CEO's Briefing

Bring your own device to work (BYOD)

Why buy kit for your staff when they would happily pay for better stuff themselves?!

Many staff use their technology routinely for work, a trend that's called Bring your Own Device (BYOD). For example, most people use their own phones for work. Often senior management use their own ipads, and some people even bring their own laptops into work as well.

Certainly, when people are working from home they will use their own kit when it suits them, whether this is dealing with occasional evening emails, or routinely working from home for several full days per week.

Many of the devices that people buy for themselves will be better and more modern than the kit provided for them in the office. And staff will normally be more familiar and productive with their own devices.

CEOs note this trend and ask why they can't simply tap into this to reduce costs! Why buy kit for your staff when they would happily pay for better stuff themselves?!

Of course, it's more complicated than that but, all too often, the conversation becomes bogged down by resistance from the IT guys who see endless hurdles and loss of control.

The result is sometimes an absurd refusal to engage with this opportunity or to support it, or even acknowledge that (according to Gartner) as many as 50% of employees will be using their own device for business regardless.

Mismatching expectations

The consumerisation of technology has led to a blurring of the distinction between personal and business technology. Many people have a very strong personal connection with their technology and, especially for millennials, is an important part of their life and self-expression. There is a growing expectation that these devices can be used at work with impunity.

FREEMAN CLARKE

contact@freemanclarke.co.uk
0203 020 1864

CEO's Briefing

> "BYOD will almost always be a negative experience when it grows in an ad-hoc fashion, without controls and at the behest of the individual."

> "...employees will gain productivity and satisfaction from using their own devices. ."

But your IT department may have very different views about what devices can be attached to your corporate network, your HR people may have questions about policies and legalities. And all of this can put the issue onto the "too difficult pile" – when actually it's going to happen whether they like it or not.

IT teams are used to carefully assessing and selecting devices and a key objective for them is to standardise and simplify the purchasing, setup and maintenance. This has become a critical factor in their drive to reduce costs, to minimise problems and to ensure security. So, from their point of view, a proliferation of different devices beyond their control is a completely alien idea.

Why should you care?

BYOD will almost always be a negative experience when it grows in an ad-hoc fashion, without controls and at the behest of the individual.

But companies who think through the consequences and put in place methods to manage the situation see benefits such as:

- Reduced technology capital costs because there's less user-technology to buy
- Improved productivity with staff using devices they like which will probably be more powerful than those offered by the business and they're happy to always carry them
- Reduced employee frustration around technology because they can choose what they want to use
- Improved flexibility of working including the ability to work at home or on the move
- Business services move to the cloud to facilitate increased mobility and connectivity

Personal devices are usually going to be newer and more advanced than the equipment you offer as part of the standard package. Therefore, BYOD means your employees have access to more powerful equipment without increasing company spend on technology.

There is no doubt that your employees will gain productivity and satisfaction from using their own devices. They are likely to be more mobile and more connected. A Cisco Internet Business Solutions Group found that BYOD users saved an average of nearly 40 minutes a week thanks to using their own device. The report also found that staff adopting BYOD start their work day earlier and work faster when using their own devices.

Working from home becomes a lot easier to achieve because staff will have devices that are set up for work, are mobile and easily brought to/from work. DR/BCP plans are also enhanced because staff will always take their devices home at the end of the day rather than leave them in a drawer.

What's my risk with BYOD?

BYOD is not without risk to the business and our clients have found that the main topics that they have had to consider, and resolve are items such as:

- Company data residing on personal equipment outside your direct control
- Increased risk of cyber-attack because the personal devices don't necessarily have appropriate security

FREEMAN CLARKE

> "Loss of data remains the company's responsibility whether it's on a company owned device or their employees."

- Increased support overheads every device is different, and issues may take longer to resolve

- Staff feeling obliged to be 'always on'

Staff need clarity

The always-on issue is a significant cultural question; what is your expectation if you email one of your team outside normal work hours? Well-motivated staff who are highly engaged with their work may enjoy sending occasional emails outside hours. It can reduce their stress if they have access to the network from home so they can be at home for an important delivery but still get their work done. But the absence of clarity and policies can lead to an ever-expanding working day and increased dissatisfaction and resentment.

Of course, security

A survey by Trend Micro revealed that nearly half of companies using BYOD have reported data breaches. The proliferation of company data outside the confines of the business stored on personal devices must be cause for concern but the genie is out of the bottle, you can't block BYOD – it is far better to ensure that where it exists, it is well managed.

Loss of data remains the company's responsibility whether it's on a company owned device or their employees. The employee is only partially responsible and the Office of the Information Commissioner (ICO) is going to be looking to the company, not the employee when there's a data breach.

Staff may be using a phone for a task as simple as reading company emails whilst on the move. But this might mean your whole customer database is sitting on their phone as well. Which is obviously an issue if they leave it in the pub.

