohibiting after-hours use of the device or by gaining an exemption for BYOD in their employment contracts.

Platforms: Management and Security

After choosing and procuring mobile devices for a mobility program, organizations must manage and secure those devices diligently — along with all interactions between the devices and the organization's IT resources. Doing so protects the organization's systems and information from illicit use, while ensuring the full benefits of mobility to the employee.

To fulfill these requirements, service providers typically use mobile device management technology, which offers a variety of capabilities:

Automated enrollment: MDM platforms can be configured to automate enrollment of new devices by authenticating and registering them as belonging to a particular employee — either through a mobility portal or via text or email messages. The MDM platform will validate the configuration of the device so that it can be supported properly, and also may automatically present an acceptable-use policy that requires sign-off from the worker before fully activating access.

Automated security: A properly configured MDM platform will safeguard IT security by enforcing authentication and encryption controls, as well as application and content access restrictions. Service partners also can set up the MDM platform to detect and neutralize mobile devices that may have been compromised by common exploits such as "rooting" or "jailbreaking."

Perhaps most important, the platform should be able to remotely lock lost or stolen devices and, where appropriate, wipe any sensitive data and files from the device's local memory. This is especially important for smartphones, given how easily they can wind up in the wrong hands.

Automated reporting: A good mobility partner will help keep an organization's program on track by monitoring such things as what devices are being used, how often they are being used and which resources workers are using, among other things. Such reporting can be passed on to IT management via an intuitive dashboard that monitors mobility across

the organization, even among BYOD employees who have received permission to use personal devices.

Because different staff members have different needs — and different roles within the organization — MDM is often used to manage devices according to user roles. For example, outside salespeople who cover large territories can be expected to use devices from many different locations. Headquarters-bound administrative staff, on the other hand, are likely to use their devices over a much smaller area. Role-based MDM tools make it easy to accommodate those differences in mobile behavior.

Service providers can implement MDM platforms internally in an organization's data center, or under a subscription-based, software as a service model. The SaaS model offers several advantages, including avoidance of both capital costs and the ongoing labor of maintaining the system. SaaS also makes it easier to keep MDM software features up to date — an essential benefit, given how quickly mobile technology changes.

Streamlining with a Self-service Mobility Portal

A service partner can significantly improve the reliability and efficiency of an organization's mobility procurement processes (and provide an audit trail) by building and maintaining a self-service mobility portal. Employees use the portal to enter personal information and choose from a list of approved devices, plans and accessories.

By presenting and capturing this information online, ordering, porting, configuration and shipping requests can be automated. The portal also can be used for lifecycle processes such as order tracking, maintenance requests and subsequent device upgrades.

A well-designed mobility portal provides the following benefits:

Greater control: Through integration with human resources databases and the use of rules-based menu options, mobility portals safeguard enforcement of role-appropriate procurement policies much more reliably than manual procurement processes.

Lower costs: Self-service portals reduce costs by eliminating manual processes and minimizing procurement errors. Workers receive their devices more quickly and can review options and submit requests outside of regular working hours.

Optimized compliance: Mobility portals make it easier to audit provisioning processes. They also enhance compliance by tracking employee assent to mobility and BYOD policies as they relate to security, appropriate use and other regulatory or governance requirements.

Regardless of how MDM is implemented, the right partner can add value by providing experience-based guidance. Most organizations do not have much in-house expertise in areas such as mobile security, acceptable-use policies and optimal mobile device settings. A carefully chosen service provider will bring best-practice expertise to ensure the MDM platform is configured properly to meet an organization's specific requirements.

Applications: Strategies for Employee Productivity

It's not enough to simply get mobile devices into users' hands and make sure those devices are managed properly. Ultimately, employees are productive thanks to the applications they use. An effective strategy must address the issues of application selection, management and development.

Application Selection

Application selection in a traditional IT environment is pretty straightforward. An organization licenses a set of desktop applications, such as Microsoft Word and Microsoft Excel, for personal productivity; and a set of enterprise applications, such as customer relationship management and enterprise resource planning systems, for various workflow processes. The application portfolio is restricted to avoid problematic software support and licensing issues.

When considering BYOD, application selection is a bit different. One issue is that users often have their own favorite apps (or apps that are the default choices of their mobile provider) on their devices. Organizations must decide if these apps are acceptable.

Multiple mobile email clients, for example, can create security and integration challenges. But that must be weighed against user preferences and the feature/function advantages of different email clients.

