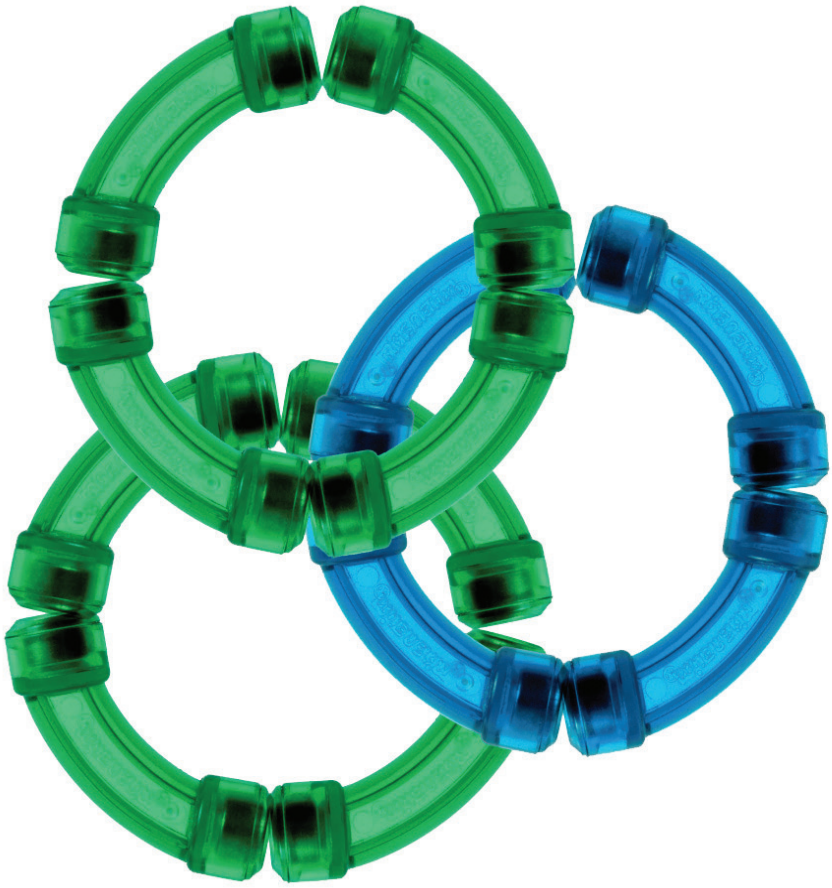
Deloitte.

Understanding the Bring-Your-Own-Device landscape

By invitation only



A Deloitte Research report

Contents

This report, commissioned by IBM Software, comprises the findings of in-depth interviews and desk research conducted by Deloitte LLP.

IBM is the world's largest information technology company, with 100 years of experience in helping businesses innovate. Deloitte and IBM's long strategic alliance unites the depth and breadth of IBM's leading technology portfolio with Deloitte's extensive range of methodologies and consulting experience.

By providing services that leverage IBM hardware and software, our teams help organisations adopt advanced technologies to drive greater enterprise value. Working together, we help you apply innovative solutions to meet specific business needs.

Foreword

The UK's love affair with technology has put powerful devices, from smartphones to tablets and many types of personal computers, into the hands of consumers. Individuals use these devices for communication and entertainment but have increasingly incorporated these devices into the professional spheres of their lives.

For UK enterprises the employees' attachment to their devices, whether personal or enterprise-owned, raises complex questions about the dividing line between work and leisure, and the acceptable use of technology through the working day and beyond.

The rising use of personal technologies for work-related activities has coined the phrase Bring-Your-Own-Device (BYOD). It is a trend that has potential to bring substantial benefits to enterprises, but can equally present considerable risks and implementation challenges.

Those executives most likely to see positive outcomes from BYOD will understand its potential impact across the organisation and develop a strategic response which balances the needs of the company and its employees. The reward for successfully navigating a way forward is likely to be tangible benefits in terms of corporate performance, employee satisfaction and workplace efficiency.

This report comprises an effort to formulate an evidence-based commentary on the state of BYOD in the United Kingdom. It attempts to cut through confusion and offer pragmatic advice incorporating a broad range of management perspectives – from IT to risk management, tax and talent. The report focuses particularly on the differences in ease of BYO by device: bringing a computer into work to access corporate data can be far more complex than accessing work e-mail via a personal smartphone. It is hoped the report will help executives understand the BYOD landscape and provide a framework for discussion and debate.

While drawing on various surveys and commentaries, the report reserves its greatest weight for the findings of 13 in-depth interviews, conducted with organisations representing a UK workforce of more than 250,000. The findings are skewed towards larger enterprises, but may offer broad points of interest for all those concerned with technology in the workplace.

For those executives who have experience of the issues raised, we welcome your feedback and comments.

Executive summary

Bring-Your-Own-Device (BYOD) is not a single idea or way of working. Rather it represents a broad spectrum of devices, capabilities and responses indicative of the evolving role of technology in the relationship between work and personal lives. Each device represents a different level of complexity when incorporating this into an enterprise IT environment.

Demand for BYOD has often in its early stages been led by employees, sometimes collaborating with employers and sometimes not. Enterprises have moved to incorporate personal smartphones and tablets into enterprise activities. Currently many enterprises are considering how to integrate employee-owned computers into enterprise infrastructures.

Wishing to respond while ensuring IT infrastructures remain secure, Chief Information Officers (CIOs) have launched formal BYOD solutions. For many the preferred approach has been a managed programme, aimed at generating a range of benefits, including lower costs, higher productivity and increased flexibility.

Early schemes have tended to offer BYOD on a complementary basis, with employee devices used alongside company technologies. However, as the market has matured, more ambitious solutions are beginning to emerge, the most potentially complex of which is the use of personal computers as a replacement to centrally provisioned and managed computers. So-called BYOC is still rare, but Deloitte estimates that an increasing proportion of companies will allow employees to bring their own computers on an unfunded basis in 2013.[1]

In seeking the most appropriate BYOD technology solution, four key considerations should be taken into account. Business objectives and targeted benefits must be identified, leading to decisions on which devices are to be included and in what manner. Security and audit requirements must be taken into account and all must sit below a broadly coherent IT strategy.

BYOD for mobile devices is typically enabled through Mobile Device Management (MDM) or a secure container approach. Computer BYOD tends to leverage desktop virtualisation and cloud-based applications to deliver functionality. Network Access Control, meanwhile can help manage access and protect data.

While responsibility for BYOD might sit with the CIO, a multidisciplinary team is required to develop coordinated policy. Colleagues from human resources, legal and individual business units should be involved, to cover matters from employee eligibility, to funding arrangements, support models, education and legal affairs.

BYOD may not be right for every employee or every company, but the trend is likely to become increasingly evaluated and established, whether or not companies develop a strategic response. But BYOD is unlikely to spell the end of the enterprise machine. In the short-medium term at least, it is much more probable that enterprises will operate BYOD programmes alongside enterprise devices schemes. In this way offering a flexible technology solution and seeking to provide the best of both worlds to enterprise and employees.

In some cases organisations may need to step back and assess the underlying drivers of BYOD, perhaps considering broadening enterprise device ranges and shortening refresh windows. Other benefits may be realised through Bring-Your-Own-Application, a trend set to take centre stage which may amplify the benefits and challenges of BYOD.

