BYOD – short for ‘Bring Your Own Device’ refers to permitting employees to bring their own devices into the workplace and then use them for business purposes, as well as on-going private use. Typically the BYOD devices in question are smart phones such as iPhones, tablets such as iPads and Laptops.

This BYOD trend has been much discussed over the last two years in larger organisations and with good reason. These large organisations with many employees have often been railroaded into allowing BYOD rather than it being implemented as a well-planned strategy. Senior executives have pushed from the top in requiring access to company networks and information using the latest mobile technology, while the young twenty-somethings from the bottom have also pushed an often despairing IT department into additionally allowing them access. Often this latter group and their managers cite access to social media as essential for both business needs and to keep the morale of the work force up by allowing private access during business hours!

Many of these companies have woken up to find out it is too late to implement sensible security strategies to stop data being leaked to others outside the organisation, or plug gaping holes in a once secure IT infrastructure. The size of the problem can be illustrated by global company IBM. They have a huge 465,000 workforce and allow something like 1.2 million mobile devices (Smartphones and Tablets) onto their network, the majority of which are not owned by IBM. In response to such a massive problem IBM purchased a company who are experts in Mobile Device Management and implemented very strict employee ‘Acceptable Use Policies’ (if employees don’t adhere to them, they don’t work for the company any longer!). Many other companies obviously cannot do the former and are incredibly weak and indecisive about the latter.

For many SME businesses the situation is not so bleak. The scale of an existing or potential BYOD problem is relatively not so large and therefore the future can be more optimistic! Even if employees are already using their own devices in your workplace you can introduce formal (and legally binding) ‘Acceptable Use’ policies which in fact will protect your business but also help the employee too. They can additionally be given clear ‘Best Practice’ guidelines so they are in no doubt as to what is acceptable and what is deemed to be not in the best interests of the organisation.

**Why is it now so different from former times?**

In the past, both large and small companies had fixed networks protected by a firewall. Inside the firewall perimeter employees used company owned PCs equipped with company owned applications. The organisation often mandated that unlicensed or unapproved software could not be
installed on company devices. It could easily set up policies and password controls to ensure who had access to what data from the company servers. Use of USB memory sticks was disabled. The IT or Network Manager could implement further controls to stop users going out on the internet to obviously undesirable places they should not visit and additionally monitor where they were going for allegedly business purposes. This traffic could be scanned for malware as could incoming and outgoing emails. As long as the organisation kept its security patches and defences updated, the organisation felt and indeed was, pretty secure.

So what are the Business Advantages of allowing BYOD?

One of the key advantages for businesses, that is often highlighted is that employees purchase the BYOD device thus saving the business costs. However, it is the same employees that totally control the devices – they make the decisions on makes, models and all the loaded applications, a situation that is obviously far from ideal. Other benefits promoted by BYOD enthusiasts include employee familiarity of using their device cutting training costs, plus allowing employees to access their private social media services while at work makes workers feel happier and consequently more productive! Additionally, the theory is that if employees can have freedom of access to business facilities from outside the workplace they will be inclined to work longer hours for free. These productivity advantages are often stated as an advantage, but rarely with any meaningful evidence.

The BYOD advantages of the company not having to fund the device and improving staff morale for many organisations is outweighed by the potential significant security risks.

BYOD Risks and Challenges

With the introduction of BYOD new risks and challenges have emerged particularly with mobile devices. Not only can sensitive company information be transmitted via all the traditional means but also via social media, including by video, photographs and voice recordings – all from the same tiny portable device. In an unregulated BYOD free-for-all, the IT or Network Manager no longer knows from day-to-day which devices are on the company network, what applications they are using or what data these devices hold. Data downloaded onto these BYOD devices or received via email is immediately vulnerable during data transmission and once on the device – if it is lost or stolen – then the consequences of a third-party obtaining the data are obvious. A company involved with regulatory compliance issues – solicitors, accountants or any financial organisation etc. obviously
have a problem justifying in any serious audit, that they are keeping data safe in such a chaotic BYOD environment.