Another issue is that the mobile app market is evolving rapidly. New apps are constantly emerging that can enhance both individual productivity and team collaboration. Organizations may find it advisable to be a bit more open and nimble than they have been when it comes to introducing new mobile apps to desktop and server software.

These are some steps organizations can take, with the advice of an experienced mobility partner, to make app selection a smooth process:

- Specify a core set of apps that are required or recommended for each type of user.
- License these apps in the aggregate, as appropriate, to minimize cost.
- Establish a process by which users can suggest new apps for broader use across the organization.

The right partner can recommend a set of mobile apps that best fulfills the requirements of various types of users — in terms of functionality, cost, ease of use and interoperability with each other and with existing enterprise systems. In some cases, the partner also can simplify deployment of those applications by managing distribution directly or via SaaS.

Application Management

Once applications are in place on users' mobile devices, they must be managed. This includes configuration and version control, access and content security, encryption management, and asset tracking for license compliance. One way is to monitor all apps residing on the target device, but that may not be practical in a BYOD environment.

For one thing, users may find it intrusive for an employer to monitor apps that are exclusively for personal use. For another, it simply may be too much work to manage the diversity of apps that a large number of users may have on their personal devices.

Another approach is to "containerize" the apps that employees use for work. With this approach, the IT team has visibility into and control over only those apps residing in a virtual "container" or "sandbox" on a user's device.

An advantage is that the number of apps that the IT department must manage is limited — and it is restricted from inappropriate access to personal apps on users' devices. Of course, that also means this team can't help users whose apps cause a problem on their device.

A third approach is to create management containers or "wrappers" for each individual work-related app — a newer (and more complex) approach that provides more granular control over apps.

A mobility partner can help with app management by recommending a solution (or a set of solutions) that best meets an organization's requirements for automation, control, ease of use and cost. In some cases, a partner may be able to provide app management as a turnkey service, thereby relieving IT staff of both the app management workload and the need to ramp up on new app management tools.

Application Development

In some cases, instead of depending on commercially available packaged software, it may be necessary for the organization to develop its own mobile apps. Certain employees, such as field personnel or mobile executives, often need mobile apps that facilitate organization-specific processes.

Essentially, there are three ways to architect a mobile app. One is to create an app that runs on the mobile device's browser. That is the simplest approach, because it allows the app to run on all kinds of devices with little or no modification. Unfortunately, this limits the app's ability to use the native capabilities of the mobile OS or the device itself.

Another approach is to develop an application that runs directly on the device's OS. Native apps run better, can include more features and can more readily utilize device resources such as cameras and GPS data. However, time and money must be invested in porting the app to every supported mobile platform.

A third, hybrid approach complements browser-based capabilities with selective use of native OS functions. OS-specific development is limited to only those areas where it is genuinely necessary. But a great deal of diligence is required in deciding and documenting where in the application code OS-specific calls are made.

Most organizations focus mobile app development efforts on the customers, students, constituents or other outside parties they serve. Such externally focused efforts tend to drive the choice of app development strategies and tools, and internal app development efforts typically piggyback on these. There are cases in which the requirements of an internal app

Windows 8 Devices

The tablet form factor has turned out to be highly appealing to users seeking notebook-like functionality in a device that is as easy to use on the go as a smartphone — and a driving force behind today's BYOD initiatives. The more users embrace the tablet devices and smartphones in their personal lives, the more pressure grows on the IT group to support them as alternative platforms for job-related mobile computing.

The introduction of Microsoft Windows 8 also presents a new opportunity for enterprises to bring greater homogeneity — and, by extension, easier manageability — to their end-user computing architectures. Because it was designed specifically to support touch-screen use, Windows 8 (along with its associated operating systems, Windows RT and Windows Phone 8) is enabling a new breed of tablets, convertible notebooks and smartphones to share core platform services — along with a common look and feel.

As a result, organizations can port applications between different classes of devices more easily, and manage those devices in a more common manner. That can be especially valuable for organizations that have made significant investments in the Windows platform over time and find native Windows clients easier to manage than those running iOS, Droid or other platforms.

That is not to say that BYOD programs are better off automatically limiting themselves to Windows-only devices. But, now that viable Windows-based alternatives are available for all popular device form factors, mobility decision-makers should consider the trade-offs of cost and complexity when choosing their end-user device options.

are sufficiently different and important enough to warrant a distinct set of development tools and techniques.

The right mobility partner can assist in choosing the optimal approach for an organization's requirements, and recommend the right development tools for executing that approach. A partner also can provide the training and support necessary to get the most out of a chosen set of tools. Some partners will even handle some or all of the development work on an outsourced basis – a compelling option for organizations that have limited internal development resources and minimal in-house mobile expertise.

