Bring your own computer
Why should we have separate devices for home and work?

The consumerisation of enterprise IT is real. IT departments can evolve, or face extinction. Many knowledge workers already use non-sanctioned applications for their work. Why not embrace this revolution and actually encourage people to use their own devices?

The consumerisation of enterprise IT

The world is changing and, sooner or later, every organisation will run up against the phenomenon known as the consumerisation of enterprise IT.

Some have attributed this change to a new generation of workplace entrants – variously known as "Generation Y", "Millennials" or the "iGeneration". Except it's nothing to do with generational attitudes – it's about people who want to get their work done – and for whom the internal IT organisation is just not responsive enough.

For many IT departments, this is the stuff of nightmares – "users" demanding that they be able to use their iPads, MacBooks, Android phones, etc. to access corporate applications and data. But it's not about devices either...

IT consumed as a service

Prior to the emergence of the world-wide web, *users* did what they were told to – making use of the hardware and software that the IT department provided. Now the dynamic has changed: the boundaries between work and play have eroded and, for many knowledge workers, there is no clear separation between business and personal tasks. Work has become something we do, not a place where we go, and those "users" have become *consumers*.

Consumers want to feel empowered – they desire flexibility, personalisation and immediate gratification. Our information workers want IT to work for them, in the way that they need it to work. They desire a portable, device independent, always-on (and instant-on) modern working environment that provides access to information from any device (including data synchronisation), with self-service subscriptions to provide access to application stores/portals and personal/professional persona management. If that sounds challenging, they are used to this in the consumer space – now they want it in business and a sizeable proportion of employees are circumventing IT policies to self-provision at least a part of their IT toolkit.

Just like our banks, social networks, recreational websites and email, the organisational IT department has become a service provider. Furthermore, if the IT department can't provide a service, consumers are happy to go elsewhere – leading to the emergence of what has become known as *shadow IT*.

Sometimes this shadow IT grows out of the need to do something that's not possible on the corporate infrastructure (like using Dropbox to share a file with a colleague in another part of the world); and sometimes it's officially sanctioned (for example, a business unit director deciding that salesforce.com is a more appropriate CRM solution than the IT-provided line of business application).

Regardless of the source of the shadow IT, it takes a brave CIO to try and fight it. Whether the approach is to embrace, contain, block or ignore, consumerisation is a trend that's increasingly difficult to avoid.

Bring your own

Bring your own (BYO) computer (sometimes referred to as bring your own device) is a model that many suggest could provide a middle ground to address the needs of both the organisation and the consumer of end user IT services. The principle is that, instead of being provided with a company-supplied personal computer (typically a notebook PC), employees may use their own device (or even devices) concurrently for business and private use, with IT controlling the services provided, rather than the operating system and applications installed on the hardware.

This model doesn't just apply to new entrants to the workplace: it impacts many of today's mobile workers who are confused or annoyed by having separate "work" and "home" devices (PCs or phones) and who want to simplify their IT, consolidating personal and corporate computing onto the same device(s).

The idea is not new – parallels could be drawn with moving away from dedicated ISDN lines for remote workers to VPN over home broadband – and, whereas once it was inconceivable that a non-corporate device could be connected to the company network, many organisations have guest networks (generally wireless) for use by visitors, external consultants and business partners. A BYO model extends this to employees, with appropriate controls on data and network security. In some organisations, it's already common practice to allow employees to provide their own smartphones; extending this to personal computing is a logical next step.

Potential benefits

BYO computer is an exciting model with a number of potential benefits for the consumer, the business, and the provider of IT services.

For the consumer, the benefits include:

- Ability to use a device that fits their needs and style.
- A better user experience and higher user satisfaction, primarily driven by the ability to work from any location (for example, allowing "family-friendly" work) together with the reduced complexity and increased convenience of using one device (rather than maintaining separation between personal and work personas and activities).

For the business, potential benefits are:

- The impression of a modern employer with progressive attitudes to work (i.e. more attractive from the view of recruiting and retention).
- Shortened and simplified provisioning – if a new device is needed, it can be as simple as buying one from a high street retailer.
- A reduction in hardware assets owned – as the capital expenditure relating to devices moves from the business to the employee.
- A flexible workforce, able to work remotely (possibly allowing a reduction in the cost of providing office space).
- Breaking the divide between "work" and "home" means that employees work an extended day, with breaks to suit their lifestyle and consequential productivity increases.
- Fewer devices are lost (employees take greater care of their own devices).

