Building "Bring-Your-Own-Device" (BYOD) Strategies

This is the first part in a series designed to help organizations develop their "BYOD" (bring-your-own-device) strategies for personally-owned smartphones and tablets. This chapter provides an overview of eight components that our customers have found to be the foundation of a secure and scalable BYOD program.

Many organizations are considering personally-owned mobile devices for business apps. Their goal is to drive employee satisfaction and productivity through the use of new technologies, while simultaneously reducing mobile expenses. This BYOD trend is one of the more dramatic results of the consumerization of IT, in which consumer preference, not corporate initiative, drives the adoption of technologies in the enterprise. However, many of these technologies were not built with enterprise requirements in mind, so IT teams often feel uncomfortable about security and supportability.

Within the MobileIron customer base, we have seen a broad spectrum of BYOD approaches, ranging from top-of-the-pyramid, where a small set of executives or technical staff get to use their own devices, to broad-scale, where BYOD is opened up to a larger percentage of the employee base. In many organizations, employees are now offered a choice between a corporate-funded BlackBerry or a personally-funded iOS, Android or other new-generation device. In her Spring 2011 presentation, "Bring Your Own Mobility: Planning for Innovation and Risk Management," Monica Basso, Research VP at Gartner, Inc., predicted that by 2014 "*90% of organizations will support corporate applications on personal devices.*" As a result, IT teams are preparing for a mixed-ownership mobile environment.

But BYOD is more than just shifting ownership of the device to the employee. It has many complex and hidden implications for which a strategy needs to be defined in advance of implementation. Based on the experience of our customers, this paper outlines eight major components for successful BYOD strategies:

- Sustainability
- Device choice
- Trust model
- Liability
- User experience and privacy
- App design and governance
- Economics
- Internal marketing

Sustainability

BYOD is new to most organizations and, as a result, best practices for implementation are just now being developed. One of the traps many fall into is establishing a rigid set of BYOD policies that is not sustainable over the long term. To be sustainable, BYOD policies must meet the needs of both IT and employees for:

- *Securing corporate data*
- *Minimizing cost of implementation and enforcement*
- *Preserving the native user experience*
- *Staying up-to-date with user preferences and technology innovations*

We see organizations focusing the majority of their time and resources on the first two requirements. But the latter two are much more important for sustainability in the long term. If the BYOD implementation damages user experience or quickly becomes dated, employees will either find a way to circumvent policy or end their participation in the program. In both instances, the needs of neither the employee nor the company are met – either security is compromised or business value is lost. ***User experience is the litmus test for policy sustainability.*** If it breaks, so does the program.

Device Choice

The primary catalyst for BYOD is that employees have personal preferences for devices other than those that the enterprise has traditionally provided them. The most common example is an employee who has a corporate-owned BlackBerry for work, but a personal iPhone or Android device at home, and would prefer to carry one device instead of two. However, in a world where consumer preferences shift annually, or even quarterly, and the mobile device and apps landscape itself evolves constantly, defining how much choice to allow employees is difficult.

Building a policy around device choice requires:

- *Analyzing employee preference and understanding which devices they have already bought:* A BYOD program that doesn't support current and intended purchases will have limited appeal.
- *Defining an acceptance baseline of what security and supportability features a BYOD device should support:* The goal is to include all employees' desired mobile platforms in the program, without creating security gaps or support headaches. The acceptance baseline generally includes asset management, encryption, password policy, remote lock/wipe, and email/Wi-Fi/VPN configuration. Without these fundamentals, the mobile platform is not viable for the enterprise. The more advanced list generally focuses on app-related functionality and advanced security such as certificate-based authentication. The device platforms that match the advanced list get access to a higher level of enterprise functionality in the BYOD program.
- *Understanding the operating system, hardware, and regional variances around that baseline:* On Android especially, similar devices may actually support very different capabilities based on the manufacturer and the geographic region. The brand name of the same device may also vary by wireless operator, adding confusion.
- *Developing a light-touch certification plan for evaluation of future devices:* Most organizations invest in upfront certification when launching their BYOD program. However, new devices are introduced into the market every 3-6 months so the certification process must be ongoing and continually evolving. If the process is too heavy, it will become expensive and eventually fall behind, so speed and efficiency of certification is essential.
- *Establishing clear communication to users about which devices are allowed or not, and why*: Going BYOD without this clarity results in users purchasing unsupported devices or becoming frustrated that the service levels they expected from IT are not available to them.

