The “Enterprization” of Mobile Apps: Moving from Corporate Liability to Business Asset

A J.Gold Associates White Paper

“Many companies have established mobility as a core strategic technology, deploying corporate liable devices and allowing personally liable devices to connect to their networks and back-office applications. Yet few companies have established a realistic strategy of how to make the apps being utilized by end users (both downloaded from consumer app stores and company issued business apps) truly enterprise controlled, secured and managed... We believe companies must formulate a strategy based on an inclusive vision of apps interacting with corporate systems, and complete governance of these interactions through policy driven “guardian layers” of virtualized environments managing the entire app ecosystem and its interaction with all “touch points” at the enterprise level.”
Contents

Introduction ............................................................................................................. 3

“Consumerization” has its Implications ............................................................... 4

Figure 1: What Users do with their Smartphones: ................................................. 4

Why Should Companies Care about Mobile Apps? ............................................. 5

Figure 2: Losing Corporate Data Can Prove Very Costly........................................ 6

Enterprization of the Mobile App .......................................................................... 6

A New Direction for Mobile Management ............................................................ 7

Integrity of Device Experience ............................................................................. 7

No App Modification ............................................................................................... 7

Invisible Processes ................................................................................................. 7

Maximum Granularity ............................................................................................ 7

Off-The-Shelf Devices ............................................................................................ 7

Detection and Prevention ....................................................................................... 7

Platform Uniformity ............................................................................................... 8

Application Indifference ....................................................................................... 8

IT Operations Effectiveness ................................................................................. 8

Flexibly Supporting Users and Processes ............................................................. 8

IT and Line Of Business (LOB) Partnership ........................................................... 8

Solution Supplementation .................................................................................... 8

Ease of Deployment ............................................................................................... 9

Why MDM/Asset Management Alone is Insufficient........................................... 9

Moving Beyond MDM to a “Mobile App Guardian”............................................. 9

Enterprization of Apps – More Flexibility, Less Cost ........................................... 10

Adding to Existing Capability ............................................................................. 10

Figure 3: A Mobile Management Comparison.................................................... 10

7 Steps to “Enterprization” of Mobile Apps ....................................................... 11

Creating a Strategic Vision – Move From Reactive to Proactive........................ 11

Move Beyond the Device - Focus on the Apps..................................................... 11
The “Enterprization” of Mobile Apps: Moving from Corporate Liability to Business Asset

Defining App Requirements – What’s the Goal? ..........................................................12
Building an App Portfolio – Users, LOB, Opportunities/Tradeoffs .............................12
Getting Users on Your Side – Why User Acceptance is Critical ...............................13
Lifecycle Management – Supporting Users While Planning for Obsolescence ..........13
The Right Tools – What Technology/Infrastructure is Required? .............................14
Conclusions ..................................................................................................................14
Introduction
Many companies have established mobility as a core strategic technology, deploying corporate liable devices and allowing personally liable devices to connect to their networks and back-office applications. Yet few companies have established a realistic strategy of how to make the apps being utilized by end users (both downloaded from consumer app stores and company issued business apps) truly enterprise controlled, secured and managed. Indeed, the majority of apps, especially on personally liable devices, represent a real liability for enterprises since companies often don’t know what is being deployed or how well they serve the user and corporate needs. And organizations often don’t have any control over the information flow associated with the apps. This is an untenable situation, as it affects not only corporate security, but also compromises operational efficiency and complicates core strategic initiatives.

Most companies have taken some preliminary steps in an attempt to manage and/or control their growing mobile diversity requirements and the complexity of end users’ increasing demands for new devices. But the majority of efforts to date have focused on managing the hardware assets through use of a basic Mobile Device Management (MDM) tool. While this is a good first step, it is insufficient to address the entire gamut of new devices coming online at an accelerating rate, or the variations within device families and Operating Systems. Further, it has little effect on controlling interactions between end user downloaded consumer-class apps and corporate data services. A broader control mechanism that supplements MDM and that is more inclusive must be pursued if organizations are to fully protect themselves against potentially catastrophic loss of corporate data, security breaches, and regulatory compliance infractions. And it may be the only way companies can bring strategic control back to their operations.