From the IT department's perspective:

- There is no requirement to manage the lifecycle of non-strategic assets.
- Providing that the appropriate infrastructure is in place, BYO allows the removal, or at least sandboxing, of on-device data, thereby mitigating a number of security concerns.
- Device proliferation with ever-shorter lifecycles is no longer a concern.
- Fewer support calls as the user knows their device – IT departmental support is reduced, perhaps simply to application services, typically via a browser or a cross-platform client application.
- No complaints about aging equipment and poor performance (consumers upgrade their hardware at will).
- Cost reduction, including the avoidance of many costs associated with "desktop" technology refreshes. Training requirements are also simplified as they become concerned only with applications and processes.
- Enablement of shared service provision (i.e. provide IT services to employees, partners, customers and suppliers).
- Ability to focus on strategic projects.

Challenges

Of course, BYO is not without its challenges too. These are primarily concerned with a perceived loss of control in two areas: security and manageability.

On the security front, the major considerations are: the protection of corporate data from corruption, misuse or theft; enforcing security policies without compromising ease of use; and meeting compliance demands.

For manageability the concerns are: application compatibility, remediation and deployment across a diverse range of devices; defining responsibilities for support (of hardware, software, data); what to do if a device fails; maintaining control (e.g. of the network).

Taken at face value, these can make BYO seem complex, dangerous and expensive but, in many cases, the technology already exists to overcome these issues.

Some technologies that may help

An established example of technology that allows a form of BYO computing is the use of secure tokens and a portal of web-enabled applications for remote access. This scenario has been used for many years for occasional access from home PCs, Internet cafés, hotel Wi-Fi hotspots without VPN support, etc.

These days, many IT departments are focused on investments in desktop and application virtualisation. After all, virtualisation provides what some refer to as the "separation of church and state" – keeping work and personal data detached from one another, and removing many dependencies on the operating system and hardware.

But virtualisation takes many forms – it could be locally hosted but that relies on the consumer installing specific software on their workstation, something that may bring challenges in licensing and data security. Similarly, application streaming (combined with enterprise application stores) may assist in providing dynamic application delivery but has constraints around licensing, security and application compatibility. Hosted virtual desktops are a popular model for BYO, as is virtual desktop infrastructure – from the CIO's perspective the data is secured inside the company datacentre and the devices used to interact with it become irrelevant. These technologies rely on a network connection though – which means they work in metropolitan areas with high levels of mobile data coverage (3G and Wi-Fi), or in home/office environments but can be a challenge when travelling or in a rural location where ubiquitous network coverage may not be available.

From a network connectivity standpoint, technologies such as Network Access Control (NAC) exist to ensure the health of connected devices, making sure that the latest security patches, anti-malware updates, etc. are in place.

Even if some data is confined to the corporate datacentre and accessed remotely, users of devices such as smartphones and tablets will expect certain information. At a minimum they expect email, contacts and calendar appointments to flow onto the device. This needs to be secured, with provision for remote wiping of the device (or a portion of the device). It also makes sense that this model is equally applied to other BYO devices (netbooks, notebooks, home PCs, etc.) but consumers are far less likely to allow the company to remote wipe their PC than they are their smartphone. Even for smartphones there are complications when a company administrator wipes personal data (pictures, music, etc.) along with the company data. Legitimate remote

wipes may be covered by IT and HR policies – but what if it's an administrative error?

It's about people and process too

Introducing a BYO model to end user computing is not just about the technology though.

Consider that there may be chargeback implications. Essentially the business is offloading some of its responsibility to its end users and many organisations consider it appropriate to provide a financial stipend to employees. This is analogous to the shift from providing company cars to providing an allowance to run a car that's available for business use. Others may simply issue guidance as to the types of devices that will work with the company infrastructure.

There are HR and legal implications too – what happens if the employee leaves the company, for example? What rights does the employer have to control data on the employee-owned device? What processes are in place to ensure the protection of data, mitigating the risk of on-device documents and profile data? What happens if there is a security breach – provision may be required to confiscate the employee-owned device to facilitate investigation? Consider what happens where specialist hardware and software is required for a disabled employees (who bears that cost)?

