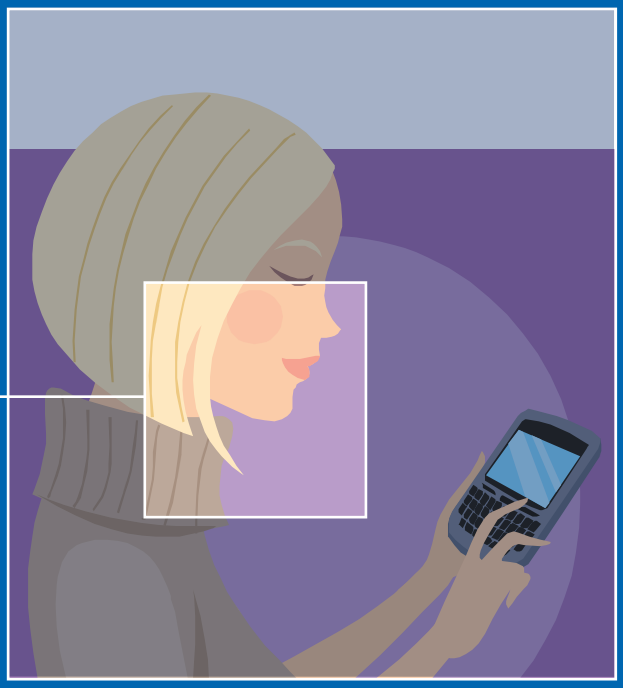
4imprint®

Blue Papers®



BYOD

4imprint.com

Bring your own device (BYOD) to work: How it can be a thirst quencher for your company

Bring your own device, or BYOD, isn't a beverage you bring to a party, it's the latest trend in the workplace. You probably know the drill, employees come to work armed with their own smartphones, computers and tablets and want them to sync to your organization. It's driven by the desire to have access to everything, when and where you want it. It blurs the line between personal and professional lives, and more and more, employees are bringing their own devices to get (and stay) linked into the corporation. And many companies are on board with the idea. According to research, 85 percent of organizations allow employees to bring their own devices to work.[1] By 2016, Forrester Research® estimates that 350 million workers will use smartphones and 200 million of them will take their own devices to work.[2] To further put this in perspective, a Gartner® study predicts that by 2016 more than 80 percent of employees will use their own equipment with employee data on board.[3]

Linking devices to company resources like email, file servers and databases is not only convenient, but it can be advantageous to both employees and corporations. When employees have 24/7 access to your organization with their own devices, it can improve productivity and operational responsiveness. As a bonus, employees get to work with the technology they already know, at any time they choose. Much like having guests bring their own drink to a party, implementing BYOD can save money, too. For this reason, nearly 70 percent of organizations express positive attitudes toward the trend.[4]

But how do you decide if BYOD is the right approach for your organization? The fact is that BYOD can cause big headaches for IT decision makers if approached in an ad hoc manner. Why? Because BYOD brings with it security risks and privacy challenges; opening your company up to more than you anticipated. It can also drain resources because syncing personal devices with company infrastructure such as servers and email is fraught with greater unknowns and variables.

---

1 *"The Definitive Guide to BYOD." N.p., n.d. Web. 25 Mar. 2014. <http://www.whitepaperwizard.com/resources/2860/the-definitive-guide-to-byod?js=1>.*

2 *"Bring Your Own Device (BYOD)." Http://www.cdw.com. Total Mobility Management, n.d. Web. 26 Mar. 2014. <http://www.cdw.com/content/solutions/mobility/byod-bring-your-own-device.aspx?utm_source=bing&utm_medium=cpc&utm_campaign=Mobility_BYOD&cm_ven=acquirgy&cm_cat=bing&cm_pla=Solutions-Mobility&cm_ite=NA&ef_id=UzL4IAAABDV7ATDo:20140326155408:s>.*

3 *"The Ten Commandments of BYOD." (n.d.): n. page. MaaS360. 2014. Web. 26 Mar. 2014. <http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf>.*

4 *"Bring Your Own Device (BYOD)." Http://www.cdw.com. Total Mobility Management, n.d. Web. 26 Mar. 2014. <http://www.cdw.com/content/solutions/mobility/byod-bring-your-own-device.aspx?utm_source=bing&utm_medium=cpc&utm_campaign=Mobility_BYOD&cm_ven=acquirgy&cm_cat=bing&cm_pla=Solutions-Mobility&cm_ite=NA&ef_id=UzL4IAAABDV7ATDo:20140326155408:s>.*

The goal is to exploit the benefits of BYOD while mitigating any potential risks. This Blue Paper® looks at the pros and cons of BYOD, and how companies can safely let employees use personal devices. It will help your organization identify critical technology and security issues, and provide tips on how to articulate an effective BYOD policy. You might want to consider adopting BYOD—do it correctly and it could be a real thirst-quencher for employees and the corporation.

