

# Overcoming the Challenges of BYOD [Infographic]

DE Brown April 20, 2017



The BYOD (Bring Your Own Device) phenomenon is steadily gaining in popularity. Employees are so fond of using their personal devices that many do so with or without the IT department's permission.

([Newswire.net](http://Newswire.net) -- April 20, 2017) -- Nearly 18 percent of respondents in one survey reported taking their devices to work though they knew IT was unaware of it. Over 28 percent of IT departments actively ignore unregulated BYOD activity themselves, which only encourages this behavior.



## CHALLENGES OF BYOD

BYOD (Bring Your Own Device) programs are becoming increasingly popular in the workplace.



Companies can **slash their tech expenses** by allowing employees to use their own devices, while employees enjoy the convenience of such programs which let them keep both business and personal communications in one place.

BYOD adoption is estimated between **40%** and **75%**.

*Prepare your company to join the trend by*

Prepare your company to join the trend by carefully considering these top factors...



## PROBLEM



Less than **1 IN 4 DEVICES**  
**CAN BE REMOTELY WIPED.**



Though **50%** of organizations believe it's important to register devices, only **32%** require it.

## SOLUTION

**USE A MOBILE SECURITY MANAGEMENT SUITE.**



Top mobile device management software programs allow:



Remote  
Wipe



Enterprise  
Wipe



Remote  
Lock



Role-Based  
Authentication

## PROBLEM





Device use is **HIGHLY UNREGULATED** in many instances.



**17.7%** of survey respondents who take their devices to work report that their IT department is unaware.



**28.4%** of IT departments actively ignore unregulated BYOD activities.

## SOLUTION

**IMPLEMENT A DETAILED BYOD POLICY AND REQUIRE ALL EMPLOYEES TO SIGN IT.**



Smart provisions include:



Restrictions on permitted apps



Requirements for disabling the camera on the premises



Stipulation of acceptable smartphone models and operating systems



## PROBLEM



PRIVACY



Employees have a strong desire to **SEGREGATE PERSONAL AND PROFESSIONAL INFORMATION** on their devices when using a BYOD program.

## SOLUTION

**DRAFT A BYOD POLICY THAT CLEARLY DEFINES HOW THE COMPANY WILL TREAT PERSONAL DATA. EXPLAIN:**



Under what circumstances the company will view personal data



Whether personal data will be wiped with company data in necessary circumstances



How much notice is required before wiping data



Make sure the **corporate legal** department and **IT** are involved in drafting this documentation and explain it clearly to employees.

With **smart preparation** and a **mindful approach** to the common challenges of BYOD, you can successfully transform the way your company manages business devices.



## RESOURCES

<http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards>

<http://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software-of-2016>

<https://www.sans.org/reading-room/whitepapers/analyst/survey-mobility-byod-security-policies-practices-35175>

<http://www.securitymagazine.com/articles/87016-bring-your-own-risk-with-byod>

<http://www.itmanagerdaily.com/byod-policy-template/>

<https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx>

<http://www.leoncosgrove.com/labor-employment/bring-your-own-device-to-work/>

While BYOD can offer a smart way for businesses to cut the cost of company-provided smartphones, it's not without its risks. If you want to utilize BYOD, it's essential that you implement a clear policy for how employees can use their devices. Use a mobile security management suite to enable remote wipes and remote locks, protecting your data if a phone is lost or an employee quits. Specify which devices are suitable for BYOD purposes so your workers are using reliable smartphones and service providers like the [Apple iPhone SE on T-Mobile's network](#) rather than unsecure and outdated technology.

Clearly disclose the company's role in BYOD programs so employees know what data your IT department can and can't access. If you plan to track the GPS location of devices or use a keystroke logger, this must be disclosed to your workers so they know what level of privacy they have. A clear and [detailed BYOD policy](#) will help you keep your data safe. Learn more about the risks and benefits of BYOD for your business in this infographic, [Overcoming the Challenges of BYOD](#).

Source: <http://newswire.net/newsroom/blog-post/00096060-overcoming-the-challenges-of-boyd-infographic.html>