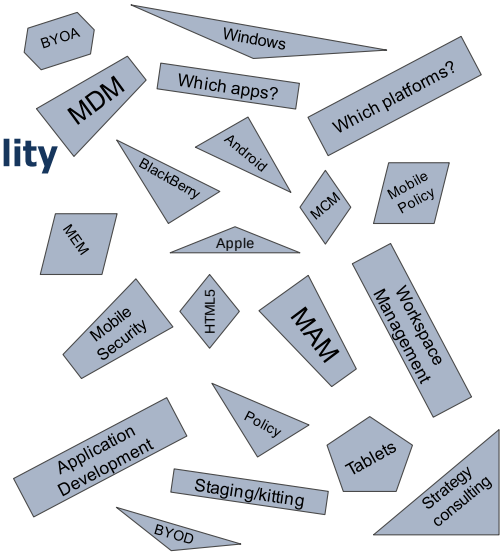
Transforming Your Organization with Mobility

Making Smart Choices in a Noisy Market



Introduction

The world of enterprise mobility enablement is a mess. There are literally hundreds of vendors offering enterprise mobile solutions and support services, and on any given day are announcements of new solutions, new suppliers, and M&A activity. Organizations cannot wait around, hoping this mess will sort itself out; they need to mobilize now to compete in today's market environment.

Adding to the complexity is the fact that mobile solutions are not just the domain of senior executives and sales personnel – the corporate liable crowd. All other employees, also known as the Bring Your Own Device (BYOD) crowd, are finding ways to leverage smartphones and tablets to help them in both work and personal activities. By 2016:

- 92% of all U.S. employees will have a smartphone.
- U.S. and Western European household tablet penetration will exceed 90% and 60%, respectively.

Even employees in developing regions are quickly adopting smart devices; by 2016, 57% of all Asia-Pacific employees will have a smartphone.

Enterprise mobile solutions also need to consider a broader set of stakeholders using mobile services, namely, customers and partners.

Bottom line, enterprise mobility needs to consider use by anyone who impacts organization success to maximize mobility benefits, and limit the risks.

This whitepaper intends to help organizations understand the critical elements of a mobilization solution, the value and interdependencies, and important enablement assessment questions. In addition, this whitepaper will assess the supplier segments that can offer one-stop shop mobilization services. Why is this important? In this highly complex environment, one-stop shop providers can:

- Limit the supplier assessment time.
- Help build a holistic mobility strategy.
- Build and manage mobilization activities.
- Ensure the mobile solution ROI is maximized across internal units, with customers, and over the long term in an ever-changing marketplace.

Enterprise Mobilization Solution Enablement

A holistic enterprise mobility solution requires assessment of approximately nine core elements. Depending on the organization's competitive environment and needs, all elements do not need be executed; however, they do need consideration to ensure that investments in one area can complement and reinforce future mobilization activities.

Mobilization Strategic Planning

Mobilization strategic planning is the first step in creating a holistic enterprise mobility solution and is needed for three reasons. First, mobilization decisions need to be tied to how an organization makes money and keeps customers. By understanding the fundamental value of an organization to the market place, the right processes are mobilized. For instance, a mobile sales force solution could be as simple as a media tablet equipped with a PowerPoint presentation and an expense management application; or as complex as full corporate database integration complete with secure content collaboration. The former can be as simple as selection of the appropriate device and application, while the latter needs to consider an organization's IT and security infrastructure.

Second, enterprise mobile enablement is not just about organizational process assessment and selection, but also about prioritization across stakeholders. For instance, some retail businesses build mobile apps for both their store associates and customers at the same time. This approach ensures a common app format, easing associate and customer interactions as well as maximizing application development and testing resources. Corporate liable employees, such as field sales, field support, and management personnel, may be the first to get mobile access to corporate data; however, all employees need consideration to create a mobile security strategy.

Third, mobile solution and support services are a wild west of vendors, products, and services. The most prudent and fiscally responsible step is to prioritize organization process and employee mobilization activities before selecting solutions or engaging the vendor community.

Mobile Policy Development

Mobile policy is the creation and assignment of rules governing mobile and corporate asset and data use. Assignment is typically to an individual, group, organizational unit, or device; several sources influence rules development, but, in large part, are defined by an organization's security requirements, which, many times, were needed to ensure compliance with an industry's rules and regulations. HIPAA is an example of healthcare regulations governing digitized patient medical records.