To further emphasize the rapidly changing environment over the next few years, we highlight one of J.Gold Associates’ key trends:

- **Trend: The path to enterprise mobile diversity leads through the app and not through the device. Indeed, within 2-3 years, Mobile Device Management (MDM) will become a sub-component of the organization’s mobile infrastructure, enhanced by more universal control mechanisms applied to corporate data and applications/interactions.**

This paper will address an approach to mobile management that we believe is imperative if organizations are to keep up with the fast pace of change in mobile user demands and devices. It will provide concrete steps companies can take to enable the organization to plan, implement and operate the most cost effective apps with the greatest degree of security and enhanced end user productivity, while keeping costs to a minimum. And the techniques described will allow organizations to regain control of their mobile strategy which is vital to mission critical operations.
“Consumerization” has its Implications
Over the past 1-2 years, a shift has been taking place in enterprises large and small. That shift, driven by the ready availability at low cost of appealing mobile devices, particularly smartphones but also increasingly tablets, has users demanding access to corporate systems through their personally obtained devices. This “Consumerization” or Bring Your Own Device (BYOD) phenomenon has spread rapidly, with greater than 50% of corporations now supporting this option. What started as a desire by users for mobile access to communications services (e.g., email) has now expanded to include demands for access to a variety of corporate back office systems (e.g., ERP, CRM, SFA) which have greatly complicated the situation for IT services. However, despite the rapid growth of this phenomenon, traditional corporate owned and issued devices have not been eliminated. Indeed, for many organizations requiring special functions or purpose-built devices, corporate liable devices are still the preferred option. And as many organizations have discovered, sometimes it’s just easier to deploy a total corporate solution. It allows ease of deployment, detailed management, defined access services, enhanced security and greater support options. However, even corporate issued devices are being influenced by the consumerization trend, with users exerting pressure on the selection of these devices and the apps to be deployed on them. Nevertheless, most organizations must embrace the consumerization trend and allow end user choice, although often within defined limits.

Clearly users are demanding particular devices because they feel they can help them to perform their jobs better, while also offering them personal features and functions they enjoy. But BYOD is creating a derivative user phenomenon; Bring Your Own Apps (BYOA). Users can obtain a wide range of low cost and easily available apps from a number of retail app storefronts. As a result, many users are repurposing consumer-grade apps for use in the enterprise and claiming increased personal productivity as a result. And the utilization and number of apps per user is growing dramatically, as indicated below.

**Figure 1: What Users do with their Smartphones:**

- Avg # of apps downloaded = 41
- (28% increase from last yr)
- Avg min/day using apps = 94
- Avg min/day browsing = 72

Source: Nielsen, May 2012

In many enterprises, a balancing act must take place between three constituencies focused on differing objectives. Users want choice and perceived productivity gains. Lines of Business (LOB) want to obtain a return on their investment. And IT wants management and security within a controlled infrastructure. Organizations must learn to deal with the increasing use of personal apps within the corporate setting even though it will be a challenge. They must create a safe environment for all constituencies, allowing choice while...
maintaining control, handling multiple device products/families, and managing both consumer and enterprise apps.

Why Should Companies Care about Mobile Apps?
As discussed above, end users are increasingly demanding that companies allow the use of personally obtained mobile apps from the many app stores. This is often because the corporate versions of mobile apps users deem desirable are not available or found lacking. Indeed, app availability is frequently the primary indicator of why users pick a particular platform (e.g., iOS, Android, BlackBerry) or form factor (e.g., smartphone, tablet, laptop). Further, with the growing number of consumer apps available, end users can pick and choose from a diverse array of useful productivity and entertainment solutions, and not be bound to a narrow choice traditionally enforced by the enterprise. It is becoming clear that most enterprises generally can no longer impose a “take it or leave it” approach to designating corporate mobile platforms. Finally, the success of consumerization is making users more adamant about being able to control their own destiny and choose their own apps.

- Trend: The number of enterprise-connected mobile devices and apps will grow dramatically within the next 2-3 years, with the average business user obtaining and using 3-4 mobile devices (e.g., smartphones, tablets, notebooks). We expect 8-10 mobile apps to be regularly employed by the average enterprise worker due to their low cost, utility and ease of acquisition.

As a result, significant challenges that most organizations face include:
- What percentage of apps represents personally chosen vs. corporate endorsed?
- What are the ramifications of personally acquired apps on enterprise-connected devices?
- And importantly, how protected is the primary corporate asset interacting with those apps: the enterprise’s data?

