Embracing Mobility and BYOD In the Workplace

PEGAS TECHNOLOGY SOLUTIONS LLC

The separation between work and personal time for most of us is quickly vanishing.

Devices like laptops, tablets, and smartphones have changed the way we work; making it easier to keep working from wherever we happen to be. The workday is no longer confined to office hours, or even to the office.

The modern workforce is a mobile workforce, with 3 in 5 employees now believing an office presence is no longer necessary for a productive day's work. A big part of that is the growing trend of BYOD – Bring Your Own Device. This trend is completely changing the way your employees do their jobs, and there’s no going back.

Whether you like it or not, your employees are more comfortable working on their own devices. Especially when this means they can say goodbye to the slow, clunky desktop computer you've supplied them. Their devices come with a wide range of functions and features that make working on-the-go simple. Tradition computer hardware just can't compete.

By now, many businesses have fully embraced the BYOD culture and all of its benefits. But some have yet to address the many security vulnerabilities it’s created. This raises a very important question — Is your team using personal devices with safely, securely, and with the long-term adaptability of your business in mind?

There are five BYOD practices every business should adhere to in order to ensure a safe and smooth transition into the age of workplace mobility. But first, a bit of background on the mobility movement.

BYOD Goes Mainstream.

While it might seem hard to believe, given how prevalent these devices are today, a mere decade ago this type of technology was all but unheard of. Employees were trapped in their cubicles, their PC was the only access they had to the company network. The odd employee might be lucky enough to get a company-issued laptop that came pre-loaded with the necessary software, and some were even trusted with File Transfer Protocol privileges to access and transfer files to the server. Cell phones were only just gaining the ability to send text messages.

The BlackBerry was a game-changer at the time, but even then, only granted users had mobile access to their email and schedules. The BlackBerry Enterprise Server made configuring and managing these devices simple for the company IT department.

Then things started to change.

BlackBerrys gave way to iPhones and Androids. Laptops gave way to tablets that gave users the best features of a laptop and smartphone combined. The number of public Wi-Fi hotspots grew, and employees were eager to access business data from just about anywhere, and on any device.

Today, BYOD is the new normal. As many as 75% of small businesses have some type of BYOD policy in place, and, of those that don't, 80% or more of their employees' access company resources with an unauthorized personal device. Initial resistance to the BYOD movement proved to be futile, and now most business owners have started to see the benefits of BYOD. Benefits such as:

- ## Increased Productivity

It's estimated that businesses gain an average of 9 extra hours of productivity a week when employees are allowed to use personal devices.

- ## Improved Client Service

Increased flexibility allows employees to handle client concerns more efficiently, responding to emails faster and handling inquiries outside of business hours. Think about how often you've gotten a reply back after 5 PM with a "Sent from my iPhone" signature attached.

- ## Reduced Costs

If your employees are supplying their own laptops and phones, that makes for a significant amount of money you don't need to invest in new hardware. In fact, a BYOD policy can save you as much as $3,150 per employee each year. Not only do you not need to provide devices, but you don't have to budget for regular upgrades, either.

This is great news since it's now universally accepted that mobile devices are a necessary part of a business' day-to-day operations. In fact, most business professionals acknowledge that it would be extremely difficult to do business otherwise – even going so far as to say that their business couldn't survive without mobile devices.

However, while businesses now admit that mobile technology is a must-have, many also admit they have no idea if their data is adequately protected against the risks posed by all of this remote access. While these businesses acknowledge that BYOD puts their organization at risk, only about 22% currently have a comprehensive policy in place to address mobile device usage and define data access privileges.

This is problematic for several reasons:

- Roughly 1 in 3 employees use more than one mobile device over the course of a typical day. It's critical for you to know what devices are accessing your network, and who they belong to.

- Public Wi-Fi is readily accessible and notoriously insecure. This exposes your employees' mobile devices to an increased risk of being hacked. In recent years, businesses have recorded a 60% increase in malware infections due to insecure mobile devices.

- BYOD makes businesses highly susceptible to costly data breaches, with 38% of these breaches resulting from a lost or stolen mobile device.

- There are over 500,000 apps available in the Apple Store, and another 200,000 apps available in the Android Marketplace. While there are security controls in place to evaluate the safety of these applications, there's no guarantee that there aren't dangers like phishing screens, hidden spyware, or malware lurking inside a seemingly harmless app.

A BYOD policy can be hugely beneficial to your business, but only if it's not putting your critical data at risk. Developing a comprehensive BYOD policy minimizes your risk while still granting full, secure access to the files and applications your employees need.

