Hybrid working: How to maintain data security

While many businesses plan to welcome more employees back into their offices as restrictions ease, a significant proportion of employees will continue to spend at least some of the time working from home. This longer term trend towards home working offers flexibility for staff and potential cost savings for businesses, but how can organisations ensure their valuable data is not compromised as their control over it decreases?

Security

Having employees working remotely multiplies the number of networks, applications and user interfaces through which data is accessed. These are the three main points in an IT system where data is most vulnerable so it is important that companies are mindful of the data security risk and put mechanisms in place to mitigate that risk.

At the most basic level, compared with PCs and networked systems, there is a greater risk that mobile phones and laptops could be lost or stolen and then used to access or store confidential company data. Also, as employees use devices for their own social purposes as well as for work, accessing websites and uploading photographs and other content, they could unintentionally infect their device with viruses or malware that could provide a backdoor into the company's systems.

Business should consider using 'mobile device management' (MDM) and/or 'sandboxing'. MDM technology enables the employer to remotely manage and monitor an employee's personal device (such as remote wiping and location tracking) and 'sandboxing' involves creating a secure section on the device to be used exclusively for company matters – which can be used to limit remote wiping just to company data.

IT teams should work closely with other stakeholders within the company to establish a structure which capitalises on the benefits of remote working and BYOD without exposing the company to unnecessary security risks.

Data Protection

Closely connected with security, is the issue of data protection. The Information Commission Office (ICO) has published updated 'working from home' guidance https://ico.org.uk/for-organisations/working-from-home/

This guidance provides some useful recommendations including:

- auditing the types of personal data being processed and the devices used to access that data;
- denying or restricting access to sensitive data on devices which lack a high level of encryption; and
- ensuring that remote access authentication is securely configured, where possible using multi-factor

authentication for remote access.

The guidance also provides that businesses should have remote locate and wipe facilities in place to maintain the confidentiality of data in the event of loss or theft and should, where possible, avoid the use of public cloud-based sharing and public backup services if the services have not been fully assessed.

Remote working arrangements can reduce the control which businesses have over their data, making it more difficult to determine what data is being stored where. This makes it harder for businesses to comply with their obligations under data protection law to record where data is being held and to delete, or amend that information in response to a subject access request. Mechanisms will need to be put in place to ensure businesses maintain visibility as to the location of their data.

It is important that appropriate security measures are put in place because the ICO can take action against organisations or individuals who fail to comply with data protection law. In 2017, a senior family law barrister was fined by the ICO for a data breach, resulting from her storing unencrypted sensitive files on her home computer. Across the pond (and considerably more expensive) in 2012 a company was fined $1.5m by US healthcare authorities for a data breach resulting from the theft of a laptop which held 3,621 patient records.

Shared work spaces

For many people working from home involves working in an area which is shared with other people and may even involve using computers and other IT equipment which is accessed by others. This sharing of work space and equipment brings with it an increased risk of breaches of confidentiality and data protection.

Where home working involves printing or handling documents and other tangible materials, staff must be given suitable facilities to store those materials and to shred them or otherwise dispose of them in a confidential manner when they are no longer needed.

Ensure no one is listening

It is important that when people are working from home they ensure that confidential information and personal data is not accessible to others (even family members). This requires them to keep documents secure and to ensure that computers are protected by suitable passwords / two factor authentication and that they logout / disconnect when they are away from the computer.

It is also crucial that telephone calls and video conferences which involve the sharing of confidential information or personal data are held in private. This not only means not holding calls in a shared space but can also mean disconnecting smart speakers or changing the privacy settings.

Smart speakers such as Alexa and Google Home have listening facilities to enable them to know when people are trying to activate them and these listening facilities can also be accessed by Amazon or Google employees for the purpose of 'improving voice-recognition features.' It is difficult for users to know whether their smart speakers are recording so it is advisable for home workers such as doctors, lawyers, social workers and teachers to change their privacy settings or unplug their devices when working to ensure that any confidential conversations are not inadvertently overheard or recorded by their smart speakers.

Licensing

Businesses seeking to introduce remote working arrangements should review their software licences to ensure they remain compliant with the licence terms.

The licensing implications of remote working and employees using their own devices can often be overlooked entirely, potentially putting the company in breach of its software licence terms. Or, companies can fail to fully consider the licensing implications until after they have committed to remove working arrangements, resulting in the company having to pay licence fees which it had not budgeted for. For example, access to Microsoft products from personally owned mobile devices or laptops may require the purchase of additional licences which may be calculated on a per device basis rather than a per user basis.

HR considerations

Allowing employees to work remotely or to use their own devices for business purposes raises a number of issues for HR departments.

Employers need to consider how the cost of the device is shared. Who purchases the initial device? Who pays any monthly contract fee? Who is responsible for anti-virus updates? etc. In some EU countries, employers are required to provide all of the tools that an employee needs in order to do their job. This means that an employer could be legally required to pay for its employees to have smartphones or other mobile devices if they become necessary for the employee's role.

A number of data protection and privacy issues will also need to be considered from an HR perspective. For example, to what extent can an employer have access to an employee's personal device (and the data stored on that device)? Is it easy for data to be segregated between company data and personal data? Is any kind of monitoring or audit access is going to be needed?

Another issue is what to do when an employee leaves the company. It is not easy for employers to make sure that any confidential or sensitive information has been deleted from their devices, particularly if an employee leaves on bad terms or goes to work for a competitor. Where a device will be the employee's personal property, and will be in the employee's physical possession, it will be difficult for that device to be accessed by an employer and for the storage of information on that device to be policed.

Remote Working Policy

It is advisable for companies to put in place a remote working policy which allows employees to access their own devices for work purposes and controls the risks associated with such use. The policy should detail who pays for what, how much control the company gets over devices and what happens if the device is lost or stolen or the employee leaves the company.

Main Tips For Getting It Right

As an increasing number of employees will now be working at home for some of the time, businesses should ensure that the following key steps are taken:

- Identify appropriate security measures to keep devices and data safe

- Review software contracts to identify any licensing issues and avoid unforeseen costs
- Communicate with staff via a clear policy that sets out: What staff can and can't do with their devices (including potentially what software they can use)

What level of control and visibility the employer may have over devices (so users know what to expect)

What happens if the device is lost or stolen, or the employee leaves the company.

- Consider using MDM and/or 'sandboxing' technology to enable the employer to remotely manage and monitor an employee's personal device.