The BYOD hype

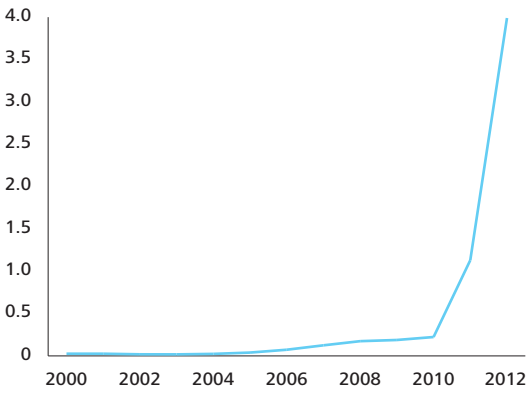
The hype around BYOD is intense, but are we all talking about the same thing?

Bring-Your-Own-Device (BYOD) is the use of employee-owned devices to access enterprise content or networks. It is an IT trend and a broader movement that impacts the way enterprises invest in assets, empower employees and attract and retain talent. The growth and potential evolution of BYOD demands the attention of any executive with an interest in the strategic role of technology over the coming years, regardless of industry or geography.

The past year has seen a spike in interest in BYOD, with Internet search returns reaching four million in 2012, representing approximately two-thirds of the total in the past 12 years.[2] Some analysts say we are at the peak of BYOD hype, with expectations far in excess of reality.[3] Our interview findings suggest the situation is polarised by category of device and that significant differences exist between organisations with mature programmes and those just beginning their BYOD journey.

BYOD dates from when personal computers were first used in the home to complete office work. The trend has accelerated in recent years as smartphones have become more popular and media tablets have been adopted in the C-suite and beyond. BYOD is now a common topic of discussion, in part because desirable devices capture the imaginations of executives and analysts. Debate has continued and deepened because of the opportunities and challenges that BYOD presents.

Figure 1. Search returns for 'BYOD', 2000-12



Source: Google search

Bring-Your-Own-Device (BYOD) is the use of employee-owned devices to access enterprise content or networks.

Commentary on BYOD in the press and elsewhere is frequently confused. Definitions are various and broad, partly because the enablers and impacts of BYOD include other key trends such as mobility, consumerisation of information technology, cloud computing and virtualisation.[4,5,6,7]

The definition of BYOD, while not universally agreed, comprises multiple devices, capabilities and 'flavour' of usage:

- **Devices:** it is sensible to focus discussion on devices with in-built processors, namely mobile devices (smartphones and tablets) and computers. For the purpose of this report BYOD's scope will not incorporate memory sticks and other computer accessories.[8]

- **Capabilities:** authorised capabilities of personal devices can range from accessing the Internet via enterprise Wi-Fi networks and use of simple applications (e.g. webmail) to the full functionality offered by access to all enterprise applications and systems.

- **'Flavour':** the use of personal devices for enterprise purposes can be categorised into three distinct 'flavour's per device category:

  – ***BYOD-as-a-Complement:*** allowing individual employees to use personal devices alongside enterprise devices.

  – ***BYOD-as-a-Replacement:*** replacing individual's enterprise devices with employee-owned devices.

  – ***BYOD-as-an-Addition:*** permitting the use of employee-owned devices for individual employees who would not otherwise have exclusive access to an enterprise device.

This report on BYOD will discuss the use of personal smartphones, tablets and computers. It will consider all levels of BYOD capability beyond Internet access via enterprise Wi-Fi and all 'flavours' of BYOD.

Demand for BYOD

A significant and influential group of employees demands the right to use personal devices at work

BYOD is already present, to some extent, in most organisations in the United Kingdom. BYOD may be mandated by CIOs or be a clandestine practice of employees. One survey of employees across 13 countries found 67 per cent use a personal device at work to some degree.[9,10] Another study found 57 per cent of IT managers believe employees use personal devices without consent.[11] The balance of usage between personal and enterprise devices is unknown, but is likely to vary according to individual circumstance.

Adoption of BYOD has been enabled by recent advances in consumer electronics. Improvements in device technology have traditionally filtered down from enterprise to consumer devices in the same way as innovations in motor racing have trickled down to consumer vehicles. This trend has been in reverse for some years and many consumer devices now equal or surpass the capabilities of enterprise devices.

Furthermore, ownership of consumer devices is significant and continues to grow. More than 50 per cent of the UK population own smartphones (13 years after the first BlackBerry device and five years after the first iPhone).[12,13,14] Approximately 10-15 per cent of the UK population has access to a media tablet, less than three years after the device first launched.[15,16,17] Tablets are likely to become increasingly affordable as Moore's law enables average prices to fall. Content-subsidised devices will also put downward pressure on prices.[18]

Improved network connectivity has been fundamental to unlocking device potential in enabling consumption of over-the-top (OTT) content and applications. The growth of Wi-Fi network coverage has transformed connectivity in homes and urban areas. About 60 per cent of UK homes now have a Wi-Fi router, and thousands of Wi-Fi hotspots are available in public areas, many of which are free.[19,20] Meanwhile, average downlink speed for UK mobile network users has increased from 1.5 Mbps in summer 2010 to 3 Mbps in October 2012.[21] The introduction of 4G LTE networks promises initial speeds of 8-12 Mbps.[22]

As smartphones have become important (and in some cases essential) to a growing number of people, and as early-adopters have rushed to purchase tablets, some employees have begun to integrate the devices into their working lives. The workforce, particularly information workers, uses personal devices for various work tasks, such as note taking, research and work email. Executives bring their own tablets into meetings, using them to review documents and give presentations. The tablet is this decade's corporate status symbol as well as a useful productivity tool.

Demand for BYOD is not universal. Employees who are not clamouring for BYOD should not be overlooked

The level of demand for BYOD depends somewhat on the definition. From a device perspective, demand for mobile devices to be brought into the enterprise is far higher than for computers (BYOC). Less than five per cent of organisations are estimated to have policies to support BYOC, while nearly 70 per cent of smartphone-owning professionals use a personal smartphone to access corporate data, survey data indicates.[23,24]

The fact that organisations offer BYOD does not mean it is demanded unanimously by employees. While some may be vocal in asking for BYOD, others, perhaps a silent majority may be indifferent or even against the concept. One employee survey suggested that only 20 per cent of respondents preferred to use a personally owned PC and/or mobile device at work, while 51 per cent preferred to choose a device at their employer's expense and 29 per cent preferred a standard enterprise device.[25] In part, an employee's view reflects their level of confidence in their ability to maintain a device. It may be relatively simple to self-administer a smartphone or tablet, but many employees would rather leave the complexities of maintaining a computer to the IT department.

BYOD 'flavours' vary in popularity. Interviewees reported that employees were enthusiastic about BYOD-as-a-Complement because it represented greater choice and freedom and meant they could retain a dependable fall-back – their enterprise device. For employees not eligible for an enterprise device, programmes which allowed and enabled BYOD-as-an-Addition were generally well received.

It is the third 'flavour', BYOD-as-a-Replacement, which tended to split opinion, as it implies a major change in the contract between employer and employee, requiring employees to provide and maintain devices they depend on to do their jobs. There is a wide range of technological ability within most organisations and while smartphones may be manageable for novices, computers could pose a significant challenge. Although employees may well maintain personal computers, typically they use them less frequently and intensively than an enterprise machine. One technology company offered an optional BYOD-as-a-Replacement programme for computers but reported just 25 per cent take-up after three years. This relatively low rate of adoption could be indicative of how niche the demand may be for the transformational 'flavour' of BYOD.

The nature of employees' roles may influence demand for BYOD, but generalisations by role type ignore individual or situational idiosyncrasies. For example, it is often assumed that information workers would be advocates of BYOD, but an office-based employee working regular hours may have no need or desire to access business tools beyond those hours. Equally, non-information workers may have specific reasons for demanding BYOD.