Users want their apps and will often go to great lengths to obtain and use them in business settings, with or without permission. Indeed, many apps from commercial app stores are quite useful in the performance of their assignments, so limiting app selection may also limit productivity. But unfettered access to corporate systems and the intermingling of personal and corporate data also means unprotected/unsafe operations, as the organization may loose control of information flow. Data loss is no small issue for enterprises, as it not only exposes the organization to customer complaints but may also lead to regulatory compliance issues. And the potential risk is substantial. Each piece of personally identifiable data record lost on a mobile device costs $258 to mitigate according to Ponemon Institute. And with the growing storage capacity of mobile devices, the amount of potential data on each lost device is quite high.
Figure 2: Losing Corporate Data Can Prove Very Costly

- 5%-10% of notebooks are lost/stolen per year
- 15%-25% of phones are lost/stolen per year
- Each lost personal record costs $258 to mitigate (Ponemon Institute)
- Losing 10K records costs $2.58M

Many users who acquire their own devices and apps resent any interference by the corporation in control and management of those personal assets. And enterprises face potential liabilities (legal or simply user disillusionment) should they create a device-damaging situation (e.g., wipe a BYOD device) in an attempt to exert more control. The challenge then is to regain enterprise control by deploying technology that offers transparency of device/app operation and control while minimizing user intrusion.

Enterprization of the Mobile App

As the diversity of mobile devices and end user demands accelerates, enterprises that focus exclusively on basic MDM without also focusing on the interaction between apps and corporate assets increasingly risk security and manageability problems and will ultimately lose control of their infrastructure. In an increasingly competitive world where companies leverage a highly mobile workforce, organizations not adapting to the new mobile reality will be left behind. They will be unable to cope with the surge in end user demand, the plethora of device types, and will be stuck hopelessly reacting to change rather than assuming a leadership position.

- Trend: By 2014-2015, enterprises that haven’t implemented a mobile device strategy focusing on mobile apps and their interaction with corporate systems will be at risk of losing control of their mobile infrastructure. This will dramatically increase security breaches and cost of operations, while decreasing end user productivity and approaching a state of mobile anarchy. Further, companies that focus on the adoption of mobile app management will see a 25%-35% lower mobile TCO than those only focused on traditional asset management.

So what should organizations do? First and foremost they need to embrace a strategy that envisions use of a wide variety of mobile devices, platforms and form factors that are obtained by the company as well as directly by the end user (either through personal preference or as an informed choice from an approved list endorsed by the organization). But it is imperative that organizations moving forward with the new mobile reality include security and compliance as a primary objective, with manageability, cost of ownership and support as critical strategic necessities. To accomplish this, enterprises must approach mobility management with an updated vision - focusing on information content and flow, rather than simply device asset management.
A New Direction for Mobile Management
Moving towards app interaction management as compared to exclusively asset management requires a new vision. To be successful, enterprises should concentrate on a number of key requirements in implementing a solution. These attributes should include:

Integrity of Device Experience – Most users pick a device based on the overall user experience it provides, and are unsatisfied when that experience is modified or disturbed. Therefore, any enterprise mobile management strategy must take into account the need to leave the native look and feel and user interface (UI) in place. Solutions that modify the device or install a new UI/app environment will receive a negative reception by most users. Dissatisfaction will lead to user resistance and/or “sabotage” of control mechanisms.

No App Modification – Some mobility management products utilize an approach to data security that requires modifying the code with a layer of specialized software. This requires access to the original code and/or a modification of the license agreement. Further, the app must be “processed” before it can be deployed, and each succeeding version of the app must be similarly processed and/or recompiled. This adds a significant degree of complexity to the operations and increased time to deployment, and should be avoided.

Invisible Processes – For maximum effectiveness, any approach to security and management should be operationally transparent to the end user. It should further be hidden from tampering and not available to be manipulated through normal device setup and menu operations. Transparency to end user day to day operations is a critical feature to assuring success of any mobile management and security solution.

Maximum Granularity – Although certain policies may be universally applied (e.g., authorization, encryption, VPN), there may be many that are user or organizational role specific (e.g., access to certain data, app access). Any effective approach should allow a high level of granularity in supporting the widest array of policies, as well as ease of enrollment, modification and deployment to the device. A highly granular policy setting is a prerequisite for establishing an effective mobile management capability in increasingly flexible organizations and business processes.