- *Ensuring the IT team has the bandwidth to stay up-to-date:* The allowed device list is strongly influenced by user demand and so may change rapidly, often multiple times a year. Someone in IT must become the expert on device and operating system evolution; otherwise, the BYOD program quickly becomes obsolete. This is especially important when the program moves beyond iOS and BlackBerry to operating systems with more variants.

Trust Model

Trust remains the foundation for enterprise security: Which users do I trust with which data or apps under what circumstances? Every major organization has gone through data classification to establish this underpinning for its security policies. However, even without BYOD, trust models for mobile add an additional level of complexity because the device itself easily falls in and out of compliance. ***The trust level of a mobile device is dynamic***, and depends on its security posture at a given point in time. For example, a company's CFO is trusted with financial data on her tablet, but not if she inadvertently downloads a risky consumer app or disables encryption. Because mobile devices are not locked down as comprehensively as traditional laptops and desktops, they fall out of compliance more frequently.

BYOD adds another layer to the trust model, because the trust level for personal devices may be different than for corporate devices. Privacy policies will vary, as will user expectations. For example, users may accept not being able to use social networking apps on corporate devices, but that type of policy is unacceptable for personal devices.

Building a BYOD trust model requires:

- *Identifying and assessing risk for common security posture issues on personal devices:* Employees use personal devices differently than corporate devices; for example, they download more apps. So with BYOD, devices may fall out of compliance with corporate policy more frequently, or for different reasons.
- *Defining remediation options (notification, access control, quarantine, selective wipe):* These options may differ in severity from BYOD to corporate devices. For example, on a corporate device with a moderate risk compliance issue, the remediation might be an immediate full wipe. But on a personal device, it may be a less severe action initially, like blocking enterprise access, followed by a selective wipe of only enterprise data.
- *Setting tiered policy:* "Ownership" is now a key dimension along which to set policy. As a result, personal and corporate devices will each have different sets of policies for security, privacy, and app distribution.
- *Establishing the identity of user and device:* As device choice becomes fluid, confirming identity of user and device, usually through certificates, becomes more important.
- *Lending a critical eye to the sustainability of the security policy being instituted:* What is the impact on user experience? Will users accept that tradeoff over the long term? If the trust level of the personal device is so low that security requires extensive usage restrictions, the employee's personal mobile experience will be damaged, and neither the policy nor the BYOD program will be sustainable.

Liability

All enterprises have long-standing approaches to assessing the risk of employee actions and the corresponding liability. These actions range from unsecured use of company data to accessing inappropriate applications or websites. BYOD introduces a new consideration: The device on which these actions may take place is not the property of the company. So the question is "Does moving device ownership from company to employee increase or decrease corporate liability?"

Some considerations around BYOD liability include:

- *Defining the elements of baseline protection for enterprise data on BYOD devices*: All companies must protect corporate data on the mobile device. But different protections may be required on different devices. For example, more protection against over-privileged consumer apps might be required on Android vs. iOS. Employees will also need clarity around which actions create and limit liability.
- *Assessing liability for personal web and app usage:* The employee's expectation is that they can use their personal device however they wish. Is inappropriate use still a liability for the company, even if it doesn't affect enterprise data?
- *Assessing liability for usage onsite vs. offsite, and inside work hours vs. outside:* Should usage be monitored when at work, but not when away from work? The boundaries of work time and personal time blur for many knowledge workers, so most companies avoid this additional complexity.
- *Evaluating whether the nature of BYOD reimbursement affects liability (partial stipend vs. full payment of service costs):* Many organizations have assumed that the level of payment doesn't impact the level of liability, but this is an area with regional variances. Financial responsibility may dictate legal obligation.
- *Quantifying the monitoring, enforcement and audit costs of the BYOD compliance policy*: If liability is lower, the corresponding compliance costs will also be lower, and potentially a significant contributor to cost savings.
- *Assessing the risk and resulting liability of accessing and damaging personal data (for example, doing a full instead of selective wipe by mistake):* Most organizations will cover themselves legally in their user agreement, but at minimum, this creates employee frustration and concern over privacy.

We have seen many large organizations decide that their liability on personal devices is limited to protecting corporate data, and that they are not liable for personal web, app, or other activity. In other words, their corporate liability decreases if they move to BYOD. However, we have also seen other organizations decide that their corporate liability remains unchanged. Each organization should seek their own legal advice on how to frame and assess liability variances between BYOD and traditional mobile programs.

