Is BYOD putting your business at risk?

The **data security nightmare** of your staff using their own devices to access your data... and the plan you need to protect yourself

Is BYOD putting your business at risk?

The **data security nightmare** of your staff using their own devices to access your data... and the plan you need to protect yourself

We're pretty sure you know this already, but just in case: BYOD is short for Bring Your Own Device. It basically means that employees are allowed to use their own mobiles, tablets and laptops for work.

Sounds great, right? Well, in lots of ways it is. BYOD dramatically reduces capital expenditure and means workers are able to communicate with the rest of the team and get their work done without the hassle of having to carry multiple devices around with them.

As many internal IT departments struggle to keep up with new tech updates, BYOD is a convenient way to keep people working without having to be tied to their desks. One of the main aims is to capitalise on the consumerisation of IT, by empowering workforces to work freely and flexibly. Employees are actively encouraged to use the technology they're the most familiar with, meaning they don't have to waste time learning new devices and systems.

While it's hard to remember a time when we weren't tied to our mobile phones unable to shut off from the outside world, arguably these devices do improve quality of life. By enabling us to stay connected with friends, family and colleagues from anywhere in the world we're able to manage our lives much more efficiently than we did 10 or 20 years ago.

For businesses, BYOD can mean increased productivity and reduced costs. Fantastic! But there's a dark side too. If not handled properly, there's also a huge security risk that – if the worst happens – could easily cost you a lot of money and damage to your reputation.

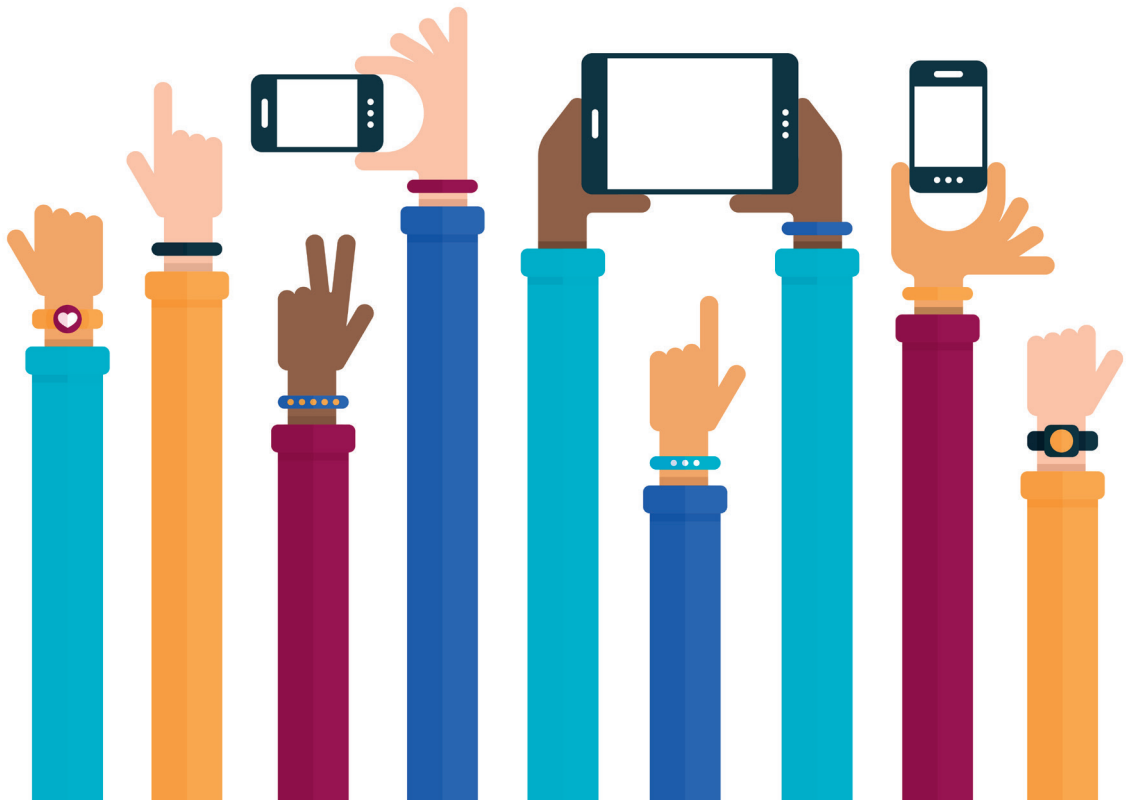
The moment you start allowing people to use their own devices for work you're at risk of all sorts of problems, like:

- Loss of total control
- Loss of visibility of important data
- Possibility of deliberate data leakage
- Physical loss or theft of devices leading to costly data audits
- Compromised integrity

Workforces are becoming increasingly mobile. It's now common practice to work on the train, at home, even in the pub, and this convenience has clear implications for data security. Nearly half a million Brits had their phones stolen in 2016, and a further 10 million handsets are lost each year. That's a whole lot of data to end up in the wrong hands.