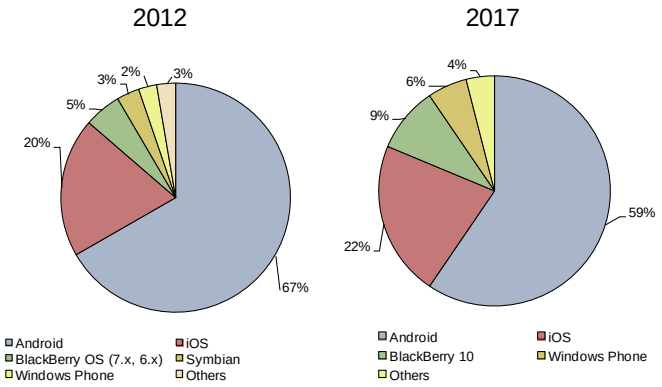
Mobile policy development is an ongoing activity that begins with a mobile strategy and continues throughout the mobile solution enablement process. Starting early with its development is critical because mobile policy governance is only as good as the tools selected for mobile solution enablement, including devices, apps, network connections, and supporting services.

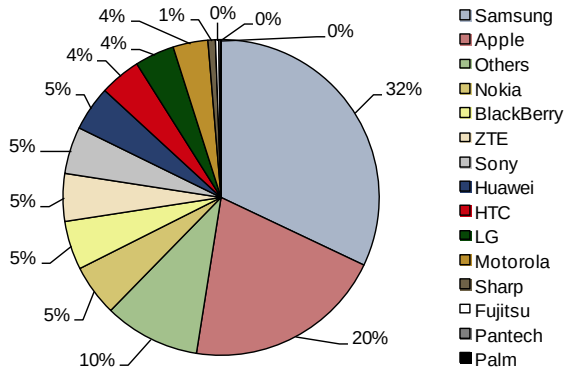
Device and Accessory Selection

Today, the mobile device market is highly fragmented on a number of levels and is not showing any signs of consolidating. First, employees are expanding the number of mobile devices used for workplace activities to include both smartphones and tablets. Smartphones offer portable access to voice and data services; tablets are the bigger screen, instant-on mobile device with greater portability than laptops. Second, smart device form factors are still evolving. This is most notable in device screen sizes, with smartphone screen sizes varying between 4 and 6 inches and tablet screen sizes varying between 7 and 10 inches. Screen size choice depends on a user's needs and use case and the market is still expanding and evolving in both of these areas.

Third, the device OS and OEM market is highly fragmented. For smartphones, there are over 8 OSes and 30 OEMs, with over 20 OEMs offering Android devices. For tablets, there are 5 OSes and over 20 OEMs. This

complex ecosystem is not expected to consolidate. The charts below for worldwide smartphone shipments provide supporting statistics.





Organizations could eliminate the complexity created by a highly fragmented mobile device market by simply setting restrictions on what devices an employee can use during work hours, on company premises, or when connected to corporate systems. For some industries and for some employee groups, this has to be done. However, organizations have generally placed few, if any, restrictions on mobile device type and use in the workplace for several reasons.

First, organizations save money if they allow an employee to use their own device, rather than purchase a device for them. Second, many choices are available by device platform for apps, support and management tools, and mobile solution security. Given these choices why would an organization be pigeonholed to a few vendors or platforms? Third, given the many options for constructing mobile solutions, it is inherently difficult to set rules that limit device options. Fourth, the vast ecosystem of mobile developers has shown how innovation is best left to the community of users versus controlled by device OEMs or mobile operators. As a result, organizations are more open to letting employees find new ways to use their own mobile devices, apps, and services to improve their productivity and balance work and personal life activities.

Adding to the complexity of the mobile device environment, but also enhancing device usability are accessories. For instance, retail tablets considered fragile and awkward for delivery drivers become workforce solutions by wrapping them in a protective case and adding a hand strap. Today, the accessory vendor market is dominated by consumer accessories; however, even for pragmatic accessories many vendor options exist.

In summary, the phenomena of BYOD and the multi-device employee are here to stay. Organizations should not think about controlling the device environment, but instead taking advantage of a mobile-equipped workforce using device-agnostic mobile solutions.

