THE BRING YOUR OWN DEVICE NIGHTMARE

Bring it on

Many of us have all heard of the acronyms BYO (bring your own), BYOW (bring your own wine) or BYOB (bring your own booze). It's where an unlicensed restaurant allows you to bring your own wine, sprits, cider or beer for no charge or for a small corkage cost.

Similarly, within many IT environments there is now a tendency to allow employees to BYOD (Bring Your Own Device). Many organisations allow their workers to bring their own PCs, *USB* hard drives, memory sticks, laptops and, more recently, smartphones and tablets. This (usually informal) policy has been around for some time but the term is relatively new.
When looking at the pros and cons of bringing your own drink to a restaurant, we see it does no real damage to the restaurant. The customer may end up a bit the worse for wear but as long as they used public transport or got a taxi to get home no real lasting harm would have been done – luckily hangovers subside! However, BYOD has far greater consequences when we look at its possible security and compliance risks.

Risky business

As data is the bread of butter of an organisation and it is hoped, secured, monitored, audited and kept firmly within the four walls of its office. However, it's clear that through the increase in BYOD this is now being compromised.

Many organisation's staff and volunteers use reasonably cheap devices which can have a large *storage* capacity, are easy to use and, unfortunately, have little security. Thousands of internal organisational confidential documents can be copied, innocently or maliciously, in minutes to someone's USB flash drive. Although many staff are just taking a document home to work on it during their evening, some may have the intent purpose to steal and sell important or incriminating documents to the press or possibly a rival organisation or company. Whatever the purpose, this creates multiple security and compliance problems. Documents are now dotted around, unsecured, unmonitored, unaudited and possibly not within the UK or EU. There are also other security risks to consider. When a staff member leaves their place of employment he or she may not have taken the time to delete or remove important documents on their mobile device. People lose their phones, iPods or USB drives all the time. This causes all sorts of security risks, can break the UK Data Protection Act and break client confidentiality. A USB flash drive lost on the train can find its way into the wrong hands, generating negative PR, fines, lost clients, members and – potentially - funding. The organisation's reputation could be critically damaged.

The Data Protection Act states data which is in transit (i.e. a USB device, laptop or CD) should be encrypted. It also states it is preferable to store data within the UK or EU. With modern home working and 'hot desking' it is not always possible for data carried by staff to always comply with these rules.

So what are the possible solutions?

Low security

Create a policy telling staff not to plug in their own devices – very flawed

This is for the lazy organisation which doesn't want to invest in time, *software* or money in examining security risks. This option is very flawed as it's very likely someone will ignore or forget this policy – hey presto, you have a data leak.

Give everyone a hardware encrypted USB flash drive – partly flawed

Hardware encrypted USB flash drives offer strong security but are sometimes expensive. It's only a matter of time before someone plugs in an unsecured devices, takes data and again hey presto a data breach.

Medium security

Block all USB drives and CD/DVD drives – for the paranoid

In theory this is a great idea as no one can plug anything in and therefore data cannot be extracted. This can be achieved through configuring a Windows Group Policy Object with a .ADM file on your server, dedicated software or end point removable media software. Also some *antivirus* programmes have this functionality (such as Eset, NOD32). However, it reduces productivity and flexibility and is therefore not conducive to modern working.

High security

Automated port blocking and encryption software – good security

This option permits devices and allows data to be copied out but forcibly encrypts files (or folders) automatically. Be careful with this option since if it is not configured properly it can 'brick' certain devices like iPods or smart phones. This option allows monitoring and auditing but possibly the removal, blocking and deletion of data.

Automated port blocking and hardware encrypted USB flash drives – ultra security

This is possibly the best option, although it is a little inflexible. All unsecured devices are blocked and only use secure devices. Automated port blocking software can block and permit devices by model, make or serial number. One major disadvantage is some hardware encrypted USB flash drives cost up to £400 – not great for the organisation's budget if you lose one.

Source : http://www.ictknowledgebase.org.uk/byodnightmare