BYOD and the Consumerisation of IT

This paper takes a look at the growth of BYOD in the workplace. It provides a high level guide to assist you with considering the steps in embracing this trend, thinking about how your security and data privacy are maintained, and ensuring that your IT management costs are kept under control.

July 2012

impeltec

+61 3 9005 5722

info@impeltec.com

www.impeltec.com

What is BYOD?

Most likely, many of your employees are already using their personal computing devices to send and receive company email, connect to your company network, or store your sensitive company data. Almost everybody has a capable smartphone, and tablets are becoming more and more popular every day. Many people are using their personal desktops or laptops for work when at home or out and about. Welcome to the consumerisation of IT and the world of Bring Your Own Device (BYOD). It's here; your employees demand it, so how are you going to manage it for your business?

Are your employees asking your IT department to configure and setup their devices for business use? Are your employees expecting you to support these devices if they have problems connecting or using line of business applications they've installed themselves? Is your HR department ready to handle new employees that demand BYOD? How are you protecting your workplace from security breaches, viruses and malware? What end-point security measures do you have in place? How are you protecting your sensitive business data if devices are lost or stolen?

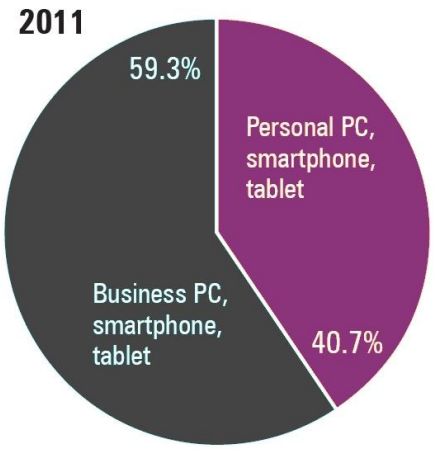
These questions, and many more, are on the lips of most IT Managers and CIOs. They are valid concerns that must be addressed to ensure your business is attractive to employees, remains competitive within your industry, and is safe from malicious attack.

impeltec provides specialist IT services, focusing on the end-user workplace. This white paper has been written by impeltec to try and help you better understand BYOD complexities and to think about ways you can address them. There is no one-size-fits-all solution for BYOD. This document is intended to give ideas to you about where to go next. It raises a lot of questions that you should think further about and discuss with your governance board, IT department or service provider.

> **The empowered workforce is challenging IT to embrace consumerisation**[1]

How will BYOD benefit me?

Work-life boundaries are blurring. By using their own personal devices, your employees will be able to work anywhere, anytime, including out of hours, during commutes, and when visiting clients onsite. They will have instant access to the information they need, including their applications and social networking tools. All these things will contribute to an increase in their productivity, giving them the flexibility and empowerment to work more smartly and efficiently.



Devices used to access business applications
Source: IDC Information Worker Custom Survey, sponsored by Unisys, May 2011

Does BYOD reduce costs?

Although you may see the perceived cost benefits involved if employees are providing hardware themselves, it would be a huge mistake to neglect the hidden costs.

Allowing BYOD opens the door to a wide range of devices and platforms. For your IT staff, this becomes very difficult to provide technical support due to the heterogeneous nature of BYOD. If your company currently uses Windows, but the device has an Android or iOS operating system, does your IT staff know *how* to support it? Also, if the employee is remote, how can your IT staff help? If you are already managing or monitoring your devices, how will you extend this to cover BYOD devices?

Do you need additional WiFi access points in your office, or security and management software? How do you handle recovery of lost data? How do you separate and manage personal and business data? How do you manage licensing of line of business applications installed on

the BYOD devices? All these things, and a host of non-technical concerns, can cost you time and money and must be considered when embracing BYOD.

What about security and data privacy?

When your employees are using BYOD devices to connect to your resources, it is imperative that you consider the security implications in order to mitigate any risk. These devices need to be treated as untrusted end-points connecting to your infrastructure.

Your upmost responsibility is protecting your company's private and sensitive data. Employees who BYOD will likely have your company data on their personal device. How do you ensure that this data doesn't fall into the wrong hands if the device is stolen or lost, or if the employee leaves your company? Will you mandate that the data is encrypted?

Also paramount is protecting your environment from potential virus or malware threats. You will need to ensure that BYOD devices have adequate end-point protection. It is not safe to assume that employees will take appropriate measures themselves to secure your business interests.