Connectivity Services

A perception exists that device connectivity is simply an operator service plan, but, in actuality, connectivity choice has broad implications based on location, application used, and costs, such as:

- Wi-Fi may be the obvious choice for a video conference call, but a remote worker may not have access to Wi-Fi in a building.
- Some organizations need Push-To-Talk (PTT) connections, but not all operators have PTT services or the same coverage.
- Rate plans now offer more options for pooling connections over multiple workers and multiple devices under a single plan.
- Some operators have begun offering plans allowing organizations to combine machine-to-machine (M2M) connections and employee connections on a single rate plan.
- Moving forward, mobile networks are becoming smarter, allowing for customizable access services paid on-demand. Such services could provide

greater speed and capacity for a mobile video connection or to ensure mobile financial transactions are given network priority.

Organizations who understand the full breadth of options for connectivity can make better choices around the device and application selection, which ultimately affects cost and worker benefits.

Mobile Application Development and Systems Integration

Mobile application development has seen tremendous innovation over the past several years. Previously mobile application development required building a native application for a particular smartphone OS. This was expensive, time consuming, and limited device choice. Over the last 2 to 3 years, application development platforms have been built that allow writing an application once and deploying it across several OS platforms and device types. For some platforms, the application can be written using standard web development languages, allowing companies to employ their own web developers instead of hiring dedicated mobile OS developers.

While this may sound like Nirvana, the challenge is selecting the right platform. Platforms that rely on web languages can be limited in app functionality, device feature use, and security. Other platforms leverage less known programming languages, requiring more extensive training. Others allow creating highly functional apps, but require developers skilled in multiple languages from native languages to web.

HTML5 has been getting lots of press as the device-agnostic platform for building mobile apps since the browser serves as the common platform on which to build the app from web programming languages. However, it is an evolving standard that will take many years before it can produce as functionally rich and secure an app as written in the native device OS. On the other hand, some enterprise apps do not need to be highly complex. The message is that organizations have lots of choice but which tools, platforms, and providers should they choose?

Mobile apps become highly relevant for the enterprise when they can connect and access an organization's databases and systems. Most mobile apps and app platforms allow enterprise connectivity using web services, which is a simple, proven integration service. However, for security and other reasons, enterprises may want a custom integration that can include traversal of multiple firewalls and directory services authentication before connection to corporate data. Regardless of system integration activities, organizations need to consider mobile app development and system integration as a single element to facilitate the best worker experience, but also address cost and security requirements.

Application development and systems integration is one of the most critical elements of a mobilization strategy. Thorough assessment and selection in these areas ensure that workers are equipped with the right apps to optimize the use of another important organizational asset – its data.

M "X" M Puzzle

The area of enterprise mobilization services that has exponentially increased the complexity over an already complex environment is Mobile "X" Management where the "X" can stand for various terms defined by their target use case, or as a term that simplifies a mobility supplier's services. M"X"M services are focused almost entirely on supporting a mobilized employee; the first M"X"M term that spawned all others is mobile device management (MDM).

Mobile Device Management

MDM has become an umbrella term for all enterprise mobility management services. However, strictly speaking, MDM applies to managing device hardware functionality and some software management. The hardware functionality management includes turning on or off any feature, such as a camera, Wi-Fi radio, Bluetooth radio, and GPS. It can also include turning device encryption on and off. Software management functionality is less sophisticated and typically involves setting and changing passwords, whitelisting and blacklisting apps, and removing or downloading apps.

These are all important services, but one of the biggest benefits of MDM services is establishing an inventory of devices and its contents allowing execution of mobile policy. MDM platforms that integrate with

Lightweight Directory Access Protocol (LDAP) or Microsoft's Active Directory services strengthen mobile policy execution by linking an employee's mobile device(s) footprint to their corporate credentials.

Mobile Application Management

Mobile application management (MAM) is a broad term for services that control the use and access to mobile applications as well as control app modifications. At one level, it provides control of both internally developed and retail mobile applications typically enabled using an enterprise application store. Enterprise app stores allow IT administrators to control app distribution based on employee work profiles and needs. On another level, MAM applies to updating internally developed apps with new features and functionality. Updates can be complete removal and replacement, but can also mean adjustments to existing applications.

