masonadvisory

WHITE PAPER

BYOD – INVITING INNOVATION OR DISASTER?

What's the best way to deal with 'bring your own device'?

Overview

Apple Watch, Samsung Galaxy, Microsoft Surface – the list goes on. There are more mobile devices than ever. And it's only natural that people want these portable, practical devices to be part of their working lives. 'Bring your own device' (BYOD) is popular with employees – so much so that many of them may not even know there's an acronym for what they're doing. But it's there, every time they use the family iPad to access their work email or use their smartphone to log in to the timesheet system.

This white paper looks at the implications of BYOD for organisations. Will it lead to a flood of viruses, support issues, data leaks and legal worries? And even if it does, is there any way to stem the tide? We suggest that you can try and deter users by improving corporate equipment, look at alternative models of provision, or even prohibit it. But ultimately the most practical approach is to try to manage it.

1 Introduction

BYOD can take different forms: there's the deliberate decision not to provide corporate IT devices (for example, tech firm VMware – presumably as part of its marketing strategy – started a BYOD approach for its 6000-plus employees in 2012).[1] And then there's BYOD by stealth: employees using their own devices instead of, or in addition to, the equipment provided by their employer. Research suggests that as many as 60% of people in the UK are using personal devices for work.[2]

In many ways, this consumer-centred push for faster technological advancement is a role reversal. Traditionally, businesses were at the forefront of funnelling technological advancements, first to the workplace, then to the home, in order to support flexible working and greater productivity. Innovation is still taking place, but now, in many cases, the owners of the change are the employees themselves, pushing their consumer choices into the workplace. It's not surprising given that UK regulator Ofcom suggests over half of UK homes now have a tablet[3], smartphones have overtaken laptops as the most popular device for getting online, and new high-end devices are nudging their way into the market, such as the Apple Watch.

That means employees are now accessing their work emails on home laptops, tablets and smartphones. They're downloading files so they can use the operating system of their choice, and they're sharing files using Dropbox or Google Drive in order to access documents on the move.

There are many reasons people want to use their own

[1] VMware started with smartphones in 2012, and then expanded to a fully BYOD policy. Unsurprisingly the approach has been adopted by a number of IT corporations, including Cisco.

[2] http://www.acronis.com/en-gb/pr/2015/07/02-13-53.html

[3] This figure is expected to rise still further in the next year according to the regulator; http://media.ofcom.org.uk/news/2015/five-years-of-tablets/

devices. While many still prefer to keep work and home separate, others may prefer to use their own equipment because the set-up is familiar (Macs versus Windows for example), because they feel the performance from a high-end consumer device is better than what their employer provides, or because they like the convenience of a mobile device (e.g. being able to review documents on a tablet rather than carrying around their laptop).

The challenges of both these forms of BYOD are similar, but in the case of corporate-driven BYOD, it is likely that the risk has been assessed and addressed. With BYOD by stealth, there are concerns that neither the employees nor the company may understand the full extent of their exposure.

2 So can you do anything about it?

There are four main approaches to dealing with insurgent BYOD:

- trying to find other ways to meet the needs that make people turn to their personal devices
- offering alternative models that provide some of the benefits of BYOD
- prohibiting it
- managing it.

These options are explored below.

Meet the need with corporate devices

Given the reasons why people opt for BYOD, IT departments can consider trying to address some of these needs through corporate equipment. Macs versus PCs and the desire for tablets as a more portable device are two of the areas where businesses can look to improve their corporate provision. Private and public-sector organisations are responding with trials of some high-end products, and companies are looking at working with hybrids such as Surface tablets with keyboards or the Lenovo Yoga laptop-to-touchscreen devices. The iPad Pro – a larger version of the consumer product with a desktop-class spec – may be another option (but at what cost?).

For many employees, a more consumer-style device will be enough, but others will still want the choice, and those who already own their preferred device don't want to carry around a second (corporate) device as well. There is also the cost involved for employers which may not want to fork out for the latest fads or for secondary devices such as tablets that may be seen as 'nice to haves'.

Look at alternative models

Where greater choice appeals to employees, but BYOD is a bridge too far, organisations are looking at other models such as 'corporately owned, personally enabled' (COPE) or 'choose your own device' (CYOD). These have been touted as the 'best of both worlds' for corporate mobility.[4] They allow companies to get the benefits of BYOD, but retain ownership from a legal perspective, as well as being able to leverage economies of scale in contract negotiations. The company provides a handful of models which should be able to cover employee hardware demand and provide compatibility for years to come.