Off-The-Shelf Devices – Some solutions require specially modified devices and/or reloading operating systems to function effectively. Yet it is often difficult to deploy such customized platforms. Users can not simply go into a retail shop to purchase one, which is the increasingly preferred method of obtaining a mobile device. Further, such custom products generally are not quickly updated as new devices/OSes are released. The lack of selection and elimination of many popular device choices will not be attractive to end users, nor will it allow companies to support the latest and most popular devices. While the device modification may have some benefits (e.g., virtualized segmentation, increased manageability, individual containerization) enterprises should avoid this approach.

Detection and Prevention – Many features and functions inherent in a good management and security strategy can be defeated if the device attached to the corporate infrastructure has an unauthorized modification to the OS (“Jailbreaking” or “Rootkitting”). Nearly all jailbroken devices include compromises to inherent built-in security mechanisms (a large reason for jailbreaking in the first place). To maximize corporate control, any effective
management solution must be able to recognize such jailbroken devices and then deny access to corporate resources to those devices, while also notifying the end user as to the cause of the rejection. In advanced management systems, remediation to factory standards might be possible in some cases, but this should not be done without the express permission of the users. The safest approach is to simply deny access to such devices.

**Platform Uniformity** – Not all platforms are equivalent when it comes to management capability and security enforcement. Indeed, it’s not uncommon for popularly deployed devices to have different versions of an OS that provide different levels of management support (e.g., various versions of Android and iOS). Any mobile management solution should include a capacity to minimize the differences by maximizing commonality whenever possible. It will not be possible to apply all policies equally to each platform, but it is important that any solution maximize deployment equivalence across diverse devices.

**Application Indifference** – Most users will employ both corporate-furnished and app store available consumer apps to maximize their productivity. As a result there will be an array of apps deployed for common functions based on end user preferences. It is imperative that any solution must embrace an “app indifference” strategy that supports a wide array of both in-house custom as well as off-the-shelf consumer apps. Any solution not providing such universal capability will only provide a partial solution. Further, apps, especially consumer apps, are updated often and users typically rapidly upgrade to the latest version. Enterprises should have some control over the type and frequency of app upgrades when it might have an influence on operations (e.g., modified or specially integrated apps). But aside from such limits, any solution that does not allow for simple app upgrading and/or replacement will ultimately be unsatisfactory to the end user and restrict the ability of the organization to manage and secure the mobile environment.

**IT Operations Effectiveness** - Many organizations have not done a satisfactory job of mobile management because they lacked the expertise and resources necessary, and solutions are not always easy to deploy. It is important that any solution be easy to implement and support and be available for either internal or cloud-based installations. The best way to keep overall Total Cost of Ownership (TCO) low is to minimize needed IT resources while simplifying end user deployments and problem support resolution.

**Flexibly Supporting Users and Processes** - Any management and security solution must be easily modifiable for new users, groups and/or applications processes. This is important for end user support as many organizations have difficulty resolving problems resulting from improperly applied policies and/or change in infrastructure requirements. This is critical for organizations with rapidly changing and continuously modified business processes.

**IT and Line Of Business (LOB) Partnership** – It’s very likely that IT will not have a complete understanding of all of the needs of the various LOBs within the organization. It’s equally likely that the various LOB’s will see traditional IT processes as a barrier to more effective use of mobility and will seek ways to bypass them. This can create a state of anarchy. An optimum solution will provide IT with the management and control mechanisms it needs while allowing LOB’s maximum flexibility in quickly deploying diverse solutions. This is the best way to minimize the IT-LOB conflict inherent in many enterprises.

**Solution Supplementation** – It’s unlikely in the fast-paced and rapidly changing world of mobility that one management product can offer all the features and functions necessary for
the long term. Organizations should therefore plan on implementing solutions that can be easily upgraded and/or supplemented with complementary products and features when/if needed (e.g., new OS support, integration with network/infrastructure components, identity management, Digital Rights Management, VPN, directories). This approach maximizes the organizational investment while assuring that any solutions deployed can meet the needs of expanding policy requirements and/or platform changes without becoming obsolete.

**Ease of Deployment** – Mobile management solutions require a component be installed on the device. It is highly desirable that any management and control solution be installable easily and on all standard device types, preferably by the end user (e.g., clicking on a link to a web page or pushed in an email). This requires minimal intervention by the enterprise, which is especially important on user-owned devices.