MAM services need to be considered along-side mobile application development platforms, as the development platform can be used to update and modify the app. This is an area where organizations need to have a broader view of their application needs across the organization and in the long term. Leveraging the right vendor(s) can consolidate sources for application development and management.

Mobile Expense Management

Mobile expense management (MEM) comes under the umbrella term of telecom expense management (TEM), which is the control of costs related to organization telecom services. TEM can cover not only mobile expenses, but also landline voice and data service costs. Regardless of the service, TEM services are needed when telecom vendor services have little central visibility and are not cost optimized. This is especially apparent in the mobile space when individual business units or government organizations are paying for employee voice and data services using different mobile operators, rather than consolidation to one or two mobile operators and purchasing access using shared voice and data plans. MEM is also valued because it can detect and stop unauthorized and very expensive international mobile roaming.

Enterprise Mobility Management

The importance of understanding MDM, MAM, and MEM/TEM is not only for their contribution to a mobility solution, but also because they designate supplier segments that have expanded their solution sets with MDM, MAM, and other M"X"M services to provide a more holistic set of support services. This expanded set is more aptly defined as enterprise mobility management services.

MDM vendors have been the most aggressive with solution set expansion, adding services like MAM, mobile content management (MCM), and MEM (both mobile email management and MEM). All vendors with an expanded solution set have sometimes then listed mobile security management (MSM) and mobile compliance management (MCM) as core services and these are generally selected capabilities from the other services.

Even as M"X"M vendors have expanded their support services capabilities, it has not led to tremendous segment consolidation. The supplier market for M"X"M services worldwide is still vast, numbering over 100 vendors by some estimates. Many organizations have held off on more extensive mobilization efforts, assuming the support services market would consolidate at least a little. That has not happened, meaning that M"X"M vendor assessment remains arduous. As one European government representative recently replied when asked about their mobility solution, "I am just trying to figure out MDM!"

Workspace Management

Workspace management means separating the work and personal persona of the mobile device. Technically this can be implemented by separating work apps, data, and contacts in a secure segment of memory or "container" in the mobile device. The less common approach is *via* the use of virtualization technologies.

Workspace management is gaining more visibility for two reasons. First, employees want to use a single device for work and personal reasons, which mean work and personal apps/data will reside on the same device. Second, employee use of mobile devices for access to corporate resources is increasing, including corporate email access, Wi-Fi access, and even corporate data access through

applications like SharePoint. Workspace management applications and services aim to:

- Ensure personal mobile activities do not adversely affect corporate apps and data.
- Allow single device use.
- Remotely wipe only work apps and data if the employee leaves the company or the device is lost/stolen.

Workspace management has become a hot topic for several reasons. First, because of the prospect of greater employee use of mobile devices for work purposes; second, because of the plethora of solutions available, each affecting the user experience differently and offering different security capabilities. Device OEMs like BlackBerry and Samsung have their own solutions. But several third-party vendors are available as well and now MDM and enterprise mobility management (EMM) vendors are adding container solutions.

The third reason workspace management has become a hot topic is because the combined capabilities of MAM and workspace management solutions have prompted the question: Is MDM needed if there is MAM and workspace management?

Mobile Security

Mobile security is a multi-faceted issue that requires attention at several levels, regardless of the enterprise concern or size of organization. The reason is that mobile security threats continue to grow; according to new research from ABI Research, uniquely mobile threats grew by 261% in the past two quarters of 2012 alone.

Mobile security needs to address three areas:

- Stopping threats from getting into the device, its apps, and its content.
- Protecting content and apps on the device, and ensuring reliable functionality of the device.
- Protecting assets the device is accessing, such as enterprise systems and data.

In addition, the protection offered must balance the security and compliance needs of IT against employee needs for application functionality and personal data privacy.

Today, most smartphone platforms offer standard security capabilities of password access and hardware encryption that provide minimum protection to address the first two threats. However, these do not protect the device from contaminated apps or malware-infected websites. In addition, protection varies by device OS and OEM platform.

Satisfying the third area of mobile security typically requires employing a mobile VPN. But not every mobile device platform has mobile VPN software for the VPN technology used by the organization. For some organizations, even a VPN is not sufficient; its weakness is that once a VPN tunnel is established, any corrupted app or data set is allowed access to corporate network resources.