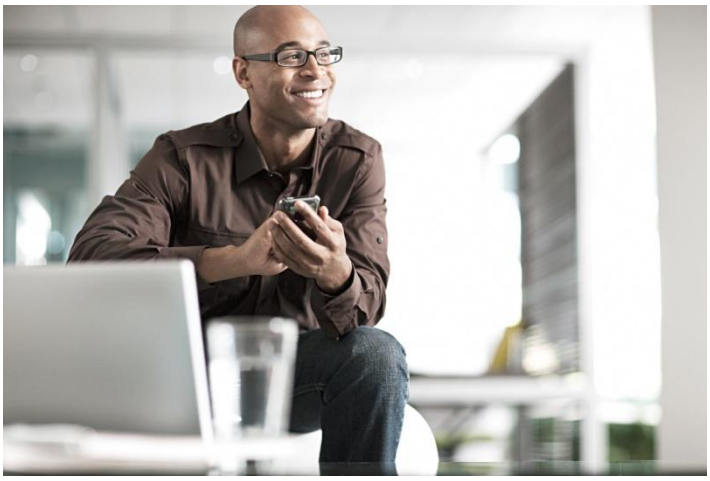
There may be opportunities to create partnerships to assist with the procurement and support of BYO devices – perhaps an online catalogue using corporate purchasing power to drive down costs to individual consumers for device purchase, together with "approved" security/office productivity software and a maintenance agreement? In time, these infrastructure elements will become less of a concern (as described in the following paragraphs) but, for now, they are considerations for many organisations taking a step towards BYO. The changes may take many years, moving from physical to virtual infrastructures on the way to a device-agnostic end user computing model and it will often be necessary to support a hybrid environment on the way.

Supporting BYO

Whilst it would be great for the IT department to wash its hands of BYO devices and require that consumers self-support, in reality this is rarely practical.

The first consideration is that BYO is not for everyone: some employees will be unwilling to provide their own IT; for others it's simply not appropriate, because of their job role, or because of the risk associated with the data they access. BYO is not just about white collar information workers either – consumerisation in general (and BYO as a specific business model) can enable new form factors (smartphones, tablets, etc.) to be used in job roles where a PC was previously impractical, underused, or just too expensive (e.g. a police officer or a hospital doctor).

For those where BYO is an option, from a pragmatic view, the IT department needs to provide some degree of support and it's the policies that surround this that will ensure success or failure of the BYO approach.



Taking the company car analogy used earlier, when that vehicle is unavailable for use (perhaps it requires repairs), there are other options available: public transport, or a temporary hire car, for example. Approaching personal computing with a similarly utilitarian view there are a number of options available to organisations providing a BYO scheme and it may be that several of these are combined within an organisation:

- Community support: establishing a community of BYO users for peer support is a simple, effective and inexpensive option that should be a part of any BYO programme, although it's unlikely to provide a complete answer.
- Loan devices. Some organisations maintain a pool of spare devices that are available for short periods when the BYO device is not. Initially, the pool may be established from the devices that were handed in as employees moved to BYO although, in time, the pool will need to be refreshed.
- Bounded support: Whether time-boxed, "best effort", or technically-bounded, there are options for limiting the extent of support provided to BYO devices. These mechanisms need to be handled with care – best effort may be unsatisfactory if issues cannot be resolved and technically-bounded only really works well where there is clear separation between the IT-provided applications and the operating system (i.e. a virtual infrastructure is used, or another means that ensures there is no on-device element to corporate applications)
- Defining arrangements for external support: where a stipend is provided it may be appropriate to require employees to take out a maintenance contract with their device. Whilst this sounds like a simple solution more technically-minded staff are likely to resent paying for a support service when they are capable of self-supporting and the scope of such a service will be limited to hardware, operating system and communications – it is unlikely to assist with problems related to corporate applications.

Regardless of the support model, BYO programmes need to be supported by policy (as previously outlined), together with education and training that clearly sets out these policies and the responsibilities of the employee as a consumer of corporate IT services. If employees don't comply with the programme policies they may simply be removed from the BYO scheme.

Device multiplication

Whilst, for some consumers, BYO may result in consolidation of "home" and "work" PCs, there's also a consideration of device multiplicity. Many employees will use a PC or a smartphone (possibly a tablet too), depending on the circumstances in which they find themselves – perhaps a notebook PC for everyday work, a smartphone for checking on communications and for urgent issues when mobile (often during the time that might once have been considered "off-the-clock") and a tablet or ultraportable PC for travelling. All of these devices can access the same data and the choice comes down to context: using the appropriate device for the circumstances. That flexibility is likely to lead to an explosion in the number of devices connecting to the corporate infrastructure and therefore requiring appropriate management.

The effect of this device proliferation is that we're likely to see some convergence in the services that we use as we'll be attracted to those services that are device independent – and that requires management of the data across those devices. This leads to another concept: the personal cloud, which is tangential to the concept of BYO but it's also an important consideration.