With the new GDPR data laws just around the corner, data security has never been a hotter or more important topic. And guess what? Even if you have nothing to do with the loss or theft of someone's mobile device, as the person at the top of the business, the buck still stops with you if your data is compromised.

All employers have to address BYOD issues before giving their staff the opportunity to use their own devices at work. This means a robust, thorough policy document that's regularly reviewed. And making sure every single person in your team has read it and signed it.



Your policy document will need to include things like:

- Ensuring work data and personal data are kept completely separate
- What sort of corporate data can be processed on personal devices
- Encryption and secure access
- How and when corporate data should be deleted
- How and when corporate data should be transferred to and from company servers
- What to do in the case of loss or theft
- Auditing procedures
- Backup frequency and verification
- Data protection requirements
- Permissions: It must be crystal clear that work data is not to be shared with anyone else
- What happens when an employee leaves the business

You should also consider using a sandbox – ring-fencing your data – by keeping it contained within a specific app.

In order to implement a BYOD policy it's essential to be clear about why it's necessary for your business. The most successful cases are always those where companies have used their business goals (such as increased productivity, and a larger workforce) to inform their BYOD implementations. Just saying you think it's a good idea because it's convenient and saves money isn't going to cut the mustard if you find yourself with a security issue on your hands.

You also need to be able to show that your BYOD policy meets the needs of your employees as well as your business. Most human beings are fundamentally selfish. If you're not able to demonstrate to your people that there's something in it for them, they might be a lot less likely to take it seriously.

There will almost certainly be lots of positives for the end user. According to a study by Ovum, 79% of employees in high growth markets said they felt that the constant connectivity offered by BYOD enabled them to do their jobs better.

On the flip side the survey also found that 28.4% of users felt that their internal IT departments ignored bad BYOD behaviour such as sharing phones and passwords or accessing inappropriate sites at work.

Without a clear policy that outlines what's acceptable and what isn't, you're **setting yourself up for a lot of grief**

So let's take a look at the really problematic aspects of BYOD and what you can do to stop them in their tracks.

1

Non-work apps

One of the most important things to nail employee behaviour, but don't assume that just because your staff are playing by the book there are no security risks. A lot of apps collect data without obtaining the user's permission first, which means you'll also need to get a handle on what employees can and can't install on their devices. That's a tough one to police effectively.

2

Jailbreaks

When employees are using their own devices they can easily argue that it's up to them what they do with it. Even if you've made some sites and apps a no-go, there are still plenty of tech savvy employees who will know how to get around it. Jail-breaking devices (where the operating system is bypassed, opening up the device so you can install any software on it) hugely increases the risk of data breaches. So it's essential that you take a zero tolerance approach to jail breaking.

3

Loss and theft

We've already touched on the staggering number of phones that are lost or stolen in the UK every year. It's upsetting enough when you're losing personal photos, videos and contacts, but when you throw in loss of work data that's a whole other can of worms. Passwords and encryption of work data are an absolute must, as are regular backups to work servers.

4

Upgrades and trade ins

We all like to get a nice shiny new phone every so often, but what happens when employees upgrade without clearing their old ones of work data? All devices must be fully wiped and reset before they find their way to their new owners to avoid any costly leakages.

5

Internet activity

There's a real ethical issue about asking people to use their own devices and then telling them what sites they're allowed to visit. It's also practically impossible – and somewhat undesirable – to keep track of people's online activity when they're outside the office. Which leaves you even more at risk of viruses and malicious pop ups. A multi layered approach to cyber security is the only way to make sure your business is safe.