Every organization will have a different set of security requirements that can be addressed at the hardware level, OS level, app level, network level, and finally via supporting services for app development, malware protection, and enterprise mobility management. Satisfying organization security needs is a menu of choices that can include:

- Username/passwords
- Location/geofencing techniques
- Malware scanning software
- Hardware control
- Whitelist/blacklist techniques
- Remote lock/wipe
- OS monitoring
- Workspace management containers
- Single app containers
- VPN
- Certificates and Single Sign-on (SSO) access
- App-level VPN

- Network level malware control
- Mobile middleware monitoring
- Enterprise directory integration
- Data encryption
- Secure boot
- Trust zones
- Hypervisors

The inter-relationships between hardware, device OS platform, device OEM, applications, and supporting services for securing an organization's mobility solutions is probably the most salient example of the challenges faced by organizations to mobilize. It also highlights the importance of thinking holistically about enterprise mobility enablement.

Support Services

Rounding out enterprise mobile enablement are support services that are not provided in the other solution elements. These include:

- Enhanced customer support with live operator assistance of mobile devices and applications.
- Staging, kitting, and testing services for custom assembly and validation of the device, apps, services, and accessories, prior to worker delivery.
- Training services for mobile devices and applications.

These services are important support pieces that knit together the hard work done building a comprehensive enterprise mobility solution. They limit IT involvement in some of the high-touch device fulfillment activities; ensure workers can fully utilize the solution; and provide ongoing support for the mobile investment.

Aggressive suppliers in this category are beginning to add services capabilities like mobilization strategic planning, MDM services, and IT consulting and systems integration services. Mobile support services companies with an expanded solution set are more aptly called mobility solution/support services providers.

One-stop Shop Providers

If the long list of requirements detailed above is not mind boggling, the numbers of companies offering enterprise mobility services is. For many organizations, sorting through all the companies is a puzzle with pieces that, in practice, do not always match up, particularly as an organization's mobilization needs grow. As a result, solutions are implemented without a thorough understanding of the trade-offs or the supplier options.

One common example is a business unit or government entity that has mobilized a group of employees with a mobile app developed internally and supported using a particular MDM vendor. Many times, the mobile implementation was done quickly to address a competitive need. Positive results cause the organization to expand its mobilization initiatives. However, because the organization wants to utilize multiple device platforms or devices that offer more security options, the application requires a new development effort. If the app development platform and suppliers had been chosen carefully, expansion would have been far less expensive leveraging existing development time, accessible to multiple device platforms, and seamless to the organization. Another issue that can arise is the chosen MDM platform does not scale easily, requiring multiple MDM instances and, therefore, unnecessary costs.

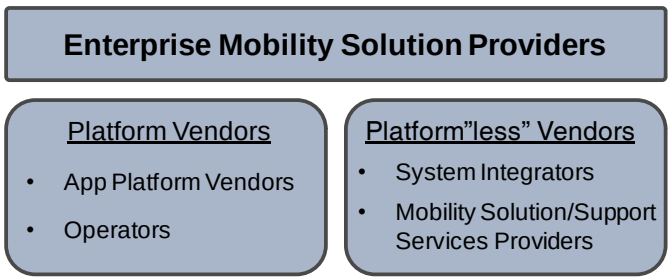
The complexity of the enterprise mobility marketplace begs the question of what supplier segments can be the one-stop shop for all enterprise mobility needs to simplify the decision making process and assist in or manage a mobilization solution implementation. Also, what supplier segments can help an organization understand its current and future mobilization needs so solution implementation is seamless and early investments support later investments (*i.e.*, mobilization ROI is maximized.)

Listed in the table below is an assessment of six supplier segments that through their position in the value chain or their own marketing efforts could be one-stop shop providers.