One large retailer is planning a BYOD-as-an-Addition, web-based solution to support shop-floor sales assistants completing occasional tasks, such as performance management. Currently, assistants queue to use the small number of terminals in the back office. The BYOD scheme does not offer a stipend but does allow employees to complete tasks from a personal device at their convenience.

Other influencing factors can be personal choice; while some employees may prefer to carry one device, others might wish to maintain a clear separation between personal and work life. Character types, preferences in receiving information and previous exposure to a BYOD environment are likely to impact demand. Clearly, individual BYOD programme details, discussed in this report, will affect demand and may not be suitable for all. While enabling BYOD is a priority for many CIOs, it is important to cater to those not comfortable with such an approach. As a result most programmes focus on employee choice, rather than requiring employees use their own devices.

Three paths for the CIO: Tolerate, clamp down or provide

Organisations should develop and communicate a position on BYOD

The Chief Information Officer (CIO) is usually responsible for the formation of a formal BYOD strategy, and is likely to face pressure to deliver from both the workforce and C-suite peers. All organisations interviewed were implementing a BYOD strategy, though some suggested it was devised following ad-hoc rollout. As a result, rationalisation of existing pilots and makeshift BYOD practices is often one of the first tasks for those formulating a prescribed approach.

The organisations highlighted three potential BYOD strategies:

1. Tolerate unmanaged BYOD

Some organisations may consider that the risks of an unmanaged BYOD environment are acceptable. This, however, is likely to be a minority of enterprises. However, a global survey reported that nearly half of respondents' employers did not know about BYOD or turned a blind eye to it.[26] But organisations should undertake a comprehensive risk assessment to inform any decision on BYOD strategy. In that way, enterprises following this path make a conscious decision to tolerate unmanaged BYOD, accepting the risks rather than falling into a default position.

2. Attempt a clamp down

Some organisations, such as government departments and their suppliers, may conclude that any BYOD programme would pose an unacceptable risk to security.[27]

Most companies, however, expect a clamp down is likely to drive BYOD 'underground', representing a far greater level of uncertainty. A recent survey of '20-something' workers discovered that more than half believe that mobile device BYOD was a right not a privilege, with one in three reporting that they would break anti-BYOD rules.[28] Clamping down on BYOD may therefore increase the risk to the organisation, as employees seek less secure workarounds (for example, emailing business presentations to personal email addresses if synchronised email is not permitted).

3. Provide a managed BYOD programme

A managed BYOD programme can offer a reasonable compromise between user experience and security. For the majority of organisations, this was the only workable option and was often intertwined with other programmes to help an enterprise achieve its broader business objectives. Such objectives included boosting productivity, enhancing employee satisfaction and improving customer understanding through familiarity with consumer devices and ways of using them.

Providing a managed BYOD programme, however, is not without its challenges, including supporting a heterogeneous device environment, adapting IT infrastructure and educating employees on acceptable usage.

From risk management to business enablement

Successful BYOD deployments have turned an initial risk management initiative into a broader programme of business enablement

Given the impetus to respond to BYOD, CIOs may feel some pressure to 'discover' benefits supporting a business case. On the other hand, they may judge that BYOD is a good investment, with IT cost savings and productivity gains offsetting infrastructure and management costs.

The reality is likely to be somewhere between. While opportunities exist for BYOD to help realise broader business objectives, the value is extremely difficult to quantify. The nature and scale of potential returns are highly context-dependent, but it is worth considering the case for those most commonly targeted:

- IT cost savings
- Productivity gains
- Employee satisfaction
- Understanding the consumer
- Operational flexibility.

IT cost savings

BYOD may save costs from initial device purchase to on-going usage and IT helpdesk support. Achieving measurable and sustainable savings, however, can prove to be challenging. In fact, the majority of interviewees expect costs to increase, because early adoption tends to be complementary or additive. A recent European survey of IT professionals revealed that 67 per cent thought BYOD would increase costs while 23 per cent believed it would reduce costs.[29]

Device and usage costs can be reduced if replacing enterprise devices is the objective, but it is unclear that employees – especially those on median incomes – would be prepared to bear the cost. While some surveys suggest employees are willing to pay for devices that would be used to complete work activities, this is most likely to capture complementary or additive devices. All interviewees with a replacement BYOD scheme provided a form of allowance. Typical reported allowances are £30-50 per month for smartphones, suggesting initial cost savings will be significantly diminished.[30,31,32]

Where organisations permit employees to top up an allowance, they may benefit from employees buying higher spec devices at their own expense. The value placed on an up-to-date consumer device may also encourage employees to take better care of their devices and refresh them more frequently.

Enterprise-issued devices benefit in most countries from volume discount rates and specific tax exemptions. In the United Kingdom, enterprises can often reclaim 20 per cent VAT and can be exempt from benefit-in-kind rules for device and usage costs for predominantly business devices. For BYOD, a stipend will result in employees paying income tax and National Insurance at their marginal rate; the enterprise will be liable to pay Employer's National Insurance and generally will not be able to reclaim VAT. Reimbursement schemes, in which the employee buys the device for mixed business and personal use, would also result in a VAT cost in most circumstance. Tax legislation affecting BYOD may change but at present the inefficiencies are likely to undermine cost savings, unless costs are borne by employees.

Support costs may, in theory, be reduced because the onus of maintaining hardware is transferred to the employee. IT support can then focus on guaranteeing the BYOD service and assisting with software enquiries. Some organisations have attempted to require that employees purchase tech support subscriptions, typically costing £90-£120 per annum for remote services, and substantially more for in-store packages.[33,34] However, employers have generally found this to be unenforceable and unpopular among tech-savvy early adopters.

Often BYOD programmes have emphasised self-service communities, which have shown early promise. Early adopters are more likely to be able to self-fix problems and help other like-minded individuals; however their enthusiasm for answering the more mundane enquiries that may represent mainstream technical support requests could be far lower.

At least in the short term, employees are unlikely to wish to leave the office to get a device examined in a retail store. So IT services remain the first port of call. A survey of IT personnel in Japan, the United States and Germany revealed that 74 per cent of respondents believe that enterprises should offer full or limited IT support for employee-owned devices.[35] Interviewees described how IT helpdesks frequently assist with out-of-scope hardware faults, at least to the point of diagnosis. Some interviewees offering smartphone BYOD have outsourced procurement and helpdesk services to a network operator, avoiding the need to become an expert for every device.

It should not be forgotten that BYOD may generate additional costs, including infrastructure improvements, security solutions and application upgrades. One example of infrastructure improvements is a requirement for greater Wi-Fi coverage, as organisations expect BYOD to continue to drive the number of connected devices in the workplace. Knowledge workers are predicted to carry an average 3.3 connected devices by 2014, compared with 2.8 in 2012.[36] Interviewees reported heavy investment in Wi-Fi networks which, for security and service quality purposes, frequently involved deploying multiple networks for different tiers of users.

Security solutions will carry licensing costs, hardware demands and administrative overheads. Interviewees reported the typical licensing cost of a secure container email and calendar application was £30-£40 per device per annum, with one-off hardware costs of £40,000-£60,000. Mobile Device Management solution costs were reported to be of a similar magnitude. For computers, a virtual desktop solution could cost around £300-400 per user, including licensing and backend server requirement costs. Access to a suite of cloud-based applications varies considerably by feature set, but could cost £30-£200 per annum for each user. As employees tend to have multiple devices, some organisations have restricted the number of BYOD devices each employee is eligible to use, or have required business unit sign off to validate the business case for multiple devices.