Operations and Support: Uptime, Cost Control and Alignment

In addition to getting devices and apps up and running effectively in the field, organizations may need the assistance of a service partner for several other key aspects of mobility that effect their overall return on investment.

Support and Training

Mobile users require all kinds of support. They may have questions about how to use a feature or application on their smartphone. They may have technical issues related to poor app performance or erratic device behavior. They may need to know how to get their phone fixed or how to temporarily turn on international roaming.

In fact, smartphone and tablet users may have support needs that go well beyond that of desktop and notebook users. That's why organizations must answer a number of questions as they prepare to support mobile users in both BYOD and non-BYOD environments:

- Which issues should be addressed by the organization's help desk, and which should be referred to device manufacturers, carriers, application vendors and other third parties?
- Will users be required to purchase maintenance or support contracts from their suppliers if they want to participate in the BYOD program?
- How will common issues be tracked in order to get at root causes, add FAQ content to web/wiki self-service pages, or proactively educate users?
- What investments must be made in training help desk staff so that issues can be resolved on the first call? What is the escalation process if issues remain unresolved?

Often, an organization is best served by outsourcing its mobile help desk to a service partner with expertise in mobility-related issues. This allows the organization to avoid the considerable investment of time and money required to ramp up internal teams on such specialized subject matter while maintaining a higher level of service than a typical internal help desk can provide.

This is no small consideration, given the lost productivity, delayed workflows and poor customer experiences that can result when mobile users don't get the timely, effective support they need. It's imperative that the mobility team ensures that mobile users get fast, accurate answers to their questions.

Of course, service providers also can help to safeguard user productivity – and drive down long-term support costs – by providing the right training for mobile workers. Training can include everything from brief instructional videos to periodic bulletins on new capabilities and policies, and also may include a mix of both ready-made and custom training content.

IT staff also may need training on a variety of topics – including MDM software, mobile service troubleshooting, and mobile development and porting tools.

83% The number of surveyed organizations that allow BYOD
10% The number of surveyed organizations "fully aware" of all the devices on their networks

Source: *SANS Annual Mobile Security Survey (Aberdeen Group)*

Carrier Costs

Another aspect to consider with BYOD is carrier expense. Many early BYOD adopters offered users a fixed stipend for their work use of carrier voice, text and data services to defray their personal phone bills. For some organizations, that approach still may be appropriate.

But several issues can crop up with fixed stipends:

Determining the right amount: Organizations often lack visibility into their employees' use of carrier services. This makes it difficult to determine exactly what a fair stipend would be. Also, different types of employees have different usage patterns, so stipends must be tailored to different roles.

Higher nonaggregated costs: The consumer rates that carriers charge to individual users are higher than those charged to organizations that aggregate a large volume of minutes and megabytes, meaning that (in almost every case) organizations will save money on carrier costs only if they partially compensate their workers for business use of their personal devices.

Usage disincentives: If staff perceive (rightly or wrongly) that their stipend does not cover their costs, they may become less inclined to use their personal devices for business productivity. That undermines the whole point of BYOD.

Responsiveness to change: Carriers regularly change their rate structures in response to changing market conditions. An individualized, stipend-based approach to carrier contracts makes it difficult for the organization as a whole to take advantage of savings opportunities when they arise –

and forces an organization to continuously re-evaluate its stipend policies.

Payment administration: Disbursement of stipends can create headaches for the finance department, especially in large organizations with high churn rates and multiple classes of users.

An alternative approach is for an organization to retain control over the carrier engagement and utilize a wireless expense management solution to track and control costs. This approach allows the organization to pool minutes and data charges across groups of employees, negotiate for lower rates and better monitor employee behavior in order to make better program decisions. It also can encourage greater use of mobile productivity resources.

Organizations can also mix and match approaches — applying a stipend model to some users and an aggregated model to others.

Here, again, the right partner can provide invaluable expertise in how to make the best decision based on an informed assessment of carrier costs, user behavior, administrative constraints and program objectives.

Ongoing Value Optimization

As with any other technology initiative, mobility programs must be diligently monitored and modified as needed to ensure a maximum return on investment for the organization. Market dynamics, user behavior and organizational requirements change over time. IT decision-makers, therefore, may want to consult with a trusted partner on an ongoing basis to re-evaluate mobility strategies in light of changing realities.

