Should you allow your employees to bring their own technology to work?

August 2014

Camford

Resolving Business Challenges Through Technology

Should you allow your employees to bring their own technology to work?

Known by a number of terms such as Bring Your Own Device (BYOD), Bring Your Own Technology (BYOT), and IT Consumerisation, the trend in allowing employees to use their personal technologies in the workplace can't have escaped any business.

BYOD has grown about from the simple fact that business technology, and IT departments, have not moved quick enough. Consumer technologies have overtaken business technologies. This has been driven through the continual reduction in technology cost, the explosion of mobile device use (reaching **7.3 billion devices** in 2014 according to a Silicon India report – greater than the world's population, and substantially greater than the number of people who have toilets!), and the growth in mobile apps (data from analytics provider Flurry shows that users are spending an average of **2h 42m** on mobile apps each day – I wonder how much of that time is on Facebook!).

7,300,000,000

According to a Silicon India report there are now 7.3 billion devices in use globally

Still, I'm not so sure BYOD is a new trend. I remember executives getting new PDA's at Christmas over 15 years ago, bringing them into the office, and then expecting the IT team to make them work. And the IT department had little say in the matter.

The difference today is that everyone wants to use their own technology, and its not just hardware, but apps too.

What have we seen so far?

Interestingly, BYOD has taken off much more in the US than it has in Europe. According to John Delaney, who heads the European Mobility Team at analyst firm IDC, *"Only one-third of companies in Europe have BYOD policies, and there's no increase being seen in the number of companies planning to adopt BYOD in the near future."*

Instead what we've seen is some rebranding, with terms such as *'Choose Your Own Device'* (CYOD), where users are offered a small choice of different devices to suit their needs. Again, I don't think there's anything new here to what's always been done, apart from branding and positioning. In fact, according to a 2013 survey, **82%** of employers allow some or all of their employees to choose their own device.

82%

of employers allow some or all of their employees to choose their own device according to a 2013 survey

But isn't this missing a trick? From my own experience, the last time I received a new laptop from the IT department it was the first time I'd possessed an item of technology that I truly didn't want! The IT department's rationale was that this new laptop was more powerful, had a larger screen, an in-built DVD player, and it was cheaper. It was also MASSIVE. The IT dept. hadn't taken into account my primary needs, which was a small, lightweight laptop. CYOD might have addressed my concerns to some degree here.

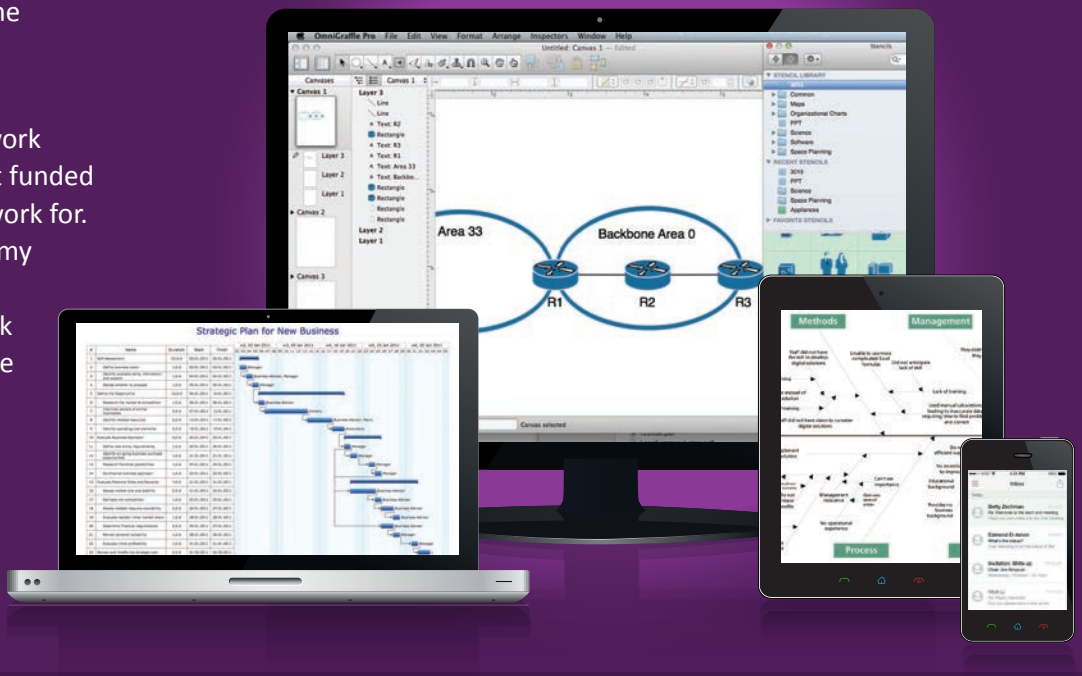
Since then I've moved on and now bring my own device to work (MacBook Air), which was part funded by the organisation I used to work for. The best thing about bringing my own device is that if I need an app to do something, I can look one up on-line, install it, and be using it within minutes.

I've done this three times in recent weeks:

- When I was looking for an app that could create fishbone diagrams
- When I needed an app that could open up Microsoft Project files on the Mac
- When I wanted to edit a Microsoft Visio file I had been sent

But you'll have noticed this laptop was part funded by my employer at the time. According to the research from IDC, *"BYOD adoption has reached a plateau [in Europe]. One reason is that employees expect companies to pay for a mobile device that's becoming the primary tool to access systems and data."*

This view is perhaps driven by employers who are looking at BYOD in the wrong way. BYOD was seen by some as an opportunity to save money, and so in funding part or all of the purchase the view was that the overall cost would be lower. But I didn't want to bring my own device to save my employer money, I wanted to give myself agility, and to empower myself to be able to make my own choice on the applications that I needed.



That sounds risky!

The notion that you would allow each and every business user to make their own choice of hardware and applications sounds crazy. And if you look at it that way, it is!

But that's not what I'm saying. There is, and will always be, corporate apps that must be managed and controlled to ensure data is harvested, maintained, distributed, and secured. But there's also a significant number of activities that don't require this same rigour.

"The substantial gap between the business computing environment and the consumer computing environment is traditionally explained by reasons such as culture, security and compliance."

Matthew Cain, research vice president at Gartner says, *"The substantial gap between the business computing environment and the consumer computing environment is traditionally explained by reasons such as culture, security and compliance.* It is these assumptions that must be challenged."

The primary challenge in allowing BYOD for any business is one of risk. Security risk; risk of support complexity with so many devices in use; risk of increased costs; and risk of dissatisfied employees when the IT department can't fix their problems. However, like all risks there are a number of ways you can mitigate them. Taking standard risk management principles into account, there are two types of risk – threats and opportunities – and a collection of ways in which they can be mitigated as shown in the table below:

Threats				Opportunities			
Avoid	Reduce	Accept	Transfer	Share	Enhance	Exploit	Reject

Let's take each one in turn...

Threat: Avoid

This is probably the number one approach being adopted to BYOD – not permitting the business to use its own technology. But what of your competitors? Are they stealing a lead because their employees have more agile technologies? Are your employees frustrated because the IT department is holding them back? Or, have you growth in Shadow IT that you don't even know about?

Threat: Reduce

The second most common approach would include initiatives such as CYOD. Reducing the threat, or the desire at least, by offering something else. This may work in the short-term and it does ensure IT remains tightly in control. It may also be the most appropriate step for a large number of job roles. But as I said earlier, I don't think this really tackles the issue so much as rebrands what IT departments have nearly always done – provide a limited choice.

Threat: Accept

You can view this form of mitigation in one of two ways: It either sounds very scary, and as though the IT department has surrendered, or it sounds forward thinking and the IT department has accepted the inevitable. But acceptance on its own is not enough. The IT department cannot afford to simply accept that employees will bring their own devices, and not do anything about it.

Threat: Transfer

Now here is where things start to get interesting. The risk can be transferred in a number of ways. The IT department could, for example, stipulate base requirements that employees need to meet to be able to use their own technology. For example, it should be insured, the hard disk must be encrypted, a support policy must be taken out, it must have anti-virus software installed and up to date, so on and so forth. So the risk is transferred, in part, to the employee. This might include the risk of support in that the IT department will support the applications it provides, but all apps and devices not provided by the IT team would essentially be out-of-scope from the Service Desk, or maybe on a 'best endeavours' basis. So the risk is transferred back to the employee.

Threat/Opportunity: Share

Sharing the risk is a natural enhancement to transferring it. Whilst the employer and the IT team can stipulate a number of base requirements, the general risk profile of the IT environment will have increased. Therefore the IT department will need to put into place technologies and tools to protect the business. For example, segregating the network so that personal devices are subject to stricter control. Installing tools that allow a mobile device to segregate corporate from personal apps and data, etc.

Opportunity: Enhance

As we start to see BYOD as an opportunity, the IT department can enhance or encourage its use. From an IT department perspective the opportunity here is to encourage the use of BYOD through simplification. The easier it is to use, the greater the adoption. Additionally the IT department could provide the business with advice and guidance on technology choice. This might include choosing specific platforms to offer greater support on, such as Android or iOS.

Opportunity: Exploit

The greater opportunity and benefit to the IT department is to exploit the change in user behaviours. Traditionally a new application rollout would need to be carefully planned, and in many cases would require a visit to the desktop, or the returning of a mobile device, for updates to be rolled out. All of us are now familiar with upgrading applications on our phones, tablets, and even desktops and laptops. In providing corporate apps in a similar way to the Application stores of Google, Apple and Microsoft, we can enable users to upgrade apps themselves and in their own timescales. We can also enable users to identify and choose to install apps themselves, thereby increasing take-up of an app and subsequently its return on investment. Instead of viewing BYOD simply as an unacceptable risk, the IT department should also focus on how it could benefit.

Opportunity: Reject

To reject an opportunity risk is, according to the Prince2 manual, *'A conscious and deliberate decision taken not to exploit or enhance the opportunity'*. It also goes on to say that the opportunity should continue to be monitored. This is perhaps where many organisations are right now – waiting to see what the industry does, or what their competitors do. But there's always a danger here that you wait too long!

So what should you do?

The research organisations such as Gartner are starting to take a different approach. Rather than focusing on a specific technology (which is fast becoming an out-dated attitude), they are positing a more holistic approach.

Gartner has coined the term *'Business Consumer'* to refer to, *"individuals who do not stop being consumers when they go to work. Business consumers often make more consumer-like choices in their workplace computing tools and styles to increase efficiency."*

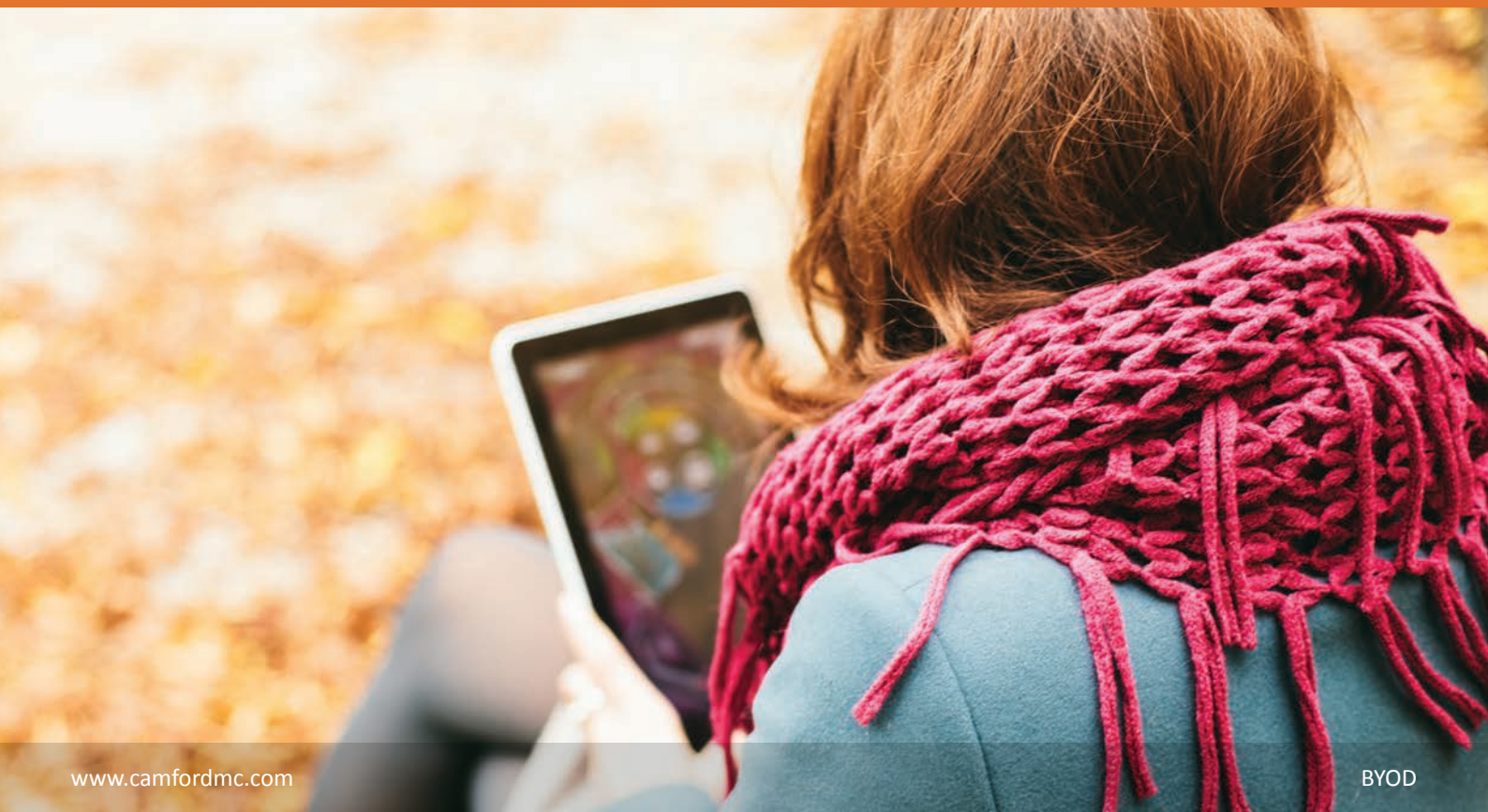
Business Consumer: "individuals who do not stop being consumers when they go to work. Business consumers often make more consumer-like choices in their workplace computing tools and styles to increase efficiency."

Gartner goes further to say, *"Given the complexity of work environments and the geographic distribution of expertise across organizations, a critical competitive advantage will accrue for businesses able to create a socially active workforce that can tap internal and external knowledge and expertise easily."*

It's easy to see the benefits of this approach as technology changes outside of the traditional business world continue to progress at a rapid pace. If I look to my own experiences, if there's something I'm trying to do I often start by looking for an app. This can be for a simple task such as scanning a business card I've been given to save me the time of typing it out, or as I did recently when researching law firm technology choices, downloading an app that provides relevant business intelligence for free! In each instance I used tools to support my search such as posing questions on LinkedIn, searching Google, and looking at App Store rankings.

So with BYOD what we're actually trying to do is:

- Encourage consumer behaviours in the workplace
- Enable employees to make their own short-term app choices
- Provide a dual-environment – one that is relatively static and secure, and one that is volatile and less secure but provides greater agility



Where to start?

We have a bespoke tried and tested framework, which we call *i5*, for the delivery of all of our engagements. It is adaptable to a wide range of situations and we would recommend you do something similar. Our framework is as follows:

Initiate

Like all initiatives, the first thing to do is to determine a Vision. Before you head off looking at solutions, determine what the vision is you are trying to achieve. The 3 bullet points above might be a good starting point for you, or you may have a different angle.

Investigate

Once you have defined your aims, undertake research to determine:

- What solutions are currently in use within your own organisation
- What others have done
- What the research organisations such as Forrester, Gartner and IDC are saying
- What solutions are currently available

Inform

The conclusion to your investigation should be a review of the solutions available and applied in the context of your business, including analysis of the likely costs. We recommend this be collated in the form of a Business Case in order to seek funding approval.

Invest

The next stage is the procurement of the solutions that you have identified as appropriate for your business. The Business Case should be continually reviewed to ensure that it remains valid and that the initiative should proceed.

Implement

Implementing the technologies and measuring that they deliver the benefits as defined in the Business Case can be a significant undertaking.

In taking the holistic approach recommended it is likely that any solutions will touch a number of different technology domains. We strongly recommend the adoption of a relevant project management framework, such as *Prince2*, and tailored to the needs of your project.

Conclusion

In conclusion, BYOD initiatives can bring tangible business benefits, and in our view it is an inevitable direction for IT organisations, and for employers to offer to their employees.

The focus, however, should not be on how to provide a specific technology, but a more holistic view as to how a combination of technologies and processes can provide employees with agility through empowering them to, in part, manage their own IT. This holistic approach should be tackled methodically, starting with the definition of a vision, as without which you risk simply deploying a technology.

One final point...

BYOD may not be suitable for everyone in your organisation. Whilst we see providing the ability as inevitable, that does not infer that it would be organisation-wide. One of the greatest challenges in IT today is the needs of the Marketing and Sales departments. These are areas where quick wins may be found and we would recommend that those functions be considered in your initial investigation.

Good luck in your journey to a *'Digital Workplace'*!

About the Author

Martin Williams is the Founder and Practice Leader at Camford Management Consultants.

He is a well-respected IT strategist and Programme Manager, with a clear focus on ensuring technology resolves business challenges, and that an organisation's IT function delivers value. Over a 20-year career, Martin has worked for a range of organisations, large and small, with a portfolio of clients that has taken him all across the globe. Martin can be contacted at martin.williams@camfordmc.com