Rewriting or adapting applications to work with multiple devices, operating systems and versions can be time-consuming and expensive. Specialist mobile apps are being demanded by employees and business units alike, and BYOD can make providing such apps increasingly complex. The proliferation of operating systems, if supported, will increase development investment, as each requires a different native application. HTML5 promises an alternative to developing multiple versions of native applications, but can lead to compromised user experience. Catering for a wide range of form factors make it difficult to present a consistent user experience and native apps typically offer smoother integration with built-in components, such as calendars or geolocation.

Productivity gains

Gains in productivity are the cornerstone of most BYOD business cases. Some 80 per cent of BYOD decision-makers at US and European 500+ employee organisations based their deployment business case on productivity gains.[39] However, few attempt to measure productivity before and after implementation, and those that do struggle to get meaningful results. One organisation estimated that BYOD delivered close to an extra hour per day per employee.[40] However, understanding whether this is productive time is another matter, and is particularly challenging in respect of knowledge workers.

Productivity can be gained through BYOD in three ways: increasing the number of working hours, improving employee efficiency in working hours and putting technology into hands that would not usually be eligible.

In a similar way that issuing BlackBerry devices increased possible working hours, BYOD as a complement or replacement means that employees could have greater access to communications and information through additional devices; or devices more likely to be used outside standard working hours. While this allows for increased workloads, there could be an adverse impact on work-life balance and employee satisfaction. Many employees may not want to work beyond agreed hours, even if it is made possible through BYOD.

During the working day, technology has often boosted employee efficiency. Employees, however, do not always choose devices for practicality, for example opting for a touchscreen device when a full keyboard would be more suitable. Instead, they tend to adapt to the limitations of their chosen device, perhaps by writing shorter documents and emails. A survey of US tablet users revealed that 44 per cent reported that typing text over 500-words was the biggest frustration with their device.[41] One telecoms company reported that BlackBerry devices were likely to remain the only corporate-issued device, due to perceived efficiency advantages over touch-screen smartphones. Of course, productivity does not necessarily require significant amounts of typing. BYOD may present a more efficient or effective method of retrieving information, engaging customers and reviewing documents.

Providing computer access to those not eligible for an enterprise device through BYOD-as-an-Addition programmes could improve productivity, but the impact is likely to be small. If there were opportunities to significantly improve productivity, it is likely enterprise devices would already have been issued.

In some cases, however, BYOD may actually make employees less efficient. Employees already attend to private matters during working hours, and BYOD is likely to bring more personal life into the workplace. Less disciplined employees are more likely to be distracted with activities such as social media updates and playing games eating into productive time. The inefficiencies introduced by constantly switching tasks are harder to quantify. Some tasks require sustained concentration, which can be difficult to maintain while receiving a torrent of personal and business communications.

As noted above, self support models may be part of a BYOD solution and offer potential savings for central IT support. The risk of such an approach, however, is that support savings are more than offset in loss of employee productivity. The average employee will be less proficient at fixing a device than a dedicated helpdesk professional. Not only would fault resolution take longer, but every minute is likely to be more expensive to the organisation, considering relative salary costs. So while helpdesk savings may be achieved, costs are effectively segmented, amplified and distributed to individual business units.

Employee satisfaction

BYOD is increasingly seen as a tool for attracting and retaining employees. Funded BYOD schemes are particularly valued in industries which rely on attracting bright graduates, or where base-level pay is particularly low.

In a poll of medium to large enterprise CIOs, 40 per cent cited allowing employee choice of device as key driver of BYOD.[42] Several interviewees have tied BYOD deployment to a 'choice agenda' with one major broadcaster considering BYOD as part of a broader flexible work initiative. It asked employees to adopt mobile working and hot-desk arrangements but in return offered increased device choice.

The term BYOD is frequently used incorrectly to describe Choose-Your-Own-Device programmes, where the selection of enterprise devices, typically smartphones, has simply been broadened. This approach is likely to satisfy many employees and the company maintains ownership of the device.

Understanding the consumer

As part of the broader consumerisation of IT, some B2C organisations increasingly see BYOD as a way to help employees understand the customer base. Employee use of a range of devices based on different operating systems can serve as a useful test-bed for customer-facing applications. As organisations look to increase digital interactions with customers it may become increasingly beneficial to replicate the diversity of the customer base within the workforce.

For some organisations, it is particularly important to be viewed as a digital leader and for external image to be reflected in internal ways of working. Technology vendors and advisors, or those that promote openness, freedom or creativity typically fall into this category.

Operational flexibility

Operational flexibility is a benefit of BYOD that is often overlooked. While not applicable to all organisations there are four scenarios in which it is particularly valuable:

High growth phases (e.g. technology start-ups) – The flexibility and scalability of BYOD is appealing to organisations experiencing high levels of growth. As an example, more than half of Deloitte's 2012 Canadian TMT Fast 50 participants supported full BYOD across smartphones, tablets and computers. As headcount grows rapidly, BYOD may be the most practical way to onboard new starters in a timely manner. This is equally true for events requiring rapid scaling up of IT access.

M&A is business as usual (e.g. oil and gas majors) – In some industries, constant inorganic growth is the norm. With each merger or acquisition a number of new people and unknown devices may require access to an enterprise's networks. At least in the short-term, these devices can effectively be treated as BYOD devices, with organisations able to provide controlled access to required systems.

Workforce is highly contractor-based (e.g. broadcast media) – For organisations highly dependent on contractors or other temporary staff, BYOD offers potential time and cost advantages. Device provisioning and collection can be particularly disruptive in short projects and many freelancers reflect the need for a personally owned device in their charge out rates. Where flexible team approaches are increasingly common this application of BYOD may become relevant to other industries.

Improving flexible working and business continuity – Specifically for computers, flexible working has traditionally been provided through provision of laptops. BYOD presents another method, with the added benefit of enabling unplanned working from home. Such flexibility can reduce the impact of employee sickness or other obstructions to getting into work (such as major transport network disruptions). In the education sector, organisations are starting to use BYOD to access core resources beyond their IT rooms.[43]

As organisations look to increase digital interactions with customers it may become increasingly beneficial to replicate the diversity of the customer base within the workforce.

Technology can make BYOD a secure possibility

There is no one-size-fits-all technology for securing BYOD, but four considerations should be assessed to help identify the most appropriate solution

Organisations have a range of hardware and software solutions available to secure BYOD and manage associated risks. Choosing the most suitable solution will depend on:

- **BYOD device and 'flavour'**
  Giving access to one mobile application as part of a BYOD-as-an-Addition approach is very different to replacing enterprise-issued computers with BYOC. An individual mobile app can be secured at the application level, since it will often only require access to specific enterprise information, with limited reach into the corporate network. By contrast, a replacement computer is likely to require access to a portfolio of applications and databases and a greater degree of freedom in information manipulation. These requirements present a significantly greater security risk. A multi-layered approach to device and application security is advisable regardless of BYOD device and 'flavour'.

- **Business objectives and targeted benefits**
  A clear view of business objectives and targeted benefits should help set requirements for enabling technology. If BYOD is primarily intended to increase employee satisfaction, enterprises should spend time understanding what solution would work best for users. For example, to deliver an improved user experience, it may be preferential to develop multiple native mobile apps rather than a single web app. If BYOD is a cost reduction exercise then the price of solutions will feature more prominently in requirements.