However, the choice is, necessarily, limited, and again staff may not be convinced of the benefits of adding a corporate device to their personal collection.

Prohibit it

In the public sector, national accreditors don't like unmanaged devices and would rather see them off the scene entirely. And in the private sector, risk averse CIOs are loath to take on any more liabilities than they are absolutely required to (no one wants ICO fines for losing personal data, for example). Perhaps then, the easiest approach is just to stop people from using personal devices. But is zero tolerance realistic?

It's incredibly difficult to monitor use and enforce such a policy. The government's own advice from CESG states that an over-restrictive approach "may encourage staff to find workarounds which increases security

[4] http://www.theguardian.com/media-network/media-network-blog/2013/apr/24/corporate-owned-personally-enabled-cope-byod

risk".[5] So is it better to acknowledge the risk, and manage it?

Manage it

Given that it's almost impossible to stop people from using personal devices – particularly where they're using cloud-based systems – it may be better to recognise the challenges and work with employees to manage the risks.

The key issues are:

- data security
- increased support overheads.

Data security

This is the main concern when it comes to BYOD. When employees are accessing information in the office – on corporate hardware – limiting their access in terms of file sharing and Internet usage is relatively simple. But with personal devices, control is lost. The device is owned by the user, but the legal responsibility for the data on the device lies with the employer – the 'data controller'.[6] This is particularly important in terms of personal data – data about employees and consumers – for which the data controller must ensure that "appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data".[7] Although there may be direct legal threats from loss of personal data, loss of corporate data can be just as damaging, particularly where organisations have to protect their clients or there is a public interest.

The data controller will need to consider whether a personally-owned device can be effectively managed by the organisation for the complete duration of its access to company material. Organisations also need to assess the implications of security incidents: what would happen if a non-company-owned device was lost or stolen, for example? There is also the risk of inadvertently sharing corporate information, such as automatically syncing corporate files to Dropbox accounts on shared personal devices.

Increased support overheads

BYOD may seem cost effective, with people taking responsibility for their own devices, or even supplementing corporate equipment with their own. However, managing this increased ecosystem effectively can be difficult: more manufacturers, more models, more platforms and so on.

These problems are compounded when you remember that devices have to be able to access corporate – sometimes proprietary – systems. Compatibility issues can be extremely challenging, and have to be factored into application planning.

If organisations are going to assess and address both these risks, they need to have a combination of policy and technology to support BYOD working.

3 Policy and technology

IT departments need to develop a clear, pragmatic policy, with a small number of red lines, so that they can be understood and enforced. This policy needs to be communicated properly to all staff. The policy must be in line with legislation (including the right to privacy of employees), and there is a significant amount of official guidance available – including from the government and ICO – on how to best to implement BYOD policies.

For a policy to work, it should:

- encourage good practice (e.g. suggesting presenting information rather than storing it locally)
- be backed up by practical processes (e.g. easy ways of securely sharing information with colleagues)

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360959/BYOD_Guidance_-_Executive_Summary.pdf
[6] https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary
[7] https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

- be enforceable (e.g. can you audit the data stored on devices?)
- be supported by technology (e.g. could the IT team revoke access to business systems if a device were lost or stolen?).

Technology is difficult because there is only so much control an organisation can have over personal equipment, but IT departments can explore container applications and mobile device or application management to support their policies.

4 Conclusion

Most businesses are unable to stop personal devices from entering the workplace. Businesses should look at the motives behind staff bringing IT into the workplace, and may need to reconsider the hardware they are providing. But there doesn't have to be a draconian response to BYOD. Many organisations with significant security requirements can allow employees genuine freedom. They just need to have a robust policy and technical measures in place to protect themselves, their employees, and their data.

About Mason Advisory

A simple approach to complex challenges: Mason Advisory is an IT consultancy that does things differently. We're experts in IT who match technology know-how with commercial and business sense.

Businesses come to us because we solve complex business challenges through intelligent use of IT. We're here to help clients set their strategy and then deliver on those decisions.

Mason Advisory offers something a bit different from the traditional consultancy model: our clients know they'll get experienced teams where every member can quickly add value to an assignment.

And because we're independent, you know you can have confidence that our conclusions meet your needs. For 20 years, organisations of all sizes have trusted our consultants to deliver IT with an impact.

Contact us

If you would like to discuss how we can support you please email contact@masonadvisory.com or call +44 (0)333 301 0093.

www.masonadvisory.com