In the traditional IT world viruses and malware such as key loggers were well known and counter-measures worked efficiently, as they could detect unusual behaviour in a stable IT environment. New sophisticated malware attacks on mobile devices often no longer bother to attempt to control the mobile operating system, they target the browser software on these devices. Malware exploits can in fact monitor both mobile SMS transmissions and browsing activity. Potentially, an exploit can break into the mobile device while it is not even at the workplace – and then has remote access to the company network having monitored logon information. Additionally it has access to any local data downloaded to the BYOD device. As mobile devices are often now being used for two-tier authentication, using SMS as way of adding extra level security to traditional password checks – this mechanism becomes highly questionable if the mobile is being monitored and is capturing PIN or other security access information.

**Some Recommendations for SME Businesses**

So what are SMEs to do? This all sounds quite complex and depressing! We believe there are some simple steps that can quickly rectify or improve the situation:

1. You need a clear written policy document on ‘Acceptable Use’ and ‘Best Practice’ utilisation of:
   a. Company Information
   b. The Internet
   c. Social Media
   d. BYOD
   e. Passwords
   f. Cloud Services

   Each individual business needs to define what is allowed and what is not, in order to create its own tailored policies. Whatever puts the business at risk needs to be controlled. Employees need to ‘sign-up’ to these policies in all senses of the phrase.

   We have looked for some good templates written for UK businesses. We can find plenty for US corporates and UK educational establishments but nothing very worthy for UK SMEs. We
will therefore create a template and publish this to assist our customers to act as a starting place. In addition, the company needs to create some clear ‘Best Practice’ guidelines – an obvious example is in regard to passwords. These should be suitably strong and changed regularly. Consider password management software to automate this process. In the same vein do not keep important company data on cloud services that are not encrypted.

2. Segregate BYOD devices from the corporate network. This can be achieved with security devices such as NIS’s NetPilot and SoHoBlue products. For example if your organisation is prepared to allow employees to bring in their own smart phones to the workplace, then allow them to attach to a Wi-Fi service that is firewalled and separate from the main company network. Stipulate that you allow employees to use their devices in this controlled manner say at lunchtimes, but expect workers not to be regularly using them for personal use at other times. Also your policy should explain that the organisation is monitoring use – which again is easily achieved with NetPilot and SoHoBlue. It should be remembered by employees they are being given access to an expensive company resource (the internet) – which is primarily there for business purposes. Large scale downloading of music, videos etc., should be prohibited as these bandwidth hogging activities could literally be preventing the organisation taking and servicing orders from customers.

3. Work out if social media is of business benefit to your organisation. If it is of benefit, then allow only departments or individuals that actually need access to have it, but monitor and control how this is achieved. For everyone else, they can Tweet and use Facebook etc. on their own devices via the company provided BYOD Wi-Fi network.

4. Use VPNs and file encryption on mobile devices and laptops regardless of who owns the devices. NIS has excellent VPN solutions for mobiles and Laptops so the communication transmissions are encrypted. If you have decided that it is permitted to keep sensitive company data on BYOD mobile devices as well as company owned mobiles and Laptops, then all types of devices should employ encryption of sensitive files and emails. This may well limit the type of mobile device you will authorise to one particular make, where you can implement a good measure control and provide encryption software. In addition, with software such as Apple’s iOS 7, not only can you use the well-known tools to display physically where your lost or stolen device is now located, but it now also allows remote implementation of further access barriers or even the ability to wipe the mobile device
5. IT and Network Managers must make better use of tools already at their disposal. NetPilot for example offers good control and monitoring features. URL filtering can be used to restrict access to meet the goals of the company policies. Logging and analysis of device usage should be used to regularly examine exactly what devices are being connected by whom.

Action List Summary

So in summary the action list is:

- Write and implement policies
- Implement network segregation of BYOD devices
- Implement Social Media controls
- Implement VPN and Encryption
- Use existing controls, logging and monitoring

We hope this has been of some assistance and would welcome feedback.