The longer view

The current generation of virtualised solutions are best considered as transitional technologies. Many organisations are moving their application portfolios to a browser model (whether that takes the form of a traditional web application or true cloud computing) and this potentially alleviates many of the device concerns. Indeed, we are fast reaching a point where IT departments can be device and operating system agnostic, concentrating purely on the applications and data. In this sense, cloud computing may be viewed as an enabler for BYO.

In time, the advent of fourth generation mobile networks and super-fast broadband are expected to enable a shift from dedicated wide area networks to secure connections across the public Internet.

In the absence of ubiquitous connectivity and HTML5 web applications there will still be many on-device applications in use. We may not need everyone to have Microsoft Word (for example) but we might want everyone to have an application that can read and write Word documents and maintain document fidelity. Similar examples can be applied to other forms of data that lives outside the corporate datacentre.

Then there is the issue of malware – at present we rely on client firewalls and endpoint protection suites that proactively monitor for exploits at the operating system level. Perhaps we're not so far away from the point where each application has its own firewall?

Then there is access to the data itself – in the not so distant future, even authenticated users may be given different levels of data access according to the device/network that they are using. With this we start to stray away from the topic of BYO, but there is a relationship – maybe full data access is only available when working within the infrastructure controlled by the IT department.

Finally, what about the office environment? Sustainability issues are driving a greater emphasis on remote working for certain groups of employees. The need for offices is changing and the increasing use of mobile devices provides an opportunity to redesign the way in which we work – does the future of the workplace really have to be about hot desks and cubicles, or could we come up with something more exciting that encourages collaboration with natural user interfaces? By freeing the organisational IT and facilities departments from the desktop paradigm (using BYO as an enabler), we can start to evolve towards a new experience of work.

Starting out in BYO

For organisations looking to set out on a journey towards BYO computing, there are some practical steps that can be taken:

1. Assess organisational readiness: consider the requirements of the consumers (locations, flexible work arrangements, etc.); the business approach to attracting and retaining employees; regulatory and security concerns; and the various "desktop" delivery models that may apply to particular user roles.
2. Segment consumers according to security requirements and identified roles. Bear in mind that BYO is not suitable for all – and not all employees will want to provide their own devices.
3. Evaluate the available technologies and develop a business case to put in place the associated infrastructure changes.
4. Define BYO policies, working with the HR, legal and finance departments. Ensure that the company insurers are aware of the change in working practices as this may impact their risk.
5. Conduct pilot programmes with small groups of early adopters to determine the effects on productivity, working practices and whether the perceived security risks and manageability concerns are real. Use the pilots to put in place appropriate support mechanisms. Encourage consumers to self-support by creating an environment to share lessons learnt and overcome issues.
6. Plan for a larger rollout – ideal candidates for BYO include business partners, external consultants, new hires, mobile/home-based workers.

In conclusion

The consumerisation of enterprise IT is a serious issue for CIOs that cannot be ignored. BYO potentially offers part of the solution but it brings its own challenges around security and manageability so, in order to be successful, IT departments need to work with their legal, HR and finance colleagues to develop a programme with appropriate guidance and policies. Whilst technology may assist in the short to medium term, in general the move should be towards services that are virtualised rather than device or technology dependent offerings. The enterprise has to redraw its boundaries, contracting around these virtual services and, in achieving this transition, it can move to a higher trajectory in terms of delivering business value.

About the author

Mark Wilson, Strategy Manager, Fujitsu.

Mark is an analyst working within Fujitsu's UK and Ireland Office of the CTO, providing thought leadership both internally and to customers, shaping business and technology strategy. He has 17 years' experience of working in the IT industry, 12 of which have been with Fujitsu. Mark has a background in leading large IT infrastructure projects with customers in the UK, mainland Europe and Australia. He has a degree in Computer Studies from the University of Glamorgan. Mark is also active in social media and won the Individual IT Professional (Male) award in the 2010 Computer Weekly IT Blog Awards. Mark may be found on Twitter @markwilsonit.

If you would like to comment on the topics in this paper, Mark would welcome your feedback, by email to mark.a.wilson@uk.fujitsu.com.

With special thanks to Declan Brady, Tony Cox, Gernot Fels, David Gentle, Vin Hughes, Mark Locke, Alex Macadam, Ian Mitchell and David Smith for their assistance in preparing this paper.

OFFICE of the CTO

Contact
FUJITSU
22 Baker Street, London, W1U 3BW
askfujitsu@uk.fujitsu.com
www.fujitsu.com/uk

REF: 3358