The good news: advantages of BYOD

So what are some of the benefits of BYOD? According to research it can:

- enable access to better technology,
- improve productivity,
- boost employee morale,
- provide greater flexibility, and
- save energy.[5]

Since many companies can't afford to provide the latest tablets, smartphones and computers, BYOD is a cost effective way to provide employees access to better technology. If you have a small business in particular, buying new IT equipment or frequently upgrading existing technology can be financially challenging. Letting staff use their own devices cuts back on the money you spend to make sure your employees have the technology they need. Since 62 percent of 18-31 year olds and 54 percent of 32-45 year olds say the technology they have at home is better than what they have at work, BYOD is a cost affordable alternative.[6] Not only will your company save money by not having to purchase additional technology, but it might even give employees access to technology that otherwise is unaffordable.

BYOD can also boost employee productivity. People work faster, smarter and better when they use a device they are comfortable with. If you've ever had to switch to a new operating system, you know there's a learning curve that can be time consuming. If you are a Mac® user, for example, switching to a PC desktop platform can be frustrating and difficult. By using their own computer, employees don't have to waste time learning a new system, and as a result, they can hit the ground running.

In addition, BYOD strategies are believed to make employees happy while promoting greater flexibility in the workplace. Employees like using their

5 "BYOD Pros and Cons." BT Business. N.p., n.d. Web. 25 Mar. 2014. <http://www.insight.bt.com/en/features/byod_pros_and_cons>.

6 "The Great Divide: Mobile Workers Challenge IT Departments with Aggressive Use of Consumer Tech, Unisys-Commissioned Study Finds." N.p., 25 Sept. 2012. Web. 31 Mar. 2014. <http://www.unisys.com/unisys/news/detail.jsp?print=true&id=1120000970023710222>.

own devices because it provides a sense of familiarity that enhances the work experience, letting them work where and when they want. It goes without saying that happy employees lead to increased morale, which in turn contributes to a positive working environment. If you operate in a business to consumer (B2C) environment, it's particularly helpful for employees to use their own devices during evenings and weekends, especially if your company requires 24/7 customer service.

Have you thought about energy consumption? Since desktop computers use eighty-five percent more energy over the course of a year than laptops or tablets, you might also see an energy savings associated with BYOD.[7] Plus, with a BYOD policy in place, employees may have the flexibility to work from home, contributing to overall energy savings across the company.

The bad news: BYOD has a downside

Despite the benefits, there can be a downside to BYOD. If you aren't careful, BYOD can:

- become a financial liability if costs are not identified upfront;
- jeopardize data security and privacy; and
- put corporate data at risk when employees leave the organization.

These risks are significant, and companies need to develop strategies that mitigate the negatives. In fact, some companies shy away from BYOD due to complications that can result. A survey from the UK-based company Dimension Data® found that more than 70 percent of respondents said that their business leaders view employee use of personal mobile devices as potentially dangerous, costly and not business critical.[8]

While there are some cost incentives to BYOD, if you don't plan accordingly, hidden costs can add up, thus mitigating any cost savings. Therefore, it's important to budget for BYOD implementation and maintenance to eliminate any surprises. Keep in mind you might need to hire more employees to manage BYOD or purchase additional software for maintenance and implementation. Research finds that 61 percent of those that adopt BYOD had to hire additional IT resources to manage the trend.[9] Another 67 percent of companies say that

7 Williams, Mike. "Do Laptops Save on Electricity Bills?" Home Guides. N.p., n.d. Web. 25 Mar. 2014. <http://homeguides.sfgate.com/laptops-save-electricity-bills-79721.html>

8 Ashford, Warwick. "Enterprises Struggle with Security Challenge of BYOD, Study Shows." ComputerWeekly.com. N.p., 16 Oct. 2013. Web. 26 Mar. 2014. <http://www.computerweekly.com/news/2240207325/Enterprises-struggle-with-security-challenge-of-BYOD-study-shows>.

9 "BYOD: Is Your Company Safe?" Whitepaper Wizard, n.d. Web. 27 Mar. 2014. <http://www.webroot.com/shared/images/byod-security-infographic.jpg>.

BYOD management of mobile device security is a great burden on IT resources.[10] On average, a company spends 57 hours a month managing mobile devices and security, so it's important to set aside funding to support BYOD and adjust as needed for ongoing maintenance.[11] By identifying the extra costs associated with implementing and maintaining a BYOD policy you can avoid surprises and prevent BYOD from becoming a financial liability.

