10 BEST PRACTICES FOR IMPLEMENTING A SUCCESSFUL BYOD PROGRAM

The Bring-Your-Own-Device (BYOD) ownership model is no longer hype or a privilege of early adopters. According to Gartner, “By 2017, half of employers will require employees to supply their own device for work purposes”¹. Businesses everywhere have acknowledged the benefits that a BYOD model delivers – including improved user productivity, engagement and satisfaction as well as potential cost savings. According to the Enterprise Mobility Exchange², mobility projects are predicted to dominate the IT agenda in 2014. This increasing visibility of mobility projects at the CXO level raises the expectation of an on time, on budget delivery that meets business needs.

A large number of Good Technology’s global 5000 customers have embraced BYOD and shared their experiences with us. As a result we bring you the top ten best practices for the successful implementation of your own BYOD program.

1. Define Your Program Objectives and Get Executive Buy-in

Arguably the most important best practice is to identify specifically why you are moving to BYOD. Is it to reduce capital and expense costs? Or is it to provide tools for higher productivity? You then need to understand how many users need to adopt BYOD, and at what rate, to meet those objectives (for example, some Good customers have launched BYOD programs sponsored by Human Resources, primarily as a recruitment and retention tool).

Ensure that your executive sponsors are part of your objectives-definition process. This is crucial to securing the budget and people resources to see the project through completion, and to gain broad acceptance by the organization. With all the noise around BYOD over the past few years, it was not uncommon to see some early adopter projects fail because they didn’t have the right sponsorship or clear, measurable business objectives. By ensuring that the leaders of your company are behind the project, you can drive broader adoption.

2. Define Your Eligible BYOD Users

One common objective of a BYOD program is to increase employee productivity. While initial deployments may be limited to only highly mobile employees, sales professionals, doctors, executives etc., BYOD no longer needs to be the exclusive privilege of a few. There is an opportunity for every employee to benefit from the increased productivity, flexibility and efficiency that mobility offers. As demand for BYOD increases across the business, you can conduct a survey to understand the working patterns of your users—how much time do they spend working when mobile, what tasks do they perform when mobile, which apps do they need access to, what type of mobile device(s) do they use, do they travel internationally etc. The key insights from an end user survey can be used to measure interest in participating (especially if it requires switching from something they are already accustomed to such as a BlackBerry device), and to invite users to share any concerns regarding the program.

You should also work to understand the goals of the lines of business and determine if your user population will include only employees of the company, or if you also see value in extending the program to users in your extended enterprise such as partners, contractors, consultants etc. Understanding your users’ requirements early on in the process will help you design a solution for maximum adoption and hence increased productivity and satisfaction. Also, if your users are part of your solution definition process, they will be much more inclined to comply with the policies you put into place to manage your BYOD implementation.

3. Define Your Acceptable Use Policy

Privacy is an increasing concern of all mobile users. Our recommendation is to move beyond MDM-only solutions, which tend to compromise user privacy, to a secure container-based solution that provides clear partitioning between corporate and personal data, thereby maintaining user privacy. A well-defined policy should not constrain usage of any personal data, apps or other content since the users own their devices. As a best practice, involve a cross-functional team of IT, business stakeholders, finance, global privacy, security, human resources and legal in the creation of your acceptable use policy.

Will you wipe the entire device if it is lost or compromised, or just your corporate information? The best practice is for your corporation to typically limit itself to managing just the corporate data (as opposed to the personal data) on a personally owned device, up to and including wiping it. However, if your intent is to wipe the entire device, including personal data, you should provide prior disclosure and gain consent by the user. Such intent typically needs to be justified with compelling business and security reasons.

Other questions to consider include, will the same employee policy also apply to contractors and consultants? What are the repercussions if a user is out of policy? We recommend that an affirmation of compliance with the Acceptable Use Policy should definitely be a condition for participating in the BYOD program. The definition of a robust, easy to understand policy is a critical step in implementing a successful BYOD program.

4. Create a Communication Plan for Your Policy

The effectiveness of any end user Policy is measured by its adoption. End user policy documents are often lengthy and filled with legal jargon. As a result, users tend to accept the terms without really reading the policy or understanding its implications. Just as likely, users may resist adopting BYOD because they view the policy as heavy-handed or onerous. To ensure policy compliance, you should implement simple, repeated end user communication and training. The communication should describe the policy T's and Cs, eligibility criteria, approval process, availability dates, training and other helpful resources your users can take advantage of.

5. Identify a Pilot

The proliferation of mobile devices among your user base may tempt you to roll out a BYOD program across the board, all at once. Our recommendation is to resist that temptation and instead identify a pilot to roll out the solution. The pilot will provide invaluable insights to potential barriers to user adoption; incremental training and IT readiness and also help you gauge if the benefits are aligned with your defined goals. Ensure that your pilot program has crisp objectives, and roll it out to a select user base that is committed to offering feedback. Also ensure that the schedule is tightly managed so that you are able to incorporate feedback and move to a production scale deployment in a timely fashion.