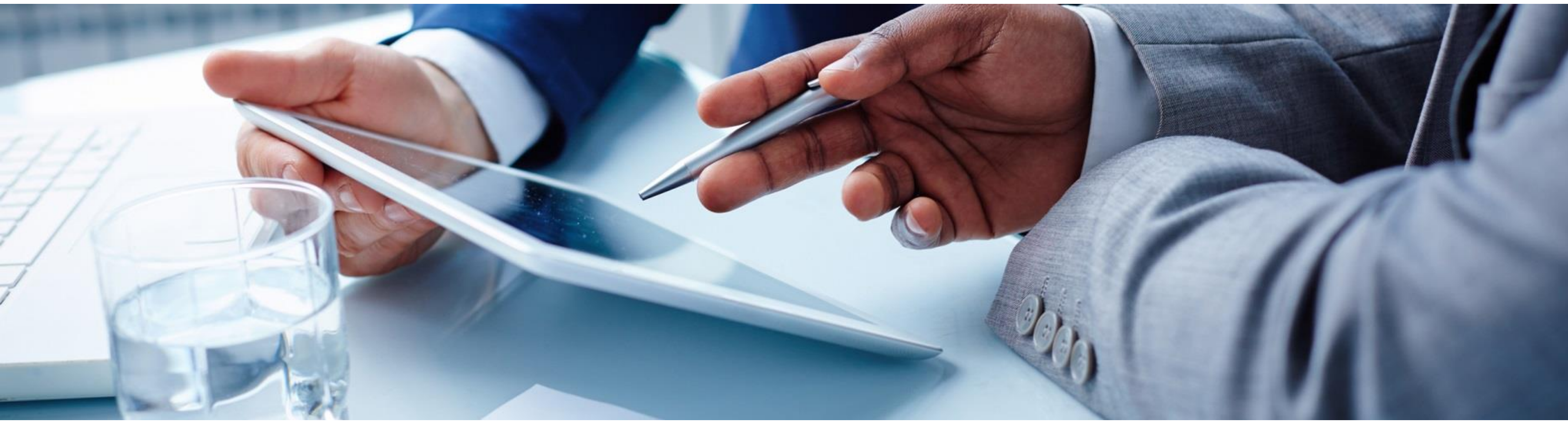
Five Tips to Do BYOD The Right Way

1. Create a Mobile Device Policy, And Enforce It: Lay out very clear guidelines for what employees are expected to do and not to do with their mobile devices. You're not just managing devices here — You're managing people. Clearly define the types of devices that are allowed, and what types of behaviors are unacceptable regarding web browsing, app downloads/usage, public Wi-Fi protocol, and data storage/transmission. And while you want to try to support as many different devices as possible, you need to set guidelines to keep things from becoming unmanageable. Set minimum requirements for device age and capability, and limit the number of devices each employee can use. Keep in mind that older devices can be difficult to secure—For example, any iPhone older than a 3G won't permit device-level encryption.

2. Keep Devices Locked and Password Protected: Devices that aren't password protected, and are left out in the open, pose a huge risk. It's also important to remember that 46% of employees will let friends or family use a device that they use for work. Most devices come with built-in security controls such as locked screens, and an option to have the device wipe itself after a set number of failed attempts. Some even have GPS tracking. Passwords should be strong, changed frequently, and NEVER written down or shared.

3. Immediately Disconnect Terminated or Voluntary-Leave Employees: Remotely wipe data stored on the personal device of any former employee as soon as possible. Ideally, the data should be retrieved and then wiped to avoid your business losing copies of important files that only the employee has. Establishing a file-sharing policy through a service like Dropbox is a good way to avoid this problem.

5. Use A Mobile Device Management (MDM) Solution: MDM solutions are a simple and cost-effective way to ensure any mobile device used to access your business' network is identified, controlled, and monitored. This method of centralized management makes configuring devices for enterprise access easy, enforces password and encryption policies and settings, automates security updates, proactively identifies and corrects device or app issues, and locates and remotely wipes and locks lost or stolen devices.



When all is said and done, any benefits your business gains in terms of flexibility, efficiency, and productivity won't count for anything if you don't have policies in place to protect your business and your data from the potential risks that come with BYOD. While you might want to accommodate employee wishes, you need to be careful that you aren't granting those wishes at your business' expense.

Create a policy, enforce it, and regularly update it to keep pace with the latest mobility trends. To learn more about BYOD best practices, contact Pegas Technology Solutions at *sales@pegas.io* or *207-835-4053.*