**Why MDM/Asset Management Alone is Insufficient**

Many companies have deployed basic Mobile Devices Management (MDM) in an attempt to regain control over the diversity of devices deployed in their organization. The primary intent of MDM is to control the asset – the device. It does so by deploying a set of policies that govern the use of the device (e.g., access control, log in authorization, device wipe).

However there is a high degree of variability in mobile device management capability. MDM can be programmed with set policies, but they are often inconsistently applied to different devices based on available control mechanisms within the platform. Further, most MDM assumes that it has overriding control of the device, with enterprise dictate over what MDM ultimately does with the device. This does not sit well with many end users who may see this as an intrusion of their personal property rights, even with company enforced and user agreed-to policies for use of BYOD devices. Nor does MDM work well for those devices that inherently have minimal APIs to enable granular control of resources and functions.

Most MDM solutions currently do not granularly control specific apps or their interactions with the corporate back end systems and data. BYOD users load apps of their choosing and expect complete control. Yet enterprises view apps that touch their systems as necessarily being under their control. This often becomes an area of contention between end users and organizations. User control means wide open access and unprotected data on the device, while enterprise control means access can be selectively denied as appropriate.

**Moving Beyond MDM to a “Mobile App Guardian”**

Clearly, while basic MDM adds value to an organization’s mobile management efforts, a more inclusive approach is desirable – one that’s more in tune with both end user desires and enterprise requirements. A primary requirement for next generation mobile management, particularly for BYOD, is to create a solution that manages enterprise connected apps, data and interactions in addition to basic MDM/asset management. Any personal app operations by the user without interaction with corporate data or systems should be ignored. This eliminates the end user dissatisfaction with overriding corporate control, while also allowing the organization to steer clear of any possible ramifications of destroying personal data.
The “Enterprization” of Mobile Apps:
Moving from Corporate Liability to Business Asset

The way to accomplish this is to change the focus from exclusively asset management to one that is focused on the apps. There are technologies that have attempted to provide such functionality. But they often do so by requiring specially created or modified apps which both alters the user experience and requires access to the source code, or by creating a specialized OS (“virtualization”) which requires modification of the off-the-shelf device OS and user interface. While both methods work and accomplish the desired goal, they require non-standard apps and/or devices. This adds a layer of complexity that negates the advantage of BYOD and commercially available mobile apps so desirable to end users, and potentially advantageous to the organization.

What’s needed is a non-invasive technique to provide enterprise oversight while allowing users to maintain the look and feel of their devices and apps. Such an approach enables utilization of off-the-shelf apps for corporate interactions. It requires a supervisory “app virtualization layer” that can monitor all activity and act as intermediary between the end user apps and the corporate assets. This results in control of security and access through specific policies, but preserves the look and feel of the app and the overall user experience.

**Enterprization of Apps – More Flexibility, Less Cost**

The new “Enterprization of Mobile Apps” solution will focus on the interaction between mobile apps and the corporate assets with the objective of controlling and protecting corporate data access and content. This direction offers greater promise going forward than exclusively asset-oriented approaches.

**Adding to Existing Capability**

Not all enterprises will be able to implement a “green field” solution deploying only next generation technology. Supplementing existing asset management approaches (MDM) is often the most advantageous approach to enterprises moving to a more complete solution. Below is a chart that highlights the additional features and functions available when adding an Enterprization of Mobile Apps capability to an existing MDM solution.

**Figure 3: A Mobile Management Comparison**

<table>
<thead>
<tr>
<th>A Mobile Management Checklist</th>
<th>MDM Alone</th>
<th>+ App Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity of Device Experience</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>No App Modification</td>
<td>-</td>
<td>++</td>
</tr>
<tr>
<td>Invisible Processes</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Maximum Granularity</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Off-The-Shelf Devices</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>Detection and Prevention</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Platform Uniformity</td>
<td>-</td>
<td>++</td>
</tr>
<tr>
<td>Application Indifference</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>IT Operations Effectiveness</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Flexibly Supporting Users and Processes</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>IT and Line Of Business (LOB) Partnership</td>
<td>-</td>
<td>++</td>
</tr>
<tr>
<td>Solution Supplementation</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Ease of Deployment</td>
<td>+</td>
<td>++</td>
</tr>
</tbody>
</table>
7 Steps to “Enterprization” of Mobile Apps