In particular, organizations need to review both costs and benefits. On the cost side, they need to understand the end-to-end costs of delivering mobility services to their staff, including:

- device procurement, configuration (including security) and administrative onboarding;
- ongoing device management, resource access and authentication controls, upgrade/update and maintenance services;
- user support and training, including policy notification and sign-off;
- application design and development (for custom apps) and application licensing (for commercial apps);
- carrier charges, wireless expense management costs, usage stipends and stipend management.

On the plus side, enterprises with well-conceived and well-managed mobility programs can also expect to reap these benefits:

- improved employee productivity;
- increased sales;
- accelerated processes that result in faster responsiveness to customers, constituents, crises and opportunities;
- reduced errors through better access to information resources and improved collaboration and oversight;
- improved employee recruitment and retention.

One of the keys to successful program optimization is to understand the costs and benefits of specific mobility enhancements, rather than for the mobility program as a whole. For example, it would be helpful to get insight into the end-to-end cost basis for a mobile sales application versus simply pricing generic organizationwide email access.

Getting the Big Picture: Advisory Services for Mobility

Because mobility involves so many moving parts, it's easy for organizations to get bogged down in implementation details. Before embarking on a mobility initiative, it may be a good idea to get big-picture advice from an experienced partner that can offer a strategic perspective on how to achieve both near- and long-term success. Such advisory services can include the following:

Strategy and roadmap development: Few organizations have the wherewithal to roll out, all at once, all the mobile capabilities that every worker needs. A knowledgeable partner can help craft a plan that appropriately prioritizes higher-value mobility services first, then adds capabilities in an efficient and logical sequence over time.

Baseline resource assessment: Every organization starts its mobility journey at a different place in terms of systems and network infrastructure, application architecture, security and access controls, and in-house skill sets. The right partner can provide an accurate, objective assessment of this mobility baseline to help understand exactly where it will need to allocate resources in order to ensure the long-term success of its mobility efforts.

Project management: Organizations often consider outsourcing specific components of their mobility initiatives, such as procurement or mobility help desk, to service providers. For many organizations, it also may make sense to outsource management of mobility projects as a whole in order to reduce risk, accelerate time-to-benefit and avoid diversion of internal staff resources away from other critical activities.

By helping organizations perform this kind of granular cost-benefit assessment, mobility service providers make it easier to pinpoint both successes and opportunities for improvement.

The complexity that mobility introduces into the IT equation can be daunting to those responsible for mobility outcomes – especially given the advent of BYOD. But few, if any, organizations can afford to sit on the sidelines.

Smart implementation of mobility has become a necessity for organizations intent on surviving and thriving in today's hyperconnected, get-it-done-now world. That's why every IT manager needs to become an aggressive student of best practices, including how to evaluate mobility-enabling technologies and find the right mobility partners.

CDW: A Mobility Partner That Gets IT

We can help get your staff mobile fast. Because CDW maintains partnerships with leading wireless vendors, including network providers and device manufacturers, we offer a one-stop shop of integrated mobility solutions consisting of software (security and management), hardware devices (smartphones, tablets and notebooks) and cellular wireless activation services.

Regardless of the mobile platform you choose, CDW can step in to help with activation and configuration services. What's more, we can ensure that the apps you want running on workers' wireless devices are installed and configured correctly before they turn them on the first time.

Working with your CIO, management team or IT department, we can design, plan, implement and support comprehensive mobile solutions built around you and your organization's needs.

Contact your CDW account manager or mobile solution architect to discuss the mobile policy checklist. Call 800.800.4239 or visit CDW.com/mobility

MaaS360 by Fiberlink

Fiberlink's unique cloud-based technology and delivery model are the foundation for its Mobility-as-a-Service platform (MaaS). MaaS360 changes the game for how IT manages, views and controls all devices, from desktops and notebooks to smartphones and tablets.

CDW.com

SAP

SAP® Afaria brings its device and application management solution to the cloud, providing a low-cost, high-returns model for deploying comprehensive enterprise mobile strategy. You will get the app management, multi-OS and BYOD flexibility that every organization needs without losing robust on-premises features such as no-touch application management, access to real-time analytics and centralized administration.

CDW.com/sap

BlackBerry

The end-to-end BlackBerry® solution helps workforces meet even the most rigorous expectations – all on a wireless platform that has received security accreditations globally.

The BlackBerry product line includes the award-winning BlackBerry smartphone, software for businesses and accessories. BlackBerry products and services are used by millions of customers around the world to stay connected to the people and content that matter most throughout their day.

CDW.com/blackberry

TWEET THIS!

CDW PEOPLE WHO GET IT