It also becomes a lot harder to control how a device is used when it isn't owned by the company. It's easy to set a code of conduct with business owned devices, but when it's the employees personal device, that becomes a lot harder. For instance, many companies block the use of gambling websites on their technology, but that's not necessarily an appropriate mandate to place on a personal device.

It is therefore important to embrace the fact that it is happening and then ensure that there are the proper controls in place. We recommend that a standard risk/ benefit analysis is conducted to understand how BYOD is impacting the business now and in the future and make some sound business decisions from the results.

BYOD and Security can play together

Making BYOD and the security of your data work together is possible, but it needs to be considered carefully. There are a number of questions your IT team will need to ask when preparing BYOD guidelines:

> "There are a number of questions your IT team will need to ask when preparing BYOD guidelines."

- What data should be accessible on personal devices?

- How is that data stored on the device? And for how long?

- How can the data be secured and encrypted so it is safe?

- How is data being moved between personal device and the central systems and how is data integrity maintained?

- What is the process of removing corporate data from the personal device (for

FREEMAN CLARKE

> "The Starter/ Leaver process will be an area that will need significant review, particularly to ensure that leavers' devices are clear of all company data."

example if it's lost or the owner leaves the company)?

- What software licences are being used and have they been gained appropriately?

Employees should be provided with a framework within which they can use their own devices. This should include areas such as:

- Maintaining company data separate from personal data
- Ensuring the device has adequate security on it (PIN, Fingerprint, etc)
- Ensuring the device has security software on it, i.e. Anti-virus, Anti-malware, etc
- Not sharing company data outside of the company
- You have a right to wipe company data from the device at any time

Being able to wipe company data from an employee's device is an absolute necessity. However, no employee is going to be happy with a process that resets their device back to factory settings so a more granular approach is required, but one that still gives you the reassurance that none of your company data is left on the device when the employee leaves or if they lose it.

In order to manage BYOD appropriately your IT people will need to understand whether their technology offers this granular approach. (Microsoft Office365 has recently moved to embrace this issue.)

The Starter/Leaver process will be an area that will need significant review, particularly to ensure that leavers' devices are clear of all company data. Starters though need to be aware of the policy before joining, particularly if it is a company wide policy otherwise they may start without technology and therefore be unable to work.

Resistance from the IT team

Many internal teams or external IT support providers contracts are setup to support standardised technology rather than a proliferation of different types of hardware and software. Because all the devices will be configured and set up in different ways, often with the user having full administrator rights, it's difficult to provide fast solutions to major issues with rebuilds and software rollouts being particularly troublesome. As a consequence, there may be additional support costs associated with BYOD.

And two tribes may form ... the Apple tribe vs the Microsoft and Android tribe. This can cause further support challenges and can create new difficulties particularly with sharing documents between staff and teams.

BYOD is more difficult where you have older systems that require installation of software (clients) on each user's PC. More modern software follows a "web app" architecture and relies only on the user having a standard browser. These kinds of systems don't require your IT team to roll out software to users' laptops and are more likely to be compatible with a broad range of Apple or Windows laptops so long as they use a standard browser like Internet Explorer (or Edge), Chrome or Safari.

Finance and HR policies

BYOD can make the Finance team's task a bit harder, particularly around mobile phone use and the additional workload from managing expenses with mobile phone calls. Employees need to be aware of the tax implications of using their own mobile phones for business calls, and of the practicalities of what they can and cannot claim on expenses. For instance, if they are using an all-inclusive package, they cannot claim for individual business calls. There are however applications that can be used to separate business calls from personal calls to reduce the pain.

FREEMAN CLARKE

> "...some adoption of BYOD in the workplace is inevitable and has probably already happened in your business. ... it must be recognised and managed appropriately and it can be a positive force to help you reduce costs, increase productivity and increase job satisfaction."

Increasingly companies are expecting the employee to cover the full cost of the technology they want to use for BYOD, however some do provide each employee with an individual budget. Where the device has been financed fully or partially by the business, then the ownership needs to be made clear.

There are HR implications as well and these kinds of changes will need to be explained to employees, and covered during the process for new recruits.

Summary

Whether your IT, finance and HR teams like it or not, some adoption of BYOD in the workplace is inevitable and has probably already happened in your business. As a consequence it must be recognised and managed appropriately and it can be a positive force to help you reduce costs, increase productivity and increase job satisfaction, especially for younger workers.

The IT support and security issues are real and your team (or external supplier) need to be challenged to have a clear strategy for dealing with this. In addition, the HR and finance teams need to amend and extend their policies and support to make this a positive step forward.

You may also find our briefing on 'How to make home working work' relevant if this has been helpful. You can access this by following this link.

Freeman Clarke
The UK's largest and most experienced team of fractional IT Directors, CIOs and CTOs

Phone
0203 020 1864

Email
contact@freemanclarke.co.uk

Locations
London & South East
Thames Valley
Southern Home Counties
West Midlands
East Midlands
North West
North East
Singapore