There are a number of practical steps that organizations can take to create a system for “Enterprization” of mobile apps. These steps include:

**Creating a Strategic Vision – Move From Reactive to Proactive**

Most end users don’t think beyond their immediate needs. This is not necessarily a bad thing, as they have specific work-related challenges they wish to solve. Yet organizations generally have broader, longer term goals that require planning and foresight, lest they become bogged down in always reacting to individual problems. Even so, less than 50% of enterprises have a mobile strategic plan in place. The organization must consider not only what apps it may need for current challenges, but what the long term requirements are for business and technical needs. If it has not, it is doing a great disservice to both end users, and to the bottom line. Enterprises must create a strategic vision that takes into account:

- **Current Line of Business Needs.** Since most mobility projects are being funded by the LOB, it is imperative to consider those needs before considering and/or deploying mobile apps. However, it is not uncommon for LOBs to act in their own self interest rather than seeing the corporate implications of their wants/desires. A balance is required in assessing mobile apps to insure they meet the needs not only of the LOB, but also the needs of the organization as a whole.

- **Longer term needs based on strategic understanding of the business requirements for the next few years.** This step is critical as it provides a way for organizations to assess the amount of effort they will need to secure current apps compared to what will be needed for future apps. This step will be used to provide a decision point for short term needs vs. longer term projects, and allow companies to maximize return on their mobile investment.

- **An understanding of technology advances and positions over the next several years, including device characteristics, connectivity options, back office connectivity, user preferences, usability models, etc.** A strategic understanding will allow companies to provide for the cost optimized deployment of mobility, while limiting potential “dead ends” and prematurely obsolete capability.

- **An ability to distinguish strategic initiatives from user preferences, and to react accordingly.** While users may request a specific capability/solution, it may not always be in the best long term interest of the organization, and an alternative may ultimately be a better fit. Having enterprise expertise available to guide users in their mobile app selection is required.

**Move Beyond the Device - Focus on the Apps**

As discussed earlier, managing device assets is not always sufficient to secure corporate assets or safely grant access to corporate systems. A better approach is to protect the app interactions with corporate data and systems. An effective way to do this is to add a supervisory layer between the app and the device OS that monitors all interactions and
controls user actions based on a predefined policy. Some of the interactions that can be controlled in this fashion include:

- Authentication/Login
- VPN requirements
- Data management/encryption
- Network Access Control
- Interaction by time, date, location, etc.
- Browsing interactions
- Role and/or LOB App segmentation
- Application to application interactions
- Commercial app support without modification
- Provisioning control
- Restrictions on data access and movement (e.g., cut and paste, forwarding to cloud)
- Wiping of data (corporate data only, not personal data)

Concentrating on the app instead of the device alone also provides the broadest device support possibilities. While not all devices are created equally when it comes to management and policy support, adding management at the app layer provides the greatest ability to embrace new devices, but requires that the supervisory layer be available for the devices the enterprise plans to support.

**Defining App Requirements – What’s the Goal?**

Many organizations have done a poor job of defining requirements for mobile apps. Indeed, the reason so many users download their own apps is often because companies have not provided the tools users want and need. Most organizations should embrace the user desire for mobile apps that make them more productive. Enterprization of apps includes a strategy for defining:

- Who gets to make the decision?
- Who pays?
- Who deploys the apps?
- How many devices/types to support with an app?
- What access does a particular app get to corporate systems?
- Will the app be available from a corporate app store?
- How will the app be supported, maintained and/or upgraded?

Ultimately the organization needs to define its goals. Is the goal a free-for-all or a consolidated approach to productivity? Generally, the latter requires planning and management for achieving a state of equilibrium, while the former is in a constant state of mismanagement and chaos.

**Building an App Portfolio – Users, LOB, Opportunities/Tradeoffs**

Enterprises should approach apps from the perspective of a broad portfolio approach rather than on an individual basis. They must look at apps based on factors such as:

- Who decides on the app?
- Where does it come from?
The “Enterprization” of Mobile Apps: Moving from Corporate Liability to Business Asset

- Who are the stakeholders?
In most cases the LOB that specified and funded the app will be making the final determination, not IT. But not all apps will be productive or useful. The average consumer app after being downloaded is discarded (or ignored) after 3-6 months. Therefore, enterprises should look at the total app portfolio rather than individual apps. Much like in an investment portfolio, some apps will do very well and gain a large following with compelling productivity enhancements and some will be quickly left behind. Enterprises should strive for a 15%-25% total portfolio ROI across all apps. A flexible approach that results from app management on top of device management provides organizations the ability to rapidly make changes to the app portfolio available to its users, while keeping costs low and protecting data and back end systems. And the ability to obtain app feedback from actual user interactions will help companies better “tune” the apps to enhance good apps and eliminate the bad.

