What is BYOD and why is it important?

By Dean Evans August 23rd 2013

As many IT departments struggle to keep up with yearly technology changes, company employees increasingly want to use their own devices to access corporate data.

It's part of a growing trend dubbed Bring Your Own Device (BYOD), which encompasses similar Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP) and Bring Your Own PC (BYOPC) initiatives. All of them have evolved to empower workforces through the so-called 'consumerisation of IT'.

As part of this consumerisation, BYOD encourages company employees to work on the device they choose - accessing corporate email on their **iPhone 5** or using a **Google Nexus 7** to view text documents. The goal for SMBs? Increased productivity and reduced costs.

But BYOD also has a darker side. If not fully understood and regulated, it can threaten IT security and put a company's sensitive business systems at risk.

Why BYOD matters

The driving force behind BYOD is a new IT self-sufficiency among company employees who already own and use personal laptops, tablets and smartphones.

These mobile devices are often newer and more advanced than the equipment deployed by many IT departments. It's hardly surprising that the rapid adoption of lightweight **Ultrabooks**, iPads and large-screened phones are changing the way that people want to work.

IT departments are playing catch up and could easily refuse to embrace the BYOD idea. Surely it's simpler to provide approved hardware and software applications so you can retain full control over them?

But Richard Absalom, an analyst at Ovum, believes that BYOD will happen whether a company plans for it or not. **He says**: "Trying to stand in the path of consumerised mobility is likely to be a damaging and futile exercise." The best thing that an SMB or enterprise can do is be aware of the benefits and understand the risks.

BYOD benefits and advantages

There are some key advantages to operating a BYOD strategy, including increased employee satisfaction (they can work more flexibly), cost savings (reduced hardware spend, software licensing and device maintenance) plus productivity gains (employees are happier, more comfortable and often work faster with their own technology).

As Mark Coates, EMEA VP at Good Technology, points out: "By enabling employees to securely and easily access corporate data on their own device, productivity levels will naturally increase. In terms of cost savings, there are huge benefits, since SMBs will not have to manage and fund a second device for employees."

Shaun Smith, technology practice director at Xceed Group, agrees. "At Xceed Group, allowing the use of consumer devices has helped improve both productivity and staff motivation," he says. But he also strikes a note of caution. "For a company to decide if a BYOD strategy would work for them they need to ensure due diligence is conducted - simply evaluating the benefits versus risks."

BYOD risks and disadvantages

While BYOD sounds attractive, businesses need to consider the full implications of allowing corporate data to be accessed on personal devices that they could have little or no control over. What data can employees have access to? What security measures are in place if an employee's device is lost, stolen or compromised?

This is where convenience clashes with security. "Security and the loss of devices with limited password protection is naturally a key concern," adds Smith. "Increased consumerisation in the workplace can bring with it an increased risk from threats such as hackers and viruses."

There might also be cost implications. Even though IT hardware spend can potentially be reduced with a BYOD approach, it may cost more for a company to integrate and support a diverse range of employee devices. As Coates points out: "Android devices can be complex to manage as there are just so many different flavours - a huge variety of devices and a number of different versions of the operating system."