Data security is another concern associated with BYOD—corporate data can be compromised if you aren't careful. Suddenly, your corporate data is on multiple devices and you don't know how it's being used. Worse yet, what if an employee loses his or her device and suddenly your intellectual property lands in the hands of strangers? According to an infographic from the WhitePaper Wizard, companies report that 45 percent of security risks are due to lost devices.[12]

In addition, privacy is a serious concern with BYOD for both the company and employee. Employees, for instance, might worry that personal information on devices can be accessed by employers. Since the computer they use for work is the same as the home computer, employees fear that the organization is able to "spy" on their activities or see how much they log into sites like Facebook® and Twitter®. They also might worry about a company obtaining their private documents. Meanwhile, the company fears that its privacy might be violated, too, as emails may be read by anyone that has access to technology at home. When the line between personal and professional life is blurred, employees and corporations tend to get nervous.

An even greater concern is what to do when an employee leaves an organization. Unless you have a plan in place, employees might still have access to proprietary information and documents even after they're gone. But most companies don't have any mechanisms in place to recoup data on personal devices. In fact, the study from Dimension Data® surveyed more than 1,600 information technology and security professionals across 22 countries and found that 90 percent of organizations that allow BYOD do not have the capability to stop employees from using personal devices to access corporate systems after they leave.[13] It's a big concern, because intellectual property and proprietary knowledge stay on personal desktops long after the employee departs. At a minimum, companies should disable email or synchronization access as part of the employee exit interview. Some companies are taking it a step further and demanding that they have the ability to do a complete wipe on personal devices as part of the mandatory exit strategy.

10 Ibid.
11 Ibid.
12 Ibid.
13 Ashford, Warwick. "Enterprises Struggle with Security Challenge of BYOD, Study Shows." ComputerWeekly.com. N.p., 16 Oct. 2013. Web. 26 Mar. 2014. <http://www.computerweekly.com/news/2240207325/Enterprises-struggle-with-security-challenge-of-BYOD-study-shows>.

Technology and security: The foundation of successful BYOD

But first things first, if you are planning to allow BYOD, you need to start by examining the technology requirements to support BYOD. The technology landscape is critical, because as mentioned, the BYOD trend brings a host of issues concerning enterprise network and data security. Corporate users (e.g. employees or contract personnel) access networks and data and can bypass corporate controls using personal Wi-Fi devices. Uncontrolled access can lead to bigger problems, like data leaks, exposure to malicious software (also known as malware) and misuse of corporate data.

How big is the risk? According to research, malware in Android® mobile operating systems grew by 33 percent last year.[14] Other research claims that at 24 percent of BYOD companies, security risks were incurred due to the presence of malware.[15] If employees unknowingly download malware on personal devices, it can manifest in corporate systems, causing important business information to be stolen or lost.

To get started, you need to assess the capabilities of your current technology. The truth is that most companies are not equipped to immediately offer BYOD and must purchase additional software and tools that can support it. Chances are, even if you do have BYOD resources they might need an upgrade. You will also need to determine where data from BYOD devices will be stored (e.g. locally or in the cloud) and outline what technology resources are required to implement and maintain BYOD.

Once you've addressed the basics, it's time to roll up your sleeves and get to work, because implementing security measures and mobile protection is perhaps the single most important facet of a BYOD strategy. There are a number of best practices to follow, and experts suggest that at a minimum companies should:

- use mobile device management (MDM) software;
- create approved application lists;
- enforce password-protected access controls; and
- use remote-wipe services.

In order to reduce security risks, experts suggest companies invest in a mobile device management (MDM) software. By implementing MDM, IT teams can

14 "Tips for Mitigating BYOD Security Risks." Tips for Mitigating BYOD Security Risks. N.p., n.d. Web. 21 Apr. 2014. <http://www.baselinemag.com/security/tips-for-mitigating-byod-security-risks.html>.

15 "BYOD: Is Your Company Safe?" Whitepaper Wizard, n.d. Web. 27 Mar. 2014. <http://www.webroot.com/shared/images/byod-security-infographic.jpg>.

implement security settings and software configurations on any devices that connect to company networks. MDM software also provides secure client applications such as email and Web browsers, Web device application distribution, configuration, monitoring and remote wipe capability. Since the use of mobile devices continues to grow, there are a lot of vendors to choose from and applications are frequently updated to protect corporate data in conjunction with BYOD policies. It's not a bad idea to double check and make sure your company is utilizing the latest and greatest tools and to add additional security if it's available.

When selecting MDM software it's important to make sure it supports more than a single platform, so that whether employees use an iOS or Android system, the data is protected. Fortunately, there are a number of MDM software packages that can do the trick. For example, the Enterprise Mobility Suite offered by Microsoft® is a comprehensive cloud solution that can help companies support BYOD. Other vendors have developed products designed to manage mobile devices and promise to do everything from detecting and blocking devices, while providing the ability to control and audit usage. PingAccess®, for example, helps companies manage mobile access and provides an application programming interface (API) to control and audit access to Web applications. If you need help choosing the right MDM, review a summary on the top 10 mobile device management suites published by technology leader ZDNet®.

To further protect security, companies should arm employees with an approved application list and encourage compliance. A survey conducted by Forrester found that 15 percent of users have downloaded unauthorized applications to their work computers in the past year.[16] Of those users, 67 percent have used two to five unauthorized applications for work and 39 percent said they use those apps daily or several times a day.[17] This is a huge concern because malware and rogue applications can cause serious damage without users realizing it. For this reason, it's important to explicitly identify approved applications and communicate that applications not on the list are prohibited. Some companies allow employees to download unapproved applications, but only once it's vetted by the IT department. Although it might be difficult to enforce and monitor application downloads, at least employees will know what to avoid if they want to keep using personal devices for work.

16 Brousell, Lauren. "Numbers You Need to Know: Employees Take Tech to Work." CIO. N.p., 12 May 2011. Web. 31 Mar. 2014. <http://www.cio.com/article/682225/Numbers_You_Need_to_Know_Employees_Take_Tech_to_Work>.

17 Brousell, Lauren. "Numbers You Need to Know: Employees Take Tech to Work." CIO. N.p., 12 May 2011. Web. 31 Mar. 2014. <http://www.cio.com/article/682225/Numbers_You_Need_to_Know_Employees_Take_Tech_to_Work>.

Password protection is another must-have to safeguard corporate data, and the device should lock after a certain number of failed attempts. Passwords should be unique for each user and device, and refreshed periodically by device owners. Since most users do not require a password or locked screen option on their devices, anyone could check their computers or phone, putting your corporate data at risk. By making it a requirement, it will be harder for others to easily access information. For many companies, it's not considered unreasonable to ask employees to adopt this as a practice if they want to use personal devices for work.

Finally, it's a best practice to include remote-wiping capabilities that can remove data when an employee leaves or when the device is lost or stolen. As previously mentioned, 45 percent of companies reported security risks from lost devices, so it's critical to have a plan that prevents data from falling into the hands of strangers.[18] Most MDM software packages include remote-wiping capabilities to help keep corporate information secure.

BYOD guidance for employees

After you've addressed technology requirements for BYOD, it's important to define the usage guidelines, especially since you may not be able to stop employees from using their personal devices for work. A Forrester® study revealed that 37 percent of employees are doing something with technology before formal permissions or policies are instituted.[19] Therefore, it's best to create formal usage policies before employees start adopting BYOD without any guidance.

Guidelines will let employees know exactly what is expected if they choose to bring their own devices to work. After a usage policy is communicated, employees should sign off on the corporate policy so there are no misunderstandings. Specifically, employee guidelines pertaining to BYOD must:

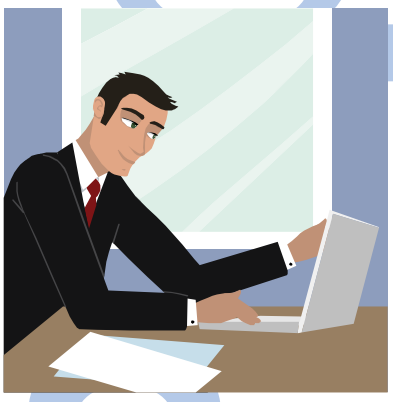
- articulate what the company means by BYOD and what devices are permitted;
- decide whether or not employees can link devices if it's not critical to do their job;
- outline a service policy for personal devices (e.g. who will maintain it if something goes wrong);
- make it clear who owns what apps and data (the company versus employee);

18 "BYOD: Is Your Company Safe?" Whitepaper Wizard, n.d. Web. 27 Mar. 2014. <http://www.webroot.com/shared/images/byod-security-infographic.jpg>.

19 "The Ten Commandments of BYOD." IT Business Edge. N.p., n.d. Web. 31 Mar. 2014. <http://www.itbusinessedge.com/slideshows/the-ten-commandments-of-byod-02.html>.

- address privacy issues;
- provide employee training;
- integrate the BYOD plan with the corporate acceptable use policy; and,
- articulate the consequences of BYOD misuse.