Who's responsible for what?

In addition to addressing the technical concerns, HR, legal, and finance policy needs to be in place to ensure you and your employees understand the rules and conditions around the use of BYOD in your environment. A User Agreement should be mandatory prior to allowing access to company resources from personal devices. Some questions to consider include:

- What technical pre-requisites do you require for BYOD devices to gain access, e.g. anti-virus software?
- What is the procedure if the device is lost or stolen, or if they retire it or leave the company?
- Who is responsible for the safekeeping of their personal data?
- Who pays for mobile data usage or mobile plans that most BYOD users need?
- If the device breaks, who is liable, and how do you ensure your employee remains productive? Will the company provide a replacement?

IT perceives employee-provided devices to be 3 times the security threat than company devices[2]

So, where do I start?

BYOD isn't something new. People have been using non-company assets such as personal laptops to access company data for many years now. What is new is the ever growing increase in smartphone and tablet devices and the wide availability of high-speed data.

Start your planning

The most important first step is to *plan*. Decide what level of access you want your employees to have from BYOD devices. Is it just email? Do you want to give them access to your company documents or applications anytime, anywhere?

What devices will you allow, and how will you allow them? Will you have a whitelist of devices, or allow any device and any platform? Can employees access resources directly from a BYOD device, or do they need to access them through a secure gateway or using virtual infrastructure?

Next, develop a *usage policy* that outlines appropriate use of company resources from BYOD devices. Consider having a User Agreement that your employees must accept before allowing access. Work with your IT, HR and legal departments to outline who is liable in the event of data loss, hardware failure or loss, how access is supported, and who pays for data usage charges.

Enforce your standards

Do you currently use a Standard Operating Environment (SOE)? The whole aim of an SOE is to realise efficiencies through standardisation of your end-user environment, so how will this fit in with your BYOD policy?

Will you force employees with personal laptops or tablets to install your company SOE to gain access to resources? Is dual-boot an option? Will you update your SOE to include a broader range of hardware support? Could you supply employees with your SOE on a USB flash drive using Windows® To Go? Will you present the SOE using Virtual Desktop Infrastructure (VDI) or Session Virtualization technology?

Manage the devices

Even though your company doesn't own the asset, if the employee is accessing your resources, you should consider bringing the device under management. Some of the traditional client management software, as well as some newer cloud-based tools, have the ability to manage devices over the internet. These tools will allow you to collect software and hardware inventory, distribute software, and provide security updates and hotfixes.

Enforce security policies

Policy enforcement depends on the level of access to resources you want to give your employees, and what type of device they are using to access your resources.

Across the board, the most likely resource your employees want to access is their email. For smartphones, there is a plethora of on-premise and cloud-based software that can enforce policies such as password protection and provide remote wipe capabilities in the event of loss or theft.

If you're allowing employees to connect to company resources by VPN or physically connecting to your Local Area Network (LAN), you should seriously consider using Network Access Protection (NAP) or Network Access Control (NAC) to identify and quarantine unknown devices. These technologies can restrict network access, allowing only compliant devices to connect.

Provide access to resources

If you want to provide access to line of business applications on BYOD devices, there are several ways to do this. For general office productivity software, you can consider one of the online hosting providers. For company-specific applications, you can consider virtualisation or migrating your on-premise applications to platform independent web-based applications.

> By 2014, 90% of organizations will support corporate applications on personal devices[3]

Another growing trend is providing employees with the capability to self-provision company applications. There are options to provide a private app marketplace within an existing public marketplace, or to provide an internal-only marketplace.

If you want your employees to be able to access their data, but don't want to provide a VPN or use VDI, there are many cloud-based storage solutions that are available.

Some final thoughts

Like everything, there are plenty of pros and cons for BYOD. The fact is, over the next several years it will become more and more prevalent, and there is no way of avoiding it if you want your business to remain competitive and attractive to employees. You can pretty much guarantee your company already has employees using BYOD whether you know it or not, so the best thing to do is plan and implement a strategy now.

References

1. Forrester Research, Inc. (February 2011). IT Managers Selectively Embrace Consumerization.
2. IDC (May 2011). IDC Business IT Custom Survey, sponsored by Unisys
3. Gartner, Inc. (2010). Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency