ENTERPRISE BYOD BEST PRACTICES

POLICY AND SECURITY BEST PRACTICES FOR A SOUND ENTERPRISE MOBILITY PROGRAM

BYOD, Bring Your Own Device, is a rapidly growing trend in which employees use their personal mobile devices such as smartphones, laptops, and tablets to do work-related tasks. Businesses that have begun supporting BYOD programs in the workplace have found not only are they able to protect and secure their data but also that there are significant benefits. This white paper details the benefits of this trend, and provides best practices for developing successful BYOD program policies and creating proper security measures.

BitzerMobile™
simplifying enterprise mobility

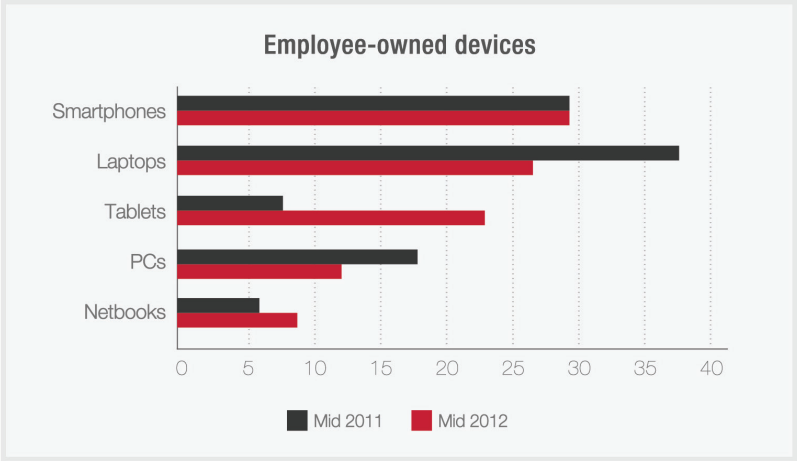
WHY BRING YOUR OWN DEVICE?

BYOD, Bring Your Own Device, is a recent and rapidly growing trend in which employees use their own personal computing devices such as smartphones, laptops, and tablets to do work-related tasks.

The BYOD phenomenon began as soon as easy-to-use mobile devices became ubiquitous. Initially, business leaders saw the development as a threat – when employees use their own devices instead of corporate issued devices for work, companies lose control of how devices are used, what they are used for, and, most critically, how company data is secured. Many organizations soon realized, though, that personal devices would continue to flood the workplace and, rather than fight it, they began to embrace it with comprehensive policies and security measures designed for a BYOD environment. These companies are thriving while also enjoying the advantages of enterprise mobility.

By being proactive with BYOD, businesses can maximize the benefits and minimize the risk of a trend that's here to stay.

Among the many companies that have embraced BYOD, are those belonging to some of the most highly-regulated and security-conscious industries. Large companies from the Finance/ Insurance and Healthcare industries dominate the BYOD landscape, but it is expected that Retail/ Wholesale and Government industries will soon get on board.



Businesses that now support BYOD programs have found not only that they are still able to protect and secure their data but also that such programs offer significant benefits. When employees use their own devices for work, companies are often able to reduce costs, keep up with new technology, and have a more satisfied and productive workforce. By being proactive with BYOD – by developing a program that includes comprehensive policies and well-considered security measures – businesses can maximize the benefits and minimize the risk of a trend that's here to stay.

THE BENEFITS OF BYOD

BYOD need not be seen as a development that is unfortunate, yet inevitable. In fact, BYOD has much to offer. With a BYOD program, employers are often able to reduce costs. But more importantly, they are better able to keep up with new technology and cultivate a more productive and satisfied workforce.

Cost savings

Cost savings is always a priority in business, and BYOD can certainly save employers money. While there are costs associated with securing corporate data on the mobile devices, these are consistent across all models of deployment.

Mobile Email Replacement

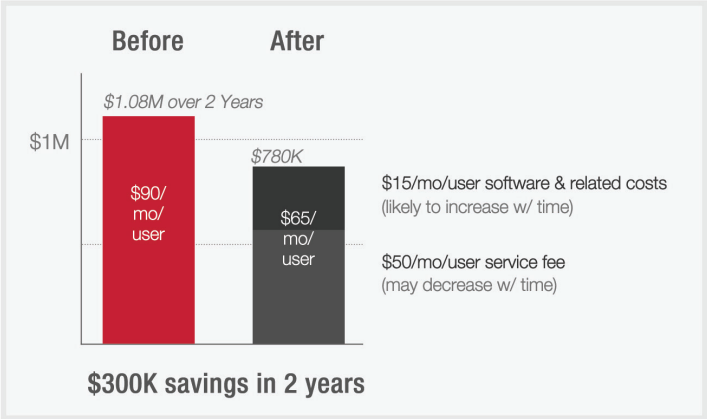
A company can save money with a BYOD program when their workforce deploys its devices in a somewhat limited manner. When mobile devices are used primarily for calendaring and messaging, a company can see a 30% cost savings. According to Gartner's analysis, the typical company owned device costs the business $90 per user for voice/data/text capabilities. On the other hand, with BYOD, company expenditures for the same level of service will be around $65 per user.

According to Gartner, companies save approximately $25 per user by adopting a BYOD program.

Flexibility of Expense Models

Organizations can also save money with BYOD, if they follow a partial reimbursement or "buy your own" policy. While the idea of allowing employees to use personal devices for work is fairly straightforward, there is no one model for who pays for the device or service. Some companies pay for employee devices, usage fees, and provide support; some provide stipends or reimbursements for hardware and monthly usage fees; and others require employees to cover all costs associated with the device and its use.

In some situations, employees are so delighted to be able to use their own devices for work that they will do so even when they have to cover all costs on their own. However, employee buy in is higher when companies share the expenses. Either way, when employees contribute to device and voice/data expenses, a company can save significant money.



Lowering the Cost of Ownership

Even when businesses opt to cover the entire expense of employee devices and monthly service, they can still see reduced costs in the form of lower cost of ownership. Traditionally, IT departments have spent substantial time and money sourcing, purchasing, managing, training, and supporting the devices they supply to employees. In that model, such activities become the department's main function, especially in light of the how quickly technologies change.

In contrast, when employees supply their own devices, IT departments are no longer overwhelmed by those tasks. Sourcing and purchasing are in the hands of the employee, and, with the proper policies in place, management, support, and training responsibilities are greatly reduced as well. Moreover, larger companies can sometimes leverage their size to secure discounts for employees, even when they are buying individually and not in bulk. BYOD can save IT time and money and enable the department to focus on improvements and innovations that can benefit the company as a whole.

Under certain circumstances, a BYOD program can save businesses money. But cost savings is not the biggest advantage of BYOD, and it is not the reason most business leaders are choosing to support it. In fact, only 10% of IT leaders look to BYOD as a way to reduce costs (Gartner). Rather, the greatest advantages of BYOD are that it enables businesses to keep pace with new technology, it promotes employee satisfaction, and it improves productivity.

Keeping Pace with Technology

Times have changed and these days, consumers, not businesses, are at the cutting edge of technology. Device features and capabilities and the devices themselves change so rapidly and frequently that organizations are hard pressed to keep pace. Consumers are not plagued by this problem; in fact, consumers are frenetically and voraciously in step with every new technological development. By welcoming BYOD into their business environment, companies can take advantage of the best and newest technology without necessarily investing capital.

The greatest advantages of BYOD are that it enables businesses to keep pace with new technology, promotes employee satisfaction, and improves productivity.

Employee Satisfaction

Users spend hard-earned money on the smartphones, tablets, and laptops they own for a reason – they have chosen the devices they prefer and what works best for them. It makes sense that they would rather use their own devices for work than the computing device selected and supplied by their company. Enabling employees to make their own choices builds morale and improves employee satisfaction.

Employee satisfaction is increased with all mobility deployments because of the freedom it offers. Employees that need to work from different sites, while travelling, or from home are able to do so efficiently and easily with their mobile devices. When employees can effectively do their jobs when and where they need to, they are more content with their work and with their employer.

Increased Productivity

BYOD can improve productivity in a variety of ways. When employees are using devices that they have chosen, they are using what is familiar to them and what works best for them. This can increase output. Productivity can also be improved because of the mobility BYOD offers. When employees can work effectively from any location – while on the road, at home, etc. – productivity goes up. Moreover, many opportunities arise when workers are no longer bound to a single desk while at the office. If employees can work anywhere in the office, there can be closer collaboration between individuals and teams, opportunities to organize temporary projects between different segments of the workforce, meetings where everyone can log in to the network, and more. With a BYOD program, businesses can reap the rewards of increased productivity.