Supplier	Benefits	Limitations/Issues
Device OEMs	App development and related requirements are limited to one or two device platforms	Focused on selling devices, which is only one part of enterprise mobilization
Mobile App Platform Vendors	Simplify app development and systems integration in a fragmented market	App development tools can be proprietary
MDM/EMM	Focus on support services - many offer several M"X"M services	Core value is on mobile management services – not mobilizing enterprise processes
System Integrators	Enterprise systems and domain expertise	Much less "mobile" knowledge – reliant on partnerships in any enterprise mobilization engagement
Operators	Have "mobile" knowledge across devices, apps, networks, and services	Most lack any IT services or systems integration (SI) expertise
Mobility Solution/ Support Services Providers	Have "mobile" knowledge across devices, apps, networks, and services	Typically focused on "filling in the gaps" for a mobility solution with little IT services or SI expertise

Enterprise Mobility Solution Providers

The typical view of each supplier segment in the table above shows each has limitations as a one-stop shop enterprise mobility provider. However, a few companies in four of the segments have expanded their solution capabilities through their own product development efforts or *via* partnerships to garner the label of enterprise mobility solution provider, effectively a one-stop shop for enterprise mobilization. They exist in two groups:



The common characteristics of enterprise mobility solution providers are:

- **IT Expertise**: Vendor has IT expertise in security, systems, and applications – preferably with industry domain knowledge. Since enterprise mobile solutions become the most valuable when they can leverage corporate data and information, supporting or executing systems integration work simplifies mobile enablement.
- **Professional Services**: Vendor is consultative and can assist in building an enterprise mobility strategy and assembling a set of requirements based on each organization's competitive needs and IT "footprint."
- **End-to-end Solutions**: Vendor can assemble the platforms and partnerships to implement and manage solutions themselves or support an organization's mobilization efforts.
- **Platform**: If the vendor offers a platform that supports or is the basis of the mobile solution, the platform is both scalable and carrier-, device-, and OS-agnostic to both protect against and leverage the limitations and benefits, respectively, of a BYO"X" world.

Enterprise Technology and Market Trends

Enterprise mobility solution providers who are also adept in the enterprise communications market and technology trends, and can offer solutions in the following areas provide additional benefits to an organization pursuing mobility enablement.

- **Cloud Technologies and Services**: The CAPEX and OPEX benefits, and the flexibility offered by cloud technologies and services are completely changing organization communications. As many mobility solution elements are offered as cloud services, tremendous value exists in enterprise mobility solution providers that help merge an organization's mobilization strategy with its cloud strategy.
- **M2M Connections**: M2M communications, the next wave of innovation in the enterprise, is connecting non-IT corporate assets, such as meters, kiosks, vehicles, and point-of-sale devices. These connections allow remote operation and management, ultimately reducing costs and providing better machine utilization intelligence. M2M data can also be used to enhance worker mobile applications. Some enterprise mobility solution providers like operators already offer solutions and support services across machine and device connections.

- **Enterprise Office Evolution**: With the growing use of mobile devices, the enterprise office of today will not look like the enterprise office of tomorrow. Enterprise mobility solution providers that can assess the broadest set of enterprise communications technologies and services offer organizations the best chance to implement mobile solutions that are timely, maximize communications ROI, and are seamless to employee work activities.

Summary and Recommendations

Nearly every organization today needs to implement mobile solutions to compete and serve customers. Some organizations may get by with simple solutions using third-party apps and smartphones. However, most need to think holistically about mobilizing their workforce and work processes. Holistic solutions also need to consider multiple stakeholders, technology and market trends, machine connections and data integration, and the "more mobile" enterprise office.

Nine essential elements make up a holistic mobilization solution. While assessment of these elements may seem complex, the more daunting challenge is evaluating the vendor and supplier options. There are literally hundreds of suppliers and, while the market will consolidate at some point in some solution areas, organizations cannot wait any longer. They must implement a mobile strategy today!

Organizations interested in building a holistic mobilization strategy need to work with at least one or several enterprise mobile solution providers. Companies in this group primarily reside in four supplier segments: app platform vendors, operators, systems integrators, and mobility solution/support services vendors. At a minimum, they can help an organization make the proper choices in vendor selection and, at most, can implement and manage the entire solution. By leveraging suppliers that offer the one-stop shop services of this select group, the painful challenge of vendor assessment is minimized today and mobile investment ROI is maximized for the future.

Contributors

Dan Shey, *Practice Director*

Published April 23, 2013

249 South Street
Oyster Bay, NY 11771 USA
Tel: +1 516-624-2500
Fax: +1 516-624-2501
http://www.abiresearch.com/analystinquiry.jsp