6. Decide Which Devices You Want to Allow

Users today have a significant choice available in device OSes and form factors. If the goal of your BYOD program is to implement business transforming mobile apps while offering users the flexibility of device choice, then a best practice is to publish a recommended list of devices that will be optimal both for the user's job profile and also the apps they will be using. The user profile information you gather early on in the process will help you arrive at an informed decision with regards to recommended devices. An important point to note is that the three popular mobile OSes today– iOS™, Android™ and Windows Phone™, each offer different device-based security and encryption solutions, as well as different user experiences. Given users today have the opportunity to switch often between mobile devices, a best practice is to ensure that your security posture as well as mobile app experience is not tied just to the device and that it stays consistent across all devices.
7. Negotiate Mobile Service Rates With Carriers

Before your employees start to rely on their mobile devices to get work done, now is a good time to negotiate favorable rates with your preferred mobile carriers - for both consumer voice and data plans - in order to make the transition to BYOD at least cost-neutral to employees. You may not even need to offer employees a stipend. Due to competitive pressure to drive down service plan costs, we have seen users with old data plans actually save money by moving to BYOD and upgrading to a better but less expensive plan, all with no stipend. In fact, Gartner predicts that by 2016, the average amount a qualified employee currently receives for the business use of a personal smartphone will be reduced by 30%³. You can then track program adoption and potentially consider adding a minimal stipend if you want to accelerate adoption.

8. Define Your End-user Support Model

With a BYOD deployment, IT can successfully pass the cost of the device to the end user. However, offloading the burden of end user support may not be as easy, especially if, for example, that end user is a senior executive who stops receiving his or her email on their personal iPad™. Often, any cost savings resulting from lowered mobile device costs may be offset by a corresponding increase in mobile app support costs. In order to manage support costs in a BYOD deployment, you should assess if you have the right staff and expertise on hand to support the growing number of users. Other best practices include the implementation of a self-service model and offering IT support on all corporate sanctioned apps for corporate sanctioned users (could include employees as well as contractors, consultants etc.) The pilot program you put in place should validate your assumptions regarding user training and IT support and help you scale your deployment.

9. Define Your Mobile App Strategy

To gain maximum value from your BYOD implementation, you need to provide your users with the right set of corporate apps that help them stay productive wherever they are. The choice of corporate mobile apps should be defined by your business objectives and the profiles of your users (field technicians, office staff, sales personnel etc.) For example, you can choose to invest primarily in off-the-shelf horizontal apps such as email, file sharing or a secure browser or you can build and deploy a suite of custom apps that enable powerful mobile workflows. In either case, the apps should be easily accessible and simple to use without compromising user privacy or corporate security. As the number of mobile apps increases, a best practice is to invest in an enterprise app store to allow for easy distribution and lifecycle management of the apps.

If you implemented a BYOD program primarily for cost saving, you can reinvest those savings towards your mobile app strategy. Also the mobile app licensing model should be tied to the user and not to the device, since each user may carry more than one device (for example both a smartphone and a tablet). Upfront planning and budgeting for your mobile app purchases, and then monitoring the usage of those apps will help you gain the maximum value from your mobility investment while keeping costs on track.

10. Monitor Program Usage

Define in advance the success metrics of your BYOD program to align with your business goals. But be prepared to experience unforeseen benefits in other areas such as offering easier access to remote specialists, faster time to market as users can collaborate easily from anywhere or a lowering of paper costs by migrating critical processes to mobile workflows. You can also monitor the satisfaction and improved engagement of your users by tracking app downloads and reviews once they have started to participate in the program. Use these metrics to drive broader adoption and implement process improvements across the organization. Widely communicate the success metrics especially to your executive sponsors in order to ensure continued investment to drive business impact.

CONCLUSION

Implementing a BYOD program is a stepping-stone towards a broader, more strategic mobility initiative, and a successful mobility deployment can have a truly transformative impact on the business. Take advantage of these best practices to get maximum benefits from your BYOD implementation. You can also visit Good.com for additional BYOD success stories.

ABOUT GOOD TECHNOLOGY

Good Technology is the leader in secure mobility, providing the leading secure mobility solution for enterprises and governments worldwide, across all stages of the mobility lifecycle. Good’s comprehensive, end-to-end secure mobility solutions portfolio consists of a suite of collaboration applications, a secure mobility platform, mobile device management, unified monitoring, management and analytics and a third-party application and partner ecosystem. Good has more than 5,000 customers in 184 countries, including more than 50 of the FORTUNE 100™ companies. Learn more at www.good.com.