User Experience and Privacy

BYOD itself reflects a realization that employee satisfaction is a primary goal for IT. But many times, security and user experience have been viewed as conflicting interests; therefore, the usability of traditional enterprise applications has substantially lagged behind that of consumer applications, which are designed with user

experience as the top priority. ***The core tenet of successful BYOD deployments is preservation of user experience***. These programs will not be sustainable if user experience is compromised when employees start using their personal devices for corporate email and apps. User experience can be compromised along many dimensions: poor battery life, 3rd party email apps that don't preserve the native experience, complex authentication, lockdown of useful features, counterintuitive interfaces, or lack of privacy.

A ***social contract*** must be established between the company and the employee. This social contract is the agreement between employer and employee about their respective roles in the BYOD relationship:

- *Identifying the activities and data IT will monitor:* On personal devices, IT will generally monitor less user data and activity, such as location. There will be an ongoing set of security vs. privacy tradeoffs to make. For example, IT might still need to monitor app inventory on the personal device in order to protect against rogue apps that might otherwise compromise enterprise data.
- *Clarifying the actions IT will take and under which circumstances:* The employee must understand the link between action and remediation, for example, the circumstances under which IT will wipe a device and the content that will be wiped. ***Transparency will create trust***.
- *Defining the BYOD privacy policy:* Granular controls across IT actions like activity monitoring, location tracking, and application visibility should be consolidated into a privacy policy and then applied to each mobile device. These policies will differ not just by device ownership, but also by organizational function, seniority, and region. Exceptions to the privacy policy should be minimized, but employees will still need to understand the circumstances of those exceptions, such as legal mandate.
- *Critically assessing security policies and restrictions for sustainability:* If the user experience is compromised by the security policy, the BYOD program will be at risk. Common restrictions that impact experience are lockdown policies for apps, browsers, or media features like camera.
- *Deploying core services (email, critical apps, WLAN access) to the employee:* The more compelling these services, the more willing the user is to accept some level of corporate control over the personal device.
- *Preserving the native experience:* Employees want to use their preferred native apps for core functions like email, calendar, contacts, and communications. Forcing these activities to different apps in the name of security will fracture the user experience and limit sustainability.
- *Communicating compliance issues clearly to the employee:* How will the employee know when his device or actions are out of compliance? What are the consequences? A closed-loop, automated notification process ensures that the employee, who will likely never fully read the user agreement, knows immediately when there is a compliance issue and what actions the company is about to take. ***BYOD users expect to be given the chance to self-remediate.***

As mentioned earlier, user experience is the litmus test for policy sustainability. In many organizations, BYOD programs are implemented with the intent of increasing employee satisfaction, but end up compromising user experience. Without a clear social contract that extends beyond a written agreement to daily activities and actions, an effective BYOD relationship cannot be established between employer and employee.

App Design and Governance

The trust model and device choice considerations described in prior sections both have a fundamental impact on the apps strategy for BYOD. At first, organizations assume BYOD is simply a device ownership decision with minimal impact on apps. But apps involve enterprise data, and if the trust level of a BYOD device is different than that of a traditional device, it will affect app design and distribution. Also, employees will expect internal apps to be supported on all the approved BYOD devices, not only a subset. That implies either a deeper investment in app development and testing by the company, or clear education and communication for employees on what apps are supported on what devices, and why. User confusion will drive helpdesk calls.

Some considerations around app design and governance include:

- *Designing mobile apps to match the trust level of personal devices:* App development teams will have to decide whether they design apps differently for personal vs. corporate devices. These differences generally center on how the app handles local data and are driven by the trust level of the target devices. A shared strategy is more cost effective while a separate strategy can optimize user experience.
- *Modifying app catalog availability based on device ownership:* Certain internal applications may not be appropriate on personal devices for security reasons. For example, all devices might have access to the mobile case management app, but only the corporate devices to the mobile financial projections app.
- *Committing to the resource investment:* There can be incremental investment to support core enterprise apps on personal devices – for example, apps may now need to support more operating systems and device types. So the app dev team must either support the broad set, or clearly communicate to the employee base how and why support is limited.
- *Updating acceptable use policies:* Employees will demand freedom to use a broad range of personal apps on their BYOD device. In their minds, the fact that the device is also being used for corporate apps doesn't justify restrictions on their personal apps. Therefore, any such restrictions that are necessary for corporate security purposes need to be clearly described to the employee, e.g., "App X is known to access and transmit personal contact lists to unknown third parties."
- *Defining enforcement levels for app violations (notification, access control, quarantine, or selective wipe):* Once again, clear communication is as important as the actual policy and outcome.