**Getting Users on Your Side – Why User Acceptance is Critical**
No mobile app enterprization strategy can be successful without the support of the end users who ultimately use the apps. Most companies are moving towards a pay as you go model, which means that the LOB will ultimately pay for the app. If the users are not satisfied with the management of the apps and the portfolio available to them, IT will have a hard time obtaining the funding it needs. Uses are very creative and will find ways around perceived roadblocks. As such, making sure the end users are satisfied with the approach is critical. Users should be made aware that:

- Their wants and desires will be taken into consideration (although not always implemented)
- The broadest choice of devices and apps are being made available
- The enterprise will avoid impacting their desired mode of operation/choice on user experience
- Management and security will be implemented in an “as transparent to the end user” mode as possible
- All reasonable attempts will be made to segregate personal from corporate assets on the device
- User input will have a major impact on future direction and implementation strategies

Companies should do regular polling of users for feedback and to determine if the goals are being met. Getting support of the end users will not only make the organization run more smoothly, it will also substantially make IT’s job easier and minimize the level of support required. Finally, companies must be able to leverage BYOA as it makes sense to do so. Enterprises can’t keep up with the market if they do everything themselves, and users likely won’t let them.

**Lifecycle Management – Supporting Users While Planning for Obsolescence**
Not all apps used for mobile productivity will be created equal. Some will be popular and highly successful, while others may be used only occasionally and/or by few users. This will likely be true both for off-the-shelf consumer and corporate sponsored/created apps.
Enterprises should have an “update/replacement” strategy in place for apps. Measuring the success and failures of apps will allow the organization to better facilitate the use of mobile devices by learning what’s important to user productivity, which apps are most popular and why, and what is missing that causes users to abandon certain apps. A continuous upgrade cycle of apps should be a prerequisite for any organization that is serious about mobility. The feedback process will prevent future products suffering from a lack of well thought out features and functions, thus eliminating most marginal or failed apps.

**The Right Tools – What Technology/Infrastructure is Required?**

The final step in creating an enterprise-centric mobile app strategy is to define and deploy tools and technologies. To this end, companies should focus on:

- Maintaining MDM functions but with “next generation” enhancements
- Employing a “Mobile Guardian” strategy that focuses on the app and its interaction with corporate assets, and not just device asset management
- Choosing a solution that works across a number of platforms and form factors
- Handling corporate and consumer apps transparently
- Integrating to existing systems (email, directory, VPN, etc.)
- Allowing deployment either on-site, in the cloud, or as a “hybrid” approach as needed.
- Obtaining a solution with maximum expandability as there is no guarantee there won’t be changes in the future
- Establishing a data “Firewall” capability that all data must pass through and be vetted for personal or corporate control.

These tools/technologies must be flexible, as it is certain that with the rapidly changing spectrum of device types, form factors and apps, the enterprise will have to make changes on a regular basis. Many solutions look alike - look beyond surface to the core technologies.

**Conclusions**

Mobile diversity and the consumerization of IT has created an environment where enterprises need to cope with an increasingly complex universe of mobile users and devices, business processes and consumer apps, connections to corporate systems, and a dizzying array of user demands for more complete and better mobile experiences. Companies have responded by implementing some initial mobile asset management functions. Indeed, BYOD has driven companies to adopt MDM to alleviate some of the confusion and “mobile anarchy” currently prevalent in many organizations. And while MDM is a good first step towards managing and securing mobility within the enterprise, companies must look to an enhanced and expanded role based on app management rather than the purely asset driven approach implemented with current systems. We believe companies must formulate a strategy based on an inclusive vision of apps interacting with corporate systems, and complete governance of these interactions through policy driven “guardian layers” of virtualized environments managing the entire app ecosystem and its interaction with all “touch points” at the enterprise level. It is only through this advanced model supplementing MDM functions that companies can hope to secure and manage their most valuable asset - their data.
About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.