- **Security and audit requirements**
  Security is likely to be a consideration for any organisation but requirements will vary by company and division. This may reflect characteristics and regulation of specific geographies and industries. Some organisations may process particularly sensitive information (e.g. personal medical records) while others are mandated to record and store phone or email communications for regulatory purposes, such as those overseen by the Financial Services Authority.

- **Broader IT strategy**
  A number of organisations with more mature BYOD strategies emphasise the need to complement the broader IT agenda. For example, if a broader move towards desktop virtualisation is underway, it is likely to be financially and operationally beneficial to pursue the same approach in BYOC.

BYOD for mobile devices is typically enabled through Mobile Device Management (MDM) or a secure container approach

Organisations typically adopt one of two approaches to securing data on BYOD mobile devices. Mobile Device Management (MDM) enables security controls to be set at a device level while a secure container or sandbox approach secures individual apps without necessarily impacting the rest of the device. Each approach can require application software to be downloaded onto a user's device and incur the associated licensing costs. Alternatively, some basic device controls can be enforced through ActiveSync, which is natively supported by a number of mobile operating systems, in which case no additional software is required.

Mobile device management

MDM is similar to traditional IT device management, whereby the whole device is subject to security controls. The primary advantage is that business activities can be performed with the device's native user interface. The solution can more broadly leverage the power of the mobile device, such as allowing interaction between applications (e.g. copying data between emails and word processing apps).

A large array of security controls can be applied through MDM, the most commonly implemented of which is a minimum strength password to unlock a device. Additionally a remote wipe capability provided by many MDM tools allows data to be deleted from lost or stolen devices. Monitoring compliance and device usage are also possible (e.g. jailbreak detection), giving the IT department full visibility of the BYOD mobile device environment.

While device-level security offers some freedoms, personal usage under this approach is usually subject to some degree of enterprise policy. Some companies have reported the need to disable device features or prohibit applications which employees find valuable. These prohibitions tend to be enforced at device level, making it impossible to use a blacklisted app for either personal or business reasons.

Often, personal and business data on mobile devices can become closely intertwined in a BYOD scenario, which raises two further issues. Firstly, remote wipe commands can result in both personal and enterprise data being deleted, with the former less likely to be backed up and more likely to cause upset to the individual. Some leading MDM products now comprise selective wipe and full wipe capability that helps mitigate this risk. Secondly, legal and privacy complications can also arise if thorough terms of use agreements are not in place. For example, is recording or searching through all device content a breach of employee privacy, or conversely a legal requirement for the employer? What if sensitive personal information is discovered?

Secure container or sandbox

A secure container or sandbox approach applies prescribed security controls to specific apps used for business purposes, but not the entire device. All enterprise data is held within the container and so is less intrusive to employees' personal usage. Maintaining a clear separation between enterprise and personal data mitigates some inconvenience and a number of the privacy and legal concerns associated with enforcing device-level MDM controls. Organisations also find it easier to minimise and communicate the scope of available support.

A common criticism of the approach is that it provides a poor user experience relative to native device applications. This is because common native app functionality (such as email, contact information and calendar entries) is replicated in the secure container, which has its own user interface. As organisations look to deploy a wider portfolio of applications, user experience may be compromised further if individual secure containers cannot be linked to provide an equivalent level of functionality to native apps.

A 'third way' may emerge as a halfway house between whole-device management and app level security. One operating system provider is launching a solution in 2013, with clear profile separation of business from personal apps and data.[44] Its success, however, will depend on the attractiveness of the complete package to consumer-employees. If combined with appealing handsets and a rich ecosystem of applications, it may offer a viable alternative to existing accepted approaches for BYOD security.

App distribution

Whichever approach to securing mobile device BYOD is used, enterprises should consider how applications are distributed to devices. For third party applications this may be done via the relevant consumer app store. For custom developed and controlled enterprise apps, internal enterprise app stores offer a secure distribution method. An estimated ten per cent of enterprises have their own app store today, and a global survey of all size businesses found that 71 per cent are looking to implement an enterprise app store.[45,46] Various third parties, including MDM and secure container providers, offer enterprise app store products capable of hosting versions of apps for each platform. Alternatively, consumer app store hosts are now customising their app stores for enterprise usage.[47]

In the short term, the native app development approach is likely to be common, with the benefit of fast and user-friendly applications. In the longer term, organisations may consider redeveloping their applications into a web based HTML5-compliant format. This has the advantage of enterprises writing and updating a single application for use across multiple platforms, and so could represent a more cost-efficient development model. However, the efficacy and user experience offered by mobile web apps may be compromised, as highlighted by the recent consumer app u-turn away from HTML5.[48] Whatever the application format, enterprises may still require an app store to allow apps to be easily discovered and downloaded by employees.

Computer BYOD tends to leverage desktop virtualisation and cloud-based applications to deliver functionality to users

For computer BYOD (BYOC), many organisations use desktop virtualisation on an ad-hoc basis. While some see this as a long-term solution, others see it as a bridging technology, believing that cloud-based applications represent the best hope for future BYOC needs.

Desktop virtualisation

Desktop virtualisation offers access to the desktop experience of an enterprise PC from a range of devices, accessed through a client-server relationship. Server side virtualisation is typically employed, meaning multiple virtual desktops exist on each physical server – usually an office computer or data centre server. All processing is performed on the server and a simple visual output is sent to the user device with the receiver software installed.

Desktop virtualisation can securely provide access to a range of enterprise applications that require greater computing power than would be available on the client device. This means that the client can be of lower specification (commonly referred to as a thin-client) and therefore relatively cheap. A combination of fewer, less complex components and limited workload means that fault rates may be reduced and replenishment cycles can be extended. One manufacturer reports an average lifespan of eight years.[49] Energy savings through reduced air conditioning requirements are also achievable in a thin-client environment.

The security of these solutions is considered to be strong, with data residing in the data centre and single-sign-on capability meaning employees can access a range of web-based applications without entering passwords for each. In fact, employees may not even be aware of the passwords used to authenticate them to enterprise systems. Not only is this convenient for the employee, but the employer benefits from the fact that passwords will not be lost or forgotten by end users and access can be instantly revoked when employees leave the organisation, or no longer require access.

The major limitation of traditional server-side virtualisation is the need for a Virtual Private Network (VPN), which requires consistently reliable and relatively high speed connectivity. One provider estimated typical average bandwidth requirements were approximately 30-80 kbps per user.[50] Office-based users may never notice the difference but mobile and rural home-based users may experience frustrating and productivity-sapping interruptions. Sometimes there is no substitute for local processing – for example during long-haul journeys via plane or train where network connectivity is unavailable.

While single sign on can significantly improve the user experience, it also presents significant potential risks to organisational security. For example, in the scenario of a compromised device being used to access the network, a single-sign-on solution may give the attacker much wider access to the corporate network than would have been possible if the solution were not in place.

The technology used to deliver a virtual desktop is evolving, primarily to tackle the core limitations discussed above. For example, some vendors are offering 'off-line' mode product features to combat connectivity concerns. However, this implies some level of security compromise as data is stored locally on devices, even if only temporarily. Client-side virtualisation takes the concept further by hosting the virtual desktop on the local machine and synching with the server. This presents a greater security threat, but significantly reduces the need for regular or high-speed connectivity.

Cloud-based applications

Cloud-based applications are a somewhat newer product class, allowing organisations to purchase and use applications on a subscription basis. The applications are hosted on a server in a public or private cloud but can be accessed through any device with a web browser and Internet connection. Subscriptions may or may not include versions for local machines.

Access to cloud applications provides even greater device freedom than desktop virtualisation as no download of the receiver software is required. As with virtualisation, the applications can be truly agnostic to the device and operating system and be made available through a range of web browsers.

Cloud-based applications avoid the need to recreate a full desktop when only specific applications are actually required, reducing connectivity requirements. For example, one cloud-based email application vendor estimates average bandwidth requirements of approximately 40 kbps for a company of 100 medium usage employees.[51] Risk can be effectively managed because each application can have security measures built in and access to information is limited.

Careful management of cloud usage is required to ensure regulatory compliance. For example, UK organisations are subject to European data protection legislation restricting the geographical movement and storage of some personal data. This may mean that data is useable within some cloud solutions and not others, depending on individual vendor agreements. Use of personal cloud storage solutions, integrated into some mobile devices, presents a broader set of Bring-Your-Own-App security issues.

While the possibility of cloud applications has sparked a new range of tools for employees, the core systems at many organisations are distinctly non-cloud. Many vendors and organisations are trying to retro-fit web portal access, but the results may be compromised because access is through specific browsers, which are often not the latest version.

Network Access Control can mitigate some barriers to BYOD

While devices, or sections of devices, can be secured with some of the above technologies, networks can be protected using Network Access Control (NAC). NAC allows enterprises to manage employee-owned device usage on corporate networks; providing access to useful applications and data while limiting access to protect sensitive data or vulnerable systems.

Using NAC can ensure that only devices which pass authentication checks and are compliant with set security policies will be permitted on the network. Such security policies may include requirements for a MDM agent to be installed on mobile devices, or that anti-virus software is up to date and patch levels are sufficient. This is likely to give many organisations the confidence to allow BYOD. In 2012, 50 per cent of organisations reported that an inability to enforce anti-virus, malware protection or patch levels was a barrier to allowing BYOD, down from 68 per cent in 2010.[52]

Even after granting access to the corporate network, NAC can allow administrators to define which devices and users can access specific parts of the network. This can help to mitigate risks of losing sensitive information, a concern which 75 per cent of organisations report as an obstacle to BYOD.[53] In addition, some organisations use monitoring techniques to identify and investigate suspicious behaviour (such as downloading unusually large quantities of information).

While this is not an exhaustive list of the security options available, it represents the major decisions being made by companies today on how to support BYOD. Clearly whatever the solution, organisations must incorporate it into their wider enterprise architecture. If not correctly integrated into enterprise architecture guidelines and principles, changes to infrastructure risk breaking BYOD services. As employees come to depend on BYOD, service downtime will have an increasingly debilitating impact.

For every organisation, a technology solution was critical to managing BYOD risks, but all respondents acknowledged that it was just one element of a wider programme. In isolation, technology cannot guarantee the security of an organisation's data. People consistently represent the greatest liability and building an understanding of security issues and measures is fundamental. Educating employees on appropriate security behaviour will help ensure the technology does its job. Failing to do so could undermine it.

Successful deployment requires a coordinated policy

While BYOD responsibility might sit with the CIO, a multidisciplinary team is required to develop coordinated policy

Technologists and risk professionals in most organisations will take the lead in selecting the appropriate technology to safeguard enterprise data. However, when it comes to determining the broader details of a BYOD programme and associated policy, colleagues from human resources, legal and individual business units should be involved. Interviewees believe a multidisciplinary team can increase stakeholder buy-in and facilitate the realisation of benefits.

Our research indicates there are five key topic areas a BYOD policy team should address:

- Employee eligibility
- BYOD funding arrangements
- Support model for employee-owned devices
- Employee education and change management
- Legal and privacy.

Employee eligibility

BYOD may only be appropriate and beneficial to subsets of the workforce. It is likely that those who stand to gain the most benefit will be among the most vocal in campaigning for BYOD adoption. These individuals might not represent the majority of employees and are likely to vary by organisation.

As initial steps, organisations should consider:

- which segments, roles or business units could benefit from the use of consumer devices;
- the case for adopting consumer devices compared to standard enterprise or specialist devices;
- if consumer devices are preferable, does BYOD offer advantages over an enterprise-owned device; and
- would eligible individuals be capable of managing BYOD, given the desired support model?

While there is scope for many employees to benefit from BYOD, not everybody need be eligible initially. For example, one organisation felt its field forces could feasibly complete certain tasks through consumer devices, and BYOD represented one route to put such devices in the hands of those employees.

After a full assessment, however, it decided that a specialised field force device would offer better reliability and reduced support, repair and replacement costs. Another interviewee in a similar situation decided that consumer devices should be adopted. It chose to retain ownership and limit the functionality of the device for consistency and management simplicity.

Similarly, employees may be eligible for BYOD by role but unsuitable in other ways. A company that promotes a BYOC policy persuaded a small number of employees not to join the BYOD programme, as they were heavy users of IT support and would likely struggle under a self-support model.

BYOD funding arrangements

Most organisations have found that voluntary BYOD-as-a-Replacement schemes have only seen significant uptake when full or partial funding is offered for device and usage. If funding of BYOD is considered beneficial, organisations must determine:

- funding mechanism (e.g. stipend or reimbursement), tax implications and refresh cycles;
- device funding level and whether that is consistent across roles and countries; and
- usage funding (e.g. home broadband and expenses policy).

A simple funding mechanism tends to create the least administrative overhead and is easy to communicate; however, it can also be a blunt tool for promoting BYOD. One organisation used a fixed pre-tax stipend for employees globally. Relative tax rates on income and devices affected affordability of devices across different countries. Such discrepancies may not impact technology solutions but could clearly drive the relative attractiveness and success of a BYOD programme across different territories.

Traditional usage funding tends to be simple for mobile devices, with standardised tools for 'tagging' and expensing business calls only. Data usage is less transparent but generally only reclaimable for replacement BYOD devices. For office-based workers, organisations have generally decided to enhance their Wi-Fi networks in order to minimise cellular network costs.

Support model for employee-owned devices

Organisations deploy a range of support models for employee-owned devices, with increased prominence of self-support featured in most programmes.

When determining an appropriate support model organisations must ascertain:

- what scope of BYOD support should be provided and whether to use an in-house or outsourced function
- to what extent self-care should be used and how the organisation can facilitate the practice
- what fall-back options might an organisation wish to provide.

The scope of BYOD support offered by organisations varies hugely. At one extreme employees benefit from the full support expected for enterprise devices, provided through an outsourced helpdesk. At the other extreme, a company with ad-hoc BYOC and web-based applications offers no support.

The majority of organisations promote self-support to some extent, facilitating it through collaboration tools, e-learning and loosely managed forums. They report that it works well, particularly in a transition period. Self-help can generate a quicker resolution for employees than a helpdesk. However, more complex issues are likely to be better resolved through specialist support.

Besides, some employees will not be comfortable asking colleagues for help and will require hand-holding. In particular the onboarding process is likely to call for some level of remote or local support.

Where BYOD issues affect an employee's ability to work, particularly senior executives, it is understandable that some fall-back support may be required, regardless of pre-agreed support processes. One organisation found that mandating employees to purchase support was unenforceable. Instead it offered limited diagnostic support and provided a small pool of old enterprise devices to cover emergencies.

Employee education and change management

BYOD adoption can mean minimal or substantial changes to the way employees work. All organisations reported the importance of a high-profile and thorough change management process with the most widely reported topics being:

- BYOD enrolment processes
- financial arrangements
- acceptable usage
- security protocols
- support.

For all forms of BYOD, organisations are seeking to make enrolment a 'zero-touch' process. This is widely believed to set employees on the self-support path, where helpdesk assistance is not the norm. The enrolment process is also commonly used as the first change management interaction, whereby users are provided information about the scheme and reminded of changes to their responsibilities prior to completing enrolment.

The financial arrangements of any BYOD scheme should avoid ambiguity, and obligations in relation to funding must be explained to employees. For example, one organisation set minimum requirements and a stipend for BYOD purchase of laptops specifically. Another set no minimum requirements for a tablet BYOD trial, allowing employees to purchase multiple low-spec devices. The full consequences of ownership should be agreed at the outset, including responsibilities for paying on-going costs, obligations for refreshing devices and rights and restrictions on selling used devices.

Acceptable usage can be a contentious issue, as employers are effectively asking employees to act in accordance with enterprise policies while using a personal device. BYOD can encourage employees to bring their own applications. Some organisations have a blacklist and strictly prohibit certain applications, while others are happy for employees to use whatever works for them; the key differentiator often being the sensitivity of the data being handled. In order to operate an application blacklist enterprise must record application inventories, which in itself presents privacy implications.

It is not just applications that can pose a security threat. Accessing some websites, failing to maintain antivirus software, jail-breaking devices or using smartphones as Wi-Fi hotspots can all present security risks.[54] Such risks can be partly mitigated through software solutions, but there are almost always workarounds. To truly safeguard enterprise data, employees must be taught to identify and avoid risks. In the event of a potential security breach, be it a lost smartphone or malware-infected computer, employees should know what is expected of them. Just because it is their device, it doesn't mean it is an issue for them only. For example, there might be a requirement for employees to report lost devices so that a remote wipe can be performed to protect sensitive business data.

As discussed in this report, employee appetite for BYOD, attitude towards BYOD and success of adoption will be a product of many factors. Support and education may need to be tailored to different segments of the BYOD audience, for example helping employees choose a device that works for them. Many will never have made such a purchase before, or will not understand detailed device specification data. Equally, most will not have had to deal without a helpdesk, so a full explanation of self-support responsibilities will help them make an informed decision.

Legal and privacy

Privacy laws and the employer's rights over enterprise data have the potential to clash. All organisations require some control over data for reasons of security, intellectual property and regulatory requirements. Employees may reasonably expect to use personally owned devices without their employer, or anyone else, being able to view what their device is being used for. When surveyed, 82 per cent of employees were concerned about employers tracking personal website browsing and 86 per cent were concerned about unauthorised deletion of personal data such as pictures and music.[55] It is preferable to avoid confusion and address any concerns through clear upfront communication and, where necessary, engagement with the relevant country Work Council. Employees should know what data can be remotely wiped and what information may be accessed by the organisation – for example, by being notified of eDiscovery requirements.

Legal ownership of a phone number is a particularly grey area. On a BYOD scheme where an employee owns the SIM card and contract he or she would be free to take that number with them. This scenario is particularly sensitive for sales personnel, who could more easily poach their previous employer's customers after moving to work for a competitor. Some analysts report that this is a major barrier to many sales groups adopting BYOD.[56] One sales-focused organisation said it was not usually an issue, but it did retain the right to keep phone numbers.

BYOD maturity and its sibling trend

Expect BYOD to spread across organisations and devices but to operate alongside enterprise devices for the foreseeable future

Most organisations are at a relatively early stage of adopting BYOD for mobile devices and are typically focused on rationalising existing pilots and makeshift BYOD practices. The mobile BYOD strategy articulated by one organisation was echoed by many others: first provide basic capabilities, such as email and calendar access on a complementary basis. Then look to leverage mobility through specific applications and consider encouraging BYOD-as-a-Replacement. Some analysts predict that by 2016, more than half of UK smartphones going into enterprises will be through a BYOD scheme.[57]

BYOD-as-a-Replacement may not require a different technological solution to BYOD-as-a-Complement, but take-up is likely to be highly dependent on financial incentives and company policies on usability. We expect a growing number of companies to consider this, but do not envisage the end of enterprise smartphones. Tablets in their current form are likely to remain a secondary device for the majority of workers. If they are not primary machines and have never been issued previously, BYOD tablets are likely to be increasingly allowed on an unfunded basis.

For computers, BYOD uptake is likely to be far slower and driven by employees who work from home most or all of the time. Organisations requiring flexibility in providing technology to new employees may also push towards BYOC, but most organisations believe there is still some way to go and demand is not at levels observed for mobile devices. This is partially explained by the dominance of PCs in the workplace and limited differences between makes and models. Larger differences and preference exist between PCs and Apple computers, and several interviewees report that this was a major contributor to demand for BYOC.

The organisations planning to move to an entirely BYOC model indicated they would stop issuing enterprise computers in five to ten years. BYOD for mobile devices is likely to act as a test bed for CIOs considering BYOC and may set expectations for device choice among employees.

As BYOD matures over the next couple of years, the buzz is likely to decline although the challenges to adoption will remain. One CIO told how conference organisers were tiring of the subject despite the fact that no definitive approach appears to be winning out. Another reason to believe BYOD will gain fewer headlines is that its first adoption understandably causes a big talking point, but evolutions and expansions of policy are likely to be much less controversial.

There is even a chance that a 'BYOD-backlash' will undermine future demand and attention for BYOD-as-a-Replacement, if differences between devices diminish or enterprise device ranges broaden. There are still advantages to enterprise device schemes and some organisations are making efforts to offer a greater degree of device choice, without adapting to BYOD. One interviewee reported the clamour for BYOD subsided once the enterprise device range was broadened and refresh cycles shortened to three years.

The emergence of thin-client devices could see employees feeling that device choice is unimportant. However, people are emotional as well as rational, and some develop strong emotional bonds with devices, brands and models regardless of functionality. As with alcoholic and soft beverages, individuals can become fiercely loyal to a brand, and be unwilling to substitute for a rival product that could be made in the same factory to near identical specifications.

With so many unknowns and difficulty in demonstrating return on investment, hybrid models of BYOD and enterprise devices are likely to dominate. Subsidised BYOD and enterprise devices would coexist for primary devices; supplemented with optional BYOD devices where enterprise provisioning or funding cannot be justified.

Enter BYOD's younger sibling: Bring-Your-Own-Application is likely to receive even greater attention as it amplifies the benefits and challenges of BYOD

As the buzz around BYOD abates to some extent, Bring-Your-Own-Application (BYOA) is likely to step to the forefront of debate. Now that the precedent has been set for employees (instead of IT functions) to provide an entry point for hardware, the same may become increasingly true for software.

Until the smartphone arrived, consumer purchase of software was predominantly limited to purchasing games or home editions of popular work software. However, consumers are now intimately familiar with downloading applications for both entertainment and utility. In 2012 it is expected that, on average, smartphone users downloaded 37 apps, up from 35 the previous year.[58] Already, employees are downloading software to help complete work-related tasks. One survey of UK and US workers revealed that 66 per cent used free file-sharing platforms to share corporate documents.[59] BYOD is not a necessary precursor to BYOA, but the two are likely to be complementary.

Since enabling employees to work the way they choose and increasing productivity are fundamental arguments for BYOD, they should carry even greater weight for BYOA. As with devices, organisations plan to expand the range of enterprise-provided applications and allow employees to choose their own. Most organisations interviewed have plans to implement an enterprise mobile app store, with a few having already done so.

Bespoke applications (such as those used for timesheet entry) tend to be first on the long wish list of corporate apps, but employees are likely to want more than their employers can feasibly build or commission. Some interviewees are analysing popular consumer applications and offering a selection of approved third party apps through the enterprise app store. Security wrapping technology, which adds enterprise-level security to consumer apps, may allow for even greater democratisation of application provisioning.

As with BYOD, BYOA will almost certainly be led by mobile, but mainstream adoption in the computer world could be far quicker for applications than for devices. This may be driven by employees and business units circumnavigating the IT department to acquire the tools they desire in a timely manner. As a starting point, many organisations already allow employees to use their Internet browser of choice.

The proliferation of cloud-based applications means that BYOA does not even require installation, and so could be near-impossible to restrict. In addition, while personal device usage can grow over months or years, popular applications could be adopted by a workforce overnight. Ensuring that such applications are acquired legally by employees and are suitable for commercial purposes will pose a significant challenge to organisations. Even as BYOD is reaching maturity, its sibling trend is hot on its heels.

If the potential explosion of BYOA comes to pass, the challenges of an increasingly heterogeneous software workplace will come to dominate the CIO agenda. A non-standard application landscape could even threaten the collaboration and information sharing it seeks to promote. On the positive side, these challenges are likely to echo those of BYOD. In the same way that caring for a second child is often considered easier than the first; the lessons learnt in adopting BYOD will stand organisations in good stead for the future.

If the potential explosion of BYOA comes to pass, the challenges of an increasingly heterogeneous software workplace will come to dominate the CIO agenda.

Notes

1 TMT Predictions 2013, Deloitte Global Services Limited, Study to be published in January 2013.

2 As per a custom date Google search for the term 'BYOD' as of 30th December 2012.

3 Gartner Hype Cycle for Emerging Technologies, Gartner, See also: http://www.gartner.com/it/page.jsp?id=2124315

4 Mobility is the ability of a business to interact with stakeholders or assets without being tethered to a specific place or infrastructure Mobility, Mobility in the Enterprise: Finding Advantage in Disruption, Deloitte Development LLC, See also: http://www.deloitte.com/view/en_US/us/Insights/Browse-by-Content-Type/podcasts/f2db02e58e981310VgnVCM1000001a56f00aRCRD.htm

5 Consumerisation of IT is the introduction of consumer-oriented technology and behaviours into the realm of Enterprise IT, The Consumerisation of I.T., Pirean, See also: http://www.pirean.com/industry-insight/blogs/bring-your-own-device

6 Cloud computing is a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies. Gartner IT Glossary, See also: http://www.gartner.com/it-glossary/cloud-computing/

7 Virtualization is the abstraction of IT resources masking the physical nature and boundaries of those resources from resource users. An IT resource can be a server, a client, storage, networks, applications or OSs. Essentially, any IT building block can potentially be abstracted from resource users. Gartner IT Glossary, See also: http://www.gartner.com/it-glossary/virtualization/

8 While BYOD can be used as a catch-all for work related hardware, more specific acronyms have been developed including BYOC (computer), BYOS (screen), and BYODKM (display, keyboard and mouse), accredited to Steve Jobs launching the Mac mini.

9 BYOD - is it good, bad or ugly from the user viewpoint?; Microsoft Security Blog, See also: http://blogs.technet.com/b/security/archive/2012/07/26/byod-is-it-good-bad-or-ugly-from-the-user-viewpoint.aspx

10 Trust in computing research; Microsoft Security Blog, See also: http://blogs.technet.com/b/security/archive/2012/03/27/test-trust-in-computing-research-0-introduction.aspx

11 Global IT survey highlights enthusiasm over tablets in the enterprise, shows customization, collaboration and virtualization as key features, Cisco Press Release, See also: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=658006

12 Deloitte Global Mobile Consumer Survey 2012, Deloitte LLP, See also: http://www.deloitte.com/view/en_GB/uk/industries/tmt/telecommunications/global-mobile-consumer-survey-2012/infographic/index.htm

13 Our Mobile planet: United Kingdom, Thinkinsights with Google, See also: http://www.thinkwithgoogle.com/insights/library/studies/our-mobile-planet-United-Kingdom/

14 Smartphone Adoption Approaches Tipping Point Across Markets, Comscore Data Mine, See also: http://www.comscoredatamine.com/2012/02/smartphone-adoption-approaches-tipping-point-across-markets/

15 Deloitte Global Mobile Consumer Survey 2012, Deloitte LLP, See also: http://www.deloitte.com/view/en_GB/uk/industries/tmt/telecommunications/global-mobile-consumer-survey-2012/infographic/index.htm

16 Trends in digital device & internet usage, Thinkinsights with Google, See also: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&sqi=2&ved=0CC8QFjAC&url=http%3A%2F%2Fwww.thinkwithgoogle.com%2Finsights%2Fuploads%2F940738.pdf%2Fdownload%2F&ei=aJKRUMrDDMGS0QW20oGQBw&usg=AFQjCNGIQ24huM7j_Y2tMpV5Q8YCRJ6LkQ&sig2=lpoHgE6ut24qqla_8QQoxg

17 Media tablet is considered a separate form factor from previous incarnations of tablets that were not designed primarily for the consumption of media.

18 Deloitte TMT Predictions 2012, Deloitte Global Services Limited, See also: http://www.deloitte.com/view/en_GB/uk/industries/tmt/predictions/predictions-2012/index.htm

19 Product Support, The Cloud. See also: http://www.thecloud.net/free-wifi/support/

20 Considering that 72 per cent of households receive fixed broadband and 85 per cent of those use a wireless router. Communication Market Report, Ofcom, See also: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&ved=0CDMQFjAC&url=http%3A%2F%2Fstakeholders.ofcom.org.uk%2Fbinaries%2Fresearch%2Fcmr%2Fcmr12%2FCMR_UK_2012.pdf&ei=TaCRUICtCcaR0QXHqYGwAg&usg=AFQjCNFyt5l7W4DTqDq7--WSuNug4juKlg&sig2=U9OFqueUVIhrUg9GA25v2w

21 How fast is your mobile internet? Help us crowd source it, Guardian, See also: http://www.guardian.co.uk/news/datablog/2012/oct/30/mobile-4g-crowdsource-speeds

22 UK's first 4G mobile service launched in 11 cities by EE, BBC, See also: http://www.bbc.co.uk/news/technology-20121025

23 Bring your own device: New opportunities, new challenges, Gartner, See also: http://www.gartner.com/resources/238100/238131/bring_your_own_device_new_op_238131.pdf

24 Ovum reveals firms face huge security risks as 80 per cent of BYOD goes unmanaged, Ovum, See also: http://ovum.com/press_releases/ovum-reveals-firms-face-huge-security-risks-as-80-of-byod-goes-unmanaged/

25 Bring or Buy your own device, Pirean, See also: http://www.pirean.com/industry-insight/blogs/bring-or-buy-your-own-device/

26 Ovum reveals firms face huge security risks as 80% of BYOD goes unmanaged, Ovum, See also: http://ovum.com/press_releases/ovum-reveals-firms-face-huge-security-risks-as-80-of-byod-goes-unmanaged/

27 Ministry of Defence: BYOD ban does not hinder productivity, Computer World, See also: http://www.computerworlduk.com/news/security/3353476/ministry-of-defence-byod-ban-does-not-hinder-productivity/

28 Young employees say BYOD a 'right' not 'privilege', Network World, See also: http://www.networkworld.com/news/2012/061912-byod-20somethings-260305.html

29 2012 BYOD Survey, Liberman Software, See also: http://