BYOD – How to manage the risk?

The popularity of personal smartphones and tablets continues to affect the workplace. Employees increasingly want to use their own devices at work because they think they are more effective or convenient than those provided by their employer. They can also check emails outside office hours even if a phone is not made available by the employer and so do not need to carry around both a work and a personal mobile.

Bring Your Own Device (BYOD) offers obvious savings to employers and greater flexibility for employees, but with opportunity come numerous and expensive risks. Some employers prefer the Corporate Owned Personally Enabled (COPE) approach, where devices are owned by the employer but personal use is enabled and managed. The benefits for an employer are that it owns the device, so wiping and access to data are made easier particularly in situations where the employment relationship breaks down. Where COPE is coupled with choices from a range of devices, the employee can still choose a device they like.

Security risks

PINs or passwords are commonly used to protect mobile devices, but often to no great effect if rarely changed. The latest iPhone is protected with fingerprint scanning software, but many security measures currently in place are limited. There is a high risk that confidential or sensitive company data may fall into the hands of third parties. Software is available which enables IT teams to remotely wipe devices, but it has obvious limitations as wiping can only be effective if theft or loss of the device is discovered immediately before confidential data can be downloaded or accessed. Where personal devices are wiped where an employee leaves employment, there is also a risk that personal and irreplaceable data is deleted from the system, although the use of "sandboxing" which separates personal from work data, enables the employer to restrict the wiping of data to that contained in the sandbox. There are however limits to remotely wiping a device and in some cases it is possible to restore data on a wiped device, meaning the wiping is not completely secure.

Stephen Musgrave Limited
T +44 (0) 20 7502 9320 M +44 (0) 7793 019562 stephen@stephenmusgrave.com www.stephenmusgrave.com

Encryption or malware/ anti-virus software can slow down a device, and employees may also choose either not to use it or else may even disable it. Ever more advanced cyber-attacks are developed daily. Software quickly becomes out of date unless updated regularly. License restrictions may prevent an employer from installing products on a private device meaning that employees will not necessarily benefit from employer-owned software. Employees also need to understand the risks of using open, unsecured WIFI networks in hotels, coffee shops, airports or tube stations which may make the device an easy target for hackers. Sophisticated software cannot stop the eyes of an eager passer-by or neighbor on public transport from glancing at your screen.

Where family members have access to or use the same devices damage can be caused by inadvertently emailing or posting company information on social media sites and so allowing third parties access to confidential company data, to delete valuable data or to disclose confidential information to a third party. Best practice requires employees to use a remote platform or VPN to access corporate data which is password-protected. This enables the employer to increase security measures for downloading data onto personal devices or accessing it, for example blanket prohibitions on downloads, password prompts to enable a download, or restricting the download of certain data.

Employers can stipulate exactly the requirements of personal devices in a policy, but realistically the monitoring of compliance is difficult and costs can outweigh benefits. Monitoring of personal devices also poses risks as some storage or SIM cards can be placed in other devices, and then data may be downloaded and accessed elsewhere without the data transfer being apparent.

Privacy and Data Protection

Holding private and personal data in the same device is problematic. "Sandboxing" - the division of data into private and business - is not foolproof but dependent on the proper use of the software and a diligent user. Sandboxed applications and software are often slimmed-down versions and may not have the same functionality as full applications. This limits user experience and defeats one of the main objects of BYOD as users expect a tailored user interface which may not be available with

sandboxing. There is also the risk that the employee inadvertently labels private data as business data and vice versa. Companies' data retention policies may require the back-up of company data stored on private devices at regular intervals, meaning it's possible that a private message saved incorrectly in a business folder is backed up onto a company server where it remains for a (potentially fairly long) period of time even if the mistake is discovered by the employee and the document is re-filed as private. Depending on the location of the servers, this may also breach data protection legislation.

Back-up of data is also problematic. How are BYOD users expected to back-up company data? Cloud-based storage systems come with risks, as applications such as Drop Box enable users to easily access documents simply by installing the application on any device. A user may have Drop Box installed on his corporate PC, his iPhone and iPad enabling instant access to documents on any of these devices as well as the ability to sync any changes made to a document. Keeping track of documents shared in the Cloud and beyond is often impossible. In addition, storing data and backing-up data at an acceptable speed is often costly, so while it is vital to keep back-up files, the increase in devices employees use inevitably increases the cost of hosting facilities. As it is not usually proportionate for an employer to sift through the wealth of data backed-up, the risk of capturing private data (such as for example holiday pictures, text messages or similar) is high. An employer does not want to pay for retaining unnecessary data, and so depends heavily upon the employee to ensure that corporate data alone is adequately backed up at regular intervals.

A further privacy concern relates to the ability to track the location of mobile devices (a feature which is commonly used by a number of apps). An employee may not wish his employer to track his whereabouts and store this data (even if not done on purpose), but as mobile devices are used for business purposes outside normal working hours it is impossible to be certain whether the employee is in fact on holiday or working. In particular the tracking of devices abroad will pose an additional risk to the employer as laws in other countries may prohibit the tracking or monitoring in this way. Employees have a legitimate expectation of privacy and whilst they may expect their internet usage to be monitored to some extent at work, may not accept this extending to the use of their own device.

An employer has to be clear about the scope of any monitoring it conducts and keep it within proportionate boundaries. It is subject to the Data Protection Act 1998 (DPA), and any data processing has to comply with its rules and principles. Failure to adhere to the legal requirements may lead to enforcement action being taken against the employer by the Information Commissioner (ICO) resulting in fines or reputational damage. For example, the Nursing and Midwifery Council received a £150,000 penalty in February 2013 following the loss of three unencrypted DVDs containing personal data. An employer may be prevented from being able to respond to a Subject Access Request under DPA, and risk a penalty, where data is held on a personal device.

Need for access

An employer may find it is unable to access data it needs. Emails and documents or drafts stored on private devices which are not properly backed-up (or stored in the wrong box folder), can expose an employer to risk in litigation if such documents can't be provided in disclosure. Financial penalties may be imposed by a court and critical evidence such as the "smoking gun" email or document can be missed resulting in a case being lost.

Clear policies

Given the risks and administrative burden of BYOD it is fair to question what benefits it provides, but much of the risk can be mitigated by strong HR involvement. There is an obvious need to safeguard commercial data and to put in place clear guidelines about the requirements for employees who wish to use private devices at work. As technology advances quickly, it is important to involve the employer's specialist IT team in devising a workable policy. It is equally important for the company to educate and train its employees on the policy so that the employee understands what is expected and the potential risk factors.

Dynamic training will cover a wide range of issues from both employer and employee's perspectives.

1. Employers will:

a. Use suitable technology to keep corporate data secure and confidential and consider appropriate access or download restrictions

b. Inform and train employees so that they understand the security and financial risks and know how to keep those to a minimum

c. Regularly consider overhauling the systems in place in collaboration with the IT team and employees in order to proactively react to new developments and changes in risk, and

d. Be clear about monitoring, sanctions for breaches of the policy and post-termination processes.

2. Employees will:

a. Store any private data in separate folders and clearly label them as private

b. Ensure that corporate data is regularly backed up

c. Not leave their device unattended and will use a pin or password, and

d. Engage in dialogue with the employer's IT team to discuss and resolve any technical glitches at an early stage.