6

Downtime

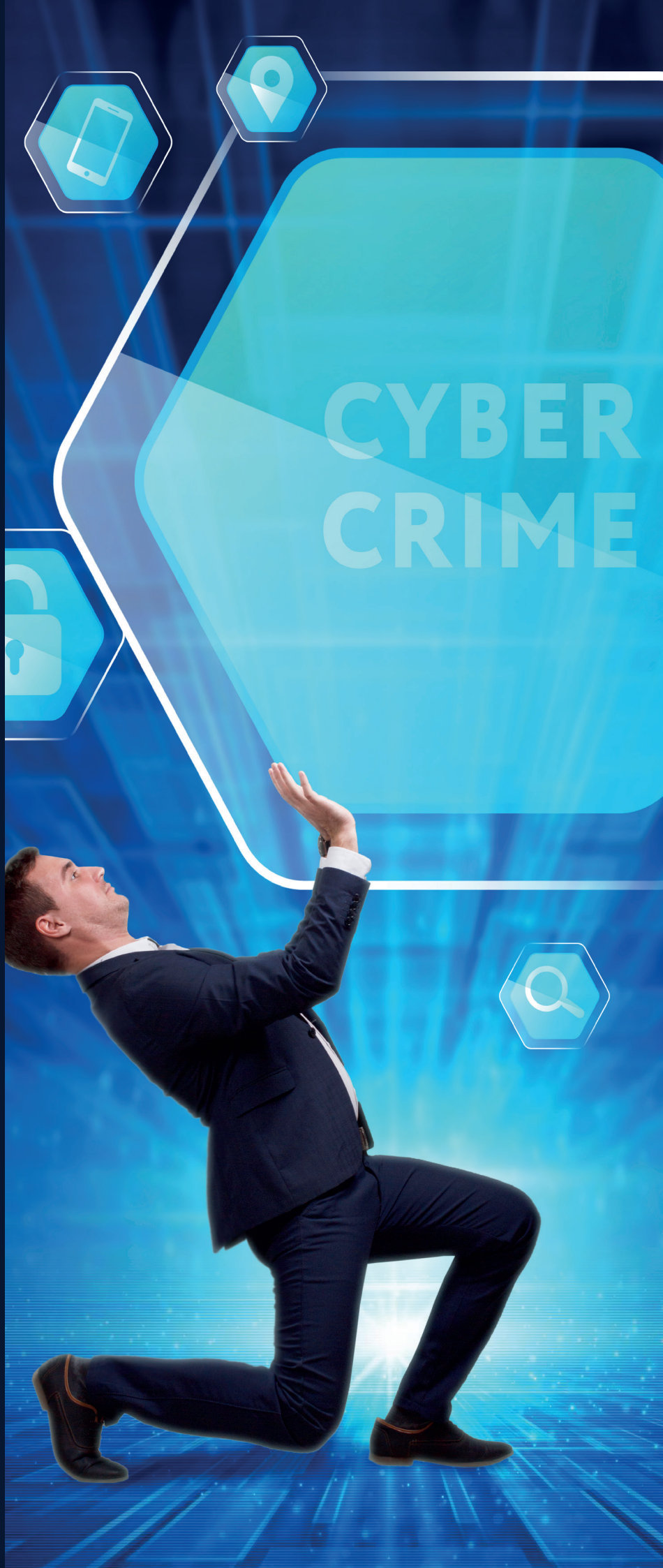
While BYOD can make people more productive outside the office, it can actually have the opposite effect inside. The constant distraction of texts, social media and even games can mean that people are actually spending a lot more time mucking about on their phones, than they are working. Be clear about how much phone use is acceptable inside the workplace and stick to it.

Over the past five years the risk landscape has changed hugely in relation to mobile devices. Mobiles now offer so many functions and capabilities that it's now entirely possible to do a full day's work without having to come within a mile of a PC or laptop. But those features also give cyber criminals much more ammunition if they do want to attack your business. In addition, the very nature of mobile devices being seen as personal means that attackers have access to a lot more sensitive data than they've ever had before.

When you're putting your BYOD strategy together, it's important that you understand the risks and manage them appropriately. All devices should have a hardware root of trust that protects your organisation's data, usually stored within the cloud.

You should also work with your internal IT Department or a trusted external partner like us to ensure that your business has:

- A sound method of registering devices
- A robust data security system in place
- The ability to track devices
- A mechanism for assessing the integrity and safety of all devices before they are accepted for work use
- The capability to isolate and protect confidential and sensitive data
- Strong authentication mechanisms and data encryption
- The ability to know how, why and when your data is being accessed and by whom at all times
- The ability to remotely wipe lost or stolen devices



2018 could easily be **the Year of the Cyber Criminal**. You need to make sure your business is 100% protected

Last year, all sorts of high profile organisations fell prey to online thieves who were lurking in the darkness, ready to steal their important data and wreak havoc on their infrastructures.

Whereas previously a lot of bosses had thought their company couldn't possibly be touched by a cyber thief, big names like the NHS, Debenhams, Wonga, Sony, T-Mobile, Mumsnet and lots more being attacked during 2017 really made people sit up and listen.

BYOD might offer all sorts of benefits, but you simply cannot afford to ignore the rise of cyber crime and the fact that allowing people to use their own devices massively increases your risks.

If you fail to put adequate mobile security policies in place you are putting your business (and its customers) in danger. Possible scenarios include:

- Sensitive personal data being leaked to third parties
- Compromised devices being used as an entry point for a larger attack, resulting in the total loss of business assets
- Hacked devices being used to impersonate users and steal their information such as bank account details and credit card information

Once your business has been attacked, it's really tough to come back. Not only are there huge costs to consider, the loss of face with customers is often the real killer.

People don't take kindly to the companies they trust taking a lackadaisical approach to their personal data. And as soon as it happens once the sad truth is they'll never fully trust you again. It starts an emotional disengagement that can ultimately lead to a long-term customer retention problem.

If you're serious about making BYOD work for your company and hanging on to your customers, you simply cannot afford to take risks with data security.

Contact us today for more information about how to keep your business safe and create a bespoke BYOD policy and setup that really works.

DIGITAL ORCHARD I.T

info@digitalorchardit.co.uk
0131 208 0080