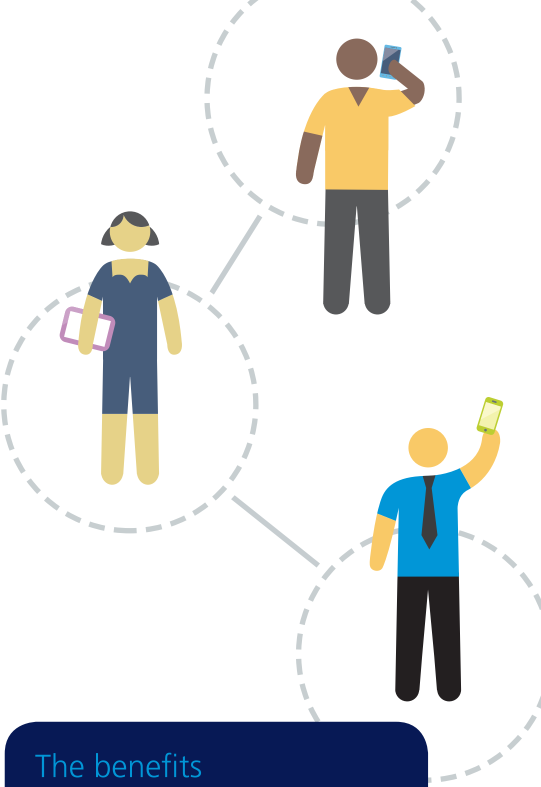

Personal technology at work: anything but black and white

Allowing your people to use their own devices at work is not an easy decision, as Nigel Watson, Head of IT Security, and Jason Endsleigh, Managed Mobility Product Specialist at Telefónica explain.

Read any Sci-Fi book from the last 50 years and you'll find the authors making all kinds of forecasts as to how we'll be using technology. What none of them picked up, though, was how more and more of us are taking our own technology to use at work. Let's face it, if you'd placed a bet just five years ago that bring-your-own (BYO) or choose-your-own (CYO) would catch on, you'd be quids in by now.

What does the future hold?

In the next 18 months we fully expect to see flexible BYO arrangements increase among certain types of companies, especially as devices become more usable and convenient. Within O_2 – and increasing numbers of our clients – it is fast becoming the normal way to work, with people using their own smartphones, tablets and laptops in the workplace.

So what are the pros and cons of such an approach? Well, we see several quite legitimate concerns centred on security. It's all very well allowing people to wander around connecting their devices to your network and accessing all sorts of information (especially customer data), but you need to put the systems and policies in place to ensure your network stays safe. At O_2 we aim to find a balance between allowing people the freedom to use their own devices, and the information they can access.

We're able to do so thanks to Mobile Device Management (MDM) and desktop virtualisation technology (thin client). MDM is part of a wider mobility management discussion which also includes apps and access to corporate resources. It tells us all kinds of things, like the name of the device that's trying to connect; the level of security software it has (or hasn't got); and who it belongs to. The system then enforces certain security controls on the device, restricting the corporate applications and services the device can access, as appropriate.

So, while organisations may be right to be concerned about the threat a BYO approach can pose – it's worth bearing in mind that there's quite a lot that can be done to secure the network. Even down to setting time-out/lock-out protocols, encryption of corporate data and PIN/password security on individual devices. MDM, which is a core element of Enterprise Mobility Management (EMM), can even detect if a device has gone feral (especially when it's been jail-broken or rooted*), and can reject access to corporate networks as a result.

Further control is provided by virtualisation technologies, which enable employees to use their personal devices to access internal corporate applications, but prevent them from storing or processing corporate data on the devices. In simple terms, the employee is given a window into the data, reducing the risk of sensitive data leaving the organisation.

The benefits

MDM and EMM integrate several services, giving you a clearer picture of your mobile estate and helping you control access to company resources. For example, MDM vendors are now integrating into Network Access Control (NAC) solutions to provide management and visibility of both the devices and the entry point to the company network.

Among other things, you can find out:

- What type of device it is (Apple, Android, Blackberry, Microsoft)
- Whether a device is known to the organisation
- Whether the user is recognised
- Whether the device has appropriate anti virus software, is up-to-date and corresponds to your standards
- Whether it has been rooted or jail-broken
- Which applications on the network the device can access
- If any time-of-day restrictions apply, for example for temporary staff
- Whether it has device encryption

*Jail-broken (iOS) and rooted (Android) devices have had the inbuilt restrictions removed by the user. Jail-broken and rooted devices pose a security risk as they're more vulnerable to malware. It's recommended to block these devices via a relevant MDM solution.

The benefits continued...

Once you know who and what you're dealing with you can take action, for example refusing connection permission or automatically updating security software before access is granted.

Other key security controls include:

- Enforcing PIN or password authentication before a device can be used
- Enforcing encryption of the whole device or the elements that store corporate data
- Centralised location look-up, and remote wipe of whole device or the elements that store data if it is lost or stolen
- Logging features for audit and compliance

The benefits of BYO are plain to see. A quick visit to our head office in Slough will demonstrate the growing number of our people who work with their own device. When we ask them why, the responses range from wanting to have all their information (personal and business) on one device, to wanting to use some of their own apps (checking train times for instance) at work. It's making them more flexible, which is also making them happier.

We're also finding that behaviours are changing, with many using their device to work outside of normal office hours, not because they are expected to but because it suits the flexible approach they apply to the way they work. And – most importantly – they are content to balance this freedom with some usage restrictions from us.

Different strokes for different folks

We've noticed that BYO appears to be more popular in some industries than others. Companies working in marketing, design and similar industries have embraced it more than others, perhaps because users are more inclined to adopt it and the productivity and revenue benefits can be seen more clearly.

In fact we're hearing more and more of our customers refer to themselves as 'pro-social' businesses, with BYO at their heart. Employees are using their own devices to check home and work email, but also apps like Twitter to follow competitor companies and undertake market research.

According to Cisco, a consistent BYO policy could save your organisation £1300 per year, per mobile user.[1]

While BYO might not be perfect for every company, we're seeing that smaller organisations are using it as a way of operating with limited resources. After all, why spend so much on technology when, with the right support in place, people are happy to use their own?

It's here to stay

BYO has a number of implications beyond security. Including whether device contributions and running costs can be a taxable benefit, or if managing BYO policies become an administrative burden.

It won't suit every type of company, but as a new generation of school and college leavers join the workforce, it's worth remembering that you are increasingly dealing with individuals who know no other way of doing things. Their lives are run through their devices – and there will be a competitor, somewhere, offering its employees device and work flexibility.

As well as providing a competitive advantage, we're also seeing organisations embrace BYO as a way of cutting costs. It might be worth looking at the figures when your mobile/laptop lease renewal is due, to see how providing technology to your people stacks up against simply allowing them to use their own.

Ready to get started?

There are a number of ways your organisation can start embracing BYO. Most start with a mixed resourcing approach, by catering for those employees who want to use their own devices, while keeping things the same for those who don't.

To find out if BYO might be right for you, speak to your Account Manager or contact Matt Worth on **01235 433 507**.

Source: [1] http://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs/

Published in July 2013. All information is correct at time of going to print.
Telefónica UK Limited Registered in England no. 1743099. Registered Office 260 Bath Road Slough SL1 4DX

O2 business