Unexpected Costs

BYOD can certainly save businesses money, but it can also introduce unexpected costs.

Excessive Charges for Usage and Roaming

Employees are using their mobile devices more and more and many of them are using multiple devices. Indeed, the average smartphone usage nearly tripled in 2011, and each tablet generated nearly 3.5 times more traffic than the average smartphone. And, the typical mobile employee uses 3.5 devices to do his or her work (ComputerWeekly.com). Moreover, many employees frequently travel internationally and use their devices liberally, in spite of costly roaming charges. All of these circumstances can lead to unexpected and shockingly high bills at the end of the month.

To avoid such problems, companies with BYOD programs should help employees manage data use. Companies may want to track in-network and roaming data usage and notify users with alerts. It is also worthwhile to encourage users to use Wi-Fi whenever it is available.

Taxes on Stipends or Reimbursements

Another potential and unforeseen BYOD expense comes from government taxation. Some countries consider stipends and/or reimbursements to be taxable income. Thus, when businesses opt to share device and usage expenses with employees living in these countries, they can be hit with a tremendous tax bill. Companies should look carefully into the tax laws of the countries in which their employees work to ensure this does not happen to them.

Other potential unanticipated costs include hosted virtual desktop costs and licensing fees. Companies should take all of these potential expenses into consideration as they develop a BYOD policy.

BYOD POLICY BEST PRACTICES

BYOD entails more than just a simple shift in device ownership. It involves complex and diverse factors and can have unforeseen effects; therefore, businesses must develop a well-considered, comprehensive BYOD policy before onboarding the practice. The following check list will help you navigate the complexity, avoid the hazards, and develop a BYOD policy that works.

"...studies have shown that a staggering 73% of enterprises have non-IT managed devices accessing corporate resources..."

ComputerWeekly.com

Define your BYOD Strategy

As with most successful projects, it is best to begin with the end in mind.

- ❑ Define the goals for your program.
- ❑ Identify stakeholders.
- ❑ Determine your criteria for selecting a solution.

Attend to your Bottom Line

When crafting your BYOD policy, consider how it will impact ROI.

- ❑ Compare costs of traditional company-owned approach with BYOD model.
- ❑ Shift some or all device hardware costs to users.
- ❑ Set controls to prevent service charges.
- ❑ Determine appropriate service plans.
- ❑ Reduce help desk involvement – encourage and provide tools for self-support.
- ❑ Enable self-service for device enrollment, data use tracking, etc.
- ❑ Assess tax implications.

Compare Approaches

Company-owned	BYOD
• Cost of fully subsidized data plan	• Savings from eliminating device purchase or • Cost of partially subsidized device purchase
• Cost of warranty plans	• Cost of a partially subsidized data plan or • Savings from eliminating data plan responsibilities
• Cost of each device	• Cost of mobile information management tools
• Cost of recycling dated devices	
• Cost of managing program	

Program Basics

- ❑ Create a tiered policy that reflects the different ways that devices are used by diverse user types.
- ❑ Specify who qualifies for participation in program.
- ❑ Create a simple enrollment program.
- ❑ Develop BYOD policy with user input and thoroughly educate all participants on company expectations.
- ❑ Regularly disseminate minimum specifications and requirements (e.g. supported operating systems, storage requirements, minimum processing speeds, screen size).

Devices & Applications

- ❑ Evaluate employee preferences and assess which devices they already own.
- ❑ Specify what devices are allowed.
- ❑ Choose devices, platforms, and architectures that are easy to support.
- ❑ Design applications for supportability.
- ❑ Specify applications and devices that are banned (e.g. rooting/jailbreaking apps, non-market apps, rooted devices).
- ❑ Specify required security control solutions (e.g. Mobile Information Management (MIM) tool).

Support

- ❑ Establish what devices and applications IT will support.
- ❑ Detail the types of incidents supported and the extent of support offered.
- ❑ Define and limit IT support parameters.
- ❑ Enable and encourage user self-support (e.g. educate users, create internal resources, provide links to external sources).

Rights & Responsibilities

- ❑ Establish who buys/owns the device.
- ❑ Establish who pays for use – employee, company, shared expense.
- ❑ Establish limits on usage.
- ❑ Establish what expenses will be covered, and how.
- ❑ Set limits on reimbursements.
- ❑ Define what happens in the event of an overage (e.g. who pays charges, policy for first offense).
- ❑ Establish device backup requirements and responsibilities.
- ❑ Specify who is responsible for installing required security control (e.g. MIM).

HR and Legal Matters

Employee Privacy

- ❑ Identify the activities and data that will be monitored.
- ❑ Identify the data you will not collect (e.g. personal emails, contacts, call history, test messages, application data).
- ❑ Identify the information you will collect, and why.
- ❑ Clarify what actions IT will take and under what circumstances (e.g. E-discovery issues – what happens when a personal device gets subpoenaed).

Other Legal Matters

- ❑ Communicate penalties for non-compliance.
- ❑ Establish parameters for after-hours communication (e.g. Are employees obligated to respond/act in response to an email received after hours?).
- ❑ Set procedures transferring data and phone number transition termination.

"Security issues around non-managed devices are on the rise - 46% of IT executives admit to experiencing a security problem related to an employee with an unprovisioned device."

ComputerWeekly.com

BYOD SECURITY BEST PRACTICES

As with BYOD program policies, well-informed security measures will ensure that your program is a success. The following list of best practices for BYOD security will help you keep your data safe and your employees content.

When companies take the reins of BYOD by developing a well-crafted comprehensive program policy and take appropriate security measures, they can enjoy the many rewards it offers.

Security Policy Basics

- Identify and assess risk for common security issues on personal devices – consider both device risks and application risks.
- Create policy that takes existing infrastructure and risk tolerance into account.
- Establish minimum security requirements for employee devices.
- Educate users about policy; regularly remind users of policies.
- Enforce policy actively and consistently.
- Identify a software solution that enables device and data management.

Protect Data

Use a security control tool that offers at least the following:

- Supports multiple devices families, operating systems, etc.
- Tight security policy control.
- Data encryption over air and on device.
- Remote data wipe and lock.
- Strong password protection enforcement.
- Classify data, and decide what class of data mobile devices can access.
- Establish plan for handling a data breach.
- Establish a backup policy.

Protect Device

- Establish user-access policies.
- Monitor devices regularly to ensure they are configured according to security policy.
  - Mobile Device Auditing solutions report on but cannot control device configurations.
  - Mobile Device Monitoring solutions report on and control device configurations.
- Establish plan for handling lost or stolen device.

SUMMARY

BYOD adoption rates are increasing not because the trend is unstoppable but because it offers true benefits for businesses. If left to grow organically without restrictions or oversight, the growth in personal devices can become unwieldy and potentially problematic. But when companies take the reins of BYOD by developing a well-crafted comprehensive program policy and take appropriate security measures, they can enjoy the many rewards it offers.

List of References:
Citrix, “IT Organizations Embrace Bring-Your-Own Devices,” BYO Index.
Bradley, “Pros and Cons of Bringing Your Own Device to Work,” PCWorld, http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html.
Hendrikse, “How to introduce bring-your-own-device schemes in the enterprise,” ComputerWeekly.com, http://www.computerweekly.com/opinion/Bring-Your-Own-Device-in-the-Enterprise.
Fox, “Top 10 Tips for Securely Managing Your Employee’s BYOD,” Infosec Institute, http://resources.infosecinstitute.com/tips-managing-byod-security/.
Gartner, “Bring you own Device Program Best Practices,” Gartner Webinars.
Good Technology, “Good Technology State of BYOD Report.”
“The Ten Commandments of Bring Your Own Device,” www.maas360.com

ABOUT BITZER MOBILE

BitzerMobile™
simplifying enterprise mobility

Bitzer Mobile brings the secure enterprise to mobile devices

Bitzer Mobile Inc., a leading enterprise mobility solution provider, enhances employee productivity by allowing secure access to corporate apps and data from mobile devices while preserving rich user experience. Its secure container solution creates the enterprise workspace on any mobile device – corporate owned or personal, and for all mobile platforms. Employees get seamless access to intranet, corporate data and apps with enterprise-grade security and deep integration with Windows Authentication for true Single Sign-On.

440 N. Wolfe Road
Sunnyvale, CA 94085, USA
www.bitzermobile.com
sales@bitzermobile.com
866.603.8392

bitzermobile