Economics

The short-term economic analysis of BYOD generally revolves around eliminating the cost of device purchases and moving from full service payment to a predictable monthly stipend. But the long-term economics may well come from more unexpected sources. BYOD strategies have not been in place long enough at most organizations to definitively assess their economic impact, but here are some key dimensions to consider:

- *Device hardware:* Not needing to purchase hardware is appealing. However, many large enterprises have traditionally purchased highly subsidized smartphones, so the actual savings can be less than expected.

- *Excessive charges:* When employees have personal visibility into their usage, especially excess usage, their behavior tends to become more responsible. They use the device more sparingly when roaming, and they are less likely to lose it. ***BYOD drives personal responsibility***.
- *Service plans:* Some organizations continue paying for full service, while others move to a fixed monthly stipend for the user, many times based on seniority level and function within the organization. However, negotiating leverage with the wireless operator can be lost if the billing model does not provide any consolidation.
- *Productivity*: It is harder to quantify, but access to corporate functions on the employee's preferred device instead of the company's preferred device drives not only satisfaction but also increased productivity. Employees now have the tools they want to use for the work they need to do.
- *Helpdesk*: Traditional wisdom held that BYOD will increase helpdesk costs because of the fragmentation of adding device choice. Implementing new helpdesk policies around full support and "best effort" do create additional complexity. However, we have seen a countervailing force as well, which is that employees who own their devices are willing to invest time in troubleshooting instead of calling the helpdesk. They are increasingly knowledgeable about technology and, more importantly, don't want IT to touch their personal device. With the right self-service tools, ***the helpdesk may become a last resort instead of a first resort for BYOD users.***
- *Compliance and audit*: The earlier section on Liability posed the question "Does moving device ownership from company to employee increase or decrease the company's liability?" The answer to this will impact actual compliance costs dramatically. If the organization views itself as no longer liable for actions other than enterprise data protection, there may be substantial savings.
- *Tax implications*: Some regions have different tax implications for corporate vs. personally-funded devices. The cost of the BYOD program will be affected by whether the company has the obligation to tie reimbursement to a percentage estimate of business use, and how detailed that auditing needs to be.

The ROI of BYOD programs is a combination of the above variables weighed against the value of employee satisfaction and productivity. The hidden economics of BYOD center on increasing productivity, managing the cost of complexity, and realizing the value of more responsible employee usage.

Internal Marketing

BYOD offers an opportunity to improve the company's internal perception of IT's role and value. This is a great opportunity for internal marketing of both the company's mobility strategy and the IT team responsible for its implementation and support. Many organizations don't realize the value of this until well after the BYOD program is instituted. The components include:

- *Communicating why the company is moving to BYOD:* Is the desired perception "to shift the cost burden to the employee" or "to let employees use their favorite devices at work"?

- *Understanding **BYOD is an HR initiative as much as an IT initiative***: What is the desired impact on company culture, communication, and recruiting?
- *Defining IT's "brand":* Is IT a user advocate, an innovator, a source of best practices for mobile? IT can prove itself an end-user champion and ahead of the curve on technology through a BYOD program.
- *Supporting the brand message with appropriate action:* BYOD puts the burden on IT to provide a positive end-to-end experience to users, who need to easily understand the program, choose and provision the device, troubleshoot problems, and potentially migrate to new devices each year. The reality of the BYOD program needs to match its marketing.

BYOD gives IT a unique opportunity to impact perceptions, productivity, and culture across the company. Thinking through the internal marketing strategy up front will influence communications and decisions in a way that can improve IT's standing with its internal customers.

Conclusion

BYOD seems simple, but it's often not. Shifting the ownership of mobile devices has many complex implications for how a company conducts business, many of which have limited precedent. In this paper, we've discussed several considerations for building a program to address some of these issues. The initial adoption of the BYOD program will depend on effective preparation, while its long-term sustainability will depend on the ongoing quality of the employee's end-to-end experience. The goal of this paper is to provide an initial framework for that early preparation. BYOD holds tremendous promise across multiple dimensions. While many organizations look at BYOD as a possible way to reduce costs, the real value of a well-designed BYOD program is increasing employee satisfaction and productivity, while speeding up the rate of technology adoption in the enterprise.