First, companies need to clearly outline what is meant by "bring your own device." Does it apply to everything, including iPhones® and Androids? Will you allow the use of all tablets, or will your organization only support iPads®? Companies also need to decide if you want to restrict the number of devices employees use for work. Research shows that 43 percent of workers use three or more devices and that means corporate data has triple the risk of exposure.[20] For this reason, it's common practice to restrict the number of personal devices.



Also, do you want to deny employees the use of personal devices if access to critical data is not required for their job? 72 percent of IT executives surveyed by Forrester® Consulting say that employees are making use of unsupported devices or apps because of personal preference, not because they need it to do critical work.[21] Along these lines, 68 percent of tablet users and 63 percent of smartphone users say that convenience is the reason they use personal devices for work.[22] If that is the case, companies might choose to limit access to certain servers and applications.

It's also important to define clear technology service policies regarding BYOD. This will ensure that employees understand the boundaries when questions or problems arise with personal devices. Some of the questions you might want to answer in your employee service policy include:

- What type of support will be available to employees for initial connections to the company network from personally-owned devices?
- Will information technology help employees troubleshoot issues that arise with personal devices?
- What (if any) support will in-house IT provide for broken devices?
- Will you provide support for applications installed on personal devices?
- Will you provide loaner devices for employees while their phone or tablet is being serviced?

These questions outline the limits of BYOD and what the company will support. Most companies do not provide ongoing service for personal devices, simply because it can be time consuming and costly. In many cases, if something goes wrong with an employee's iPad or phone, it is up to the employee to find a solution.

20 "The Great Divide: Mobile Workers Challenge IT Departments with Aggressive Use of Consumer Tech, Unisys-Commissioned Study Finds." N.p., 25 Sept. 2012. Web. 31 Mar. 2014.
21 Ibid.
22 Ibid.

It might seem obvious, but companies must also provide clarity on who owns what apps and data. Clearly, your company owns information stored on servers that employees access with devices, but problems arise if the employee leaves and you have to wipe the device clean. Devices often store personal pictures, music and applications by the individual, but these things are lost when you reset or wipe the device. It's not a bad idea to provide guidance on how employees can back up personal content so they can restore personal information if the phone or device is wiped clean.

Privacy is another issue to address with employees when embarking on BYOD. For example, will employees relinquish a certain amount of privacy when they use their own devices? Can companies have full access on employee devices? In reality, some companies choose to have access to employee devices at any time if it houses corporate data. If you choose to do this, let employees know from the beginning that they may need to forsake a certain amount of privacy.

Providing training on BYOD policies is another critical activity. Training can help employees troubleshoot issues associated with BYOD and enforce acceptable use policies. At the very least, make sure employees know that even when they are using personal devices they still need to follow the corporate acceptable use policy. Generally, an acceptable use policy is a list of rules applied by the employer that restricts the ways in which the network, website, or system may be used. Make sure you review this policy with BYOD users so that you are on the same page. If nothing else, remind them that same rules in the office apply, whether you are using a business or personal computer.

Finally, it's a good idea to educate employees on the consequences of a BYOD violation. Articulate the violation penalties so that employees know what to expect if they use corporate data inappropriately. For some organizations, a violation might mean discontinued use of personal devices. But according to a report from Forrester Research, the simple statement of a penalty often deters misuse.[23] When employees are aware of consequences there's a greater likelihood of BYOD compliance.

BYOD and beyond

Managing BYOD is an ongoing process, and one that will require diligence to be successful. Even after you've implemented BYOD policies and technology, it's a good idea to constantly revisit policies and technology to identify what's working and what isn't. If network security has been compromised, you'll need to identify

23 Burnham, Kristin. "Social Media Safety: Acceptable-Use Policies Critical." CIO. N.p., 9 Apr. 2010. Web. 10 Apr. 2014. <http://www.cio.com.au/article/342471/social_media_safety_acceptable-use_policies_critical/>.

the root cause and make adjustments. It's also a good idea to consult with IT to make sure BYOD resources are sufficient and determine if more resources are required. Policies might need to be revisited if the same issues keep popping up, so make sure you constantly review and monitor your BYOD strategy.

Ready to adopt BYOD?

Research convenes on one major point—bringing your own device to workplace will only grow in the upcoming years. And while the benefits of BYOD are clear, it's not something that can be haphazardly implemented. Companies must develop practices to manage BYOD and ensure data security. It's also critical to clearly develop and communicate polices regarding use and maintenance to prevent misuse or misunderstandings. In the end, guests might prefer the practice of BYOD, but it needs to be served in a manner that is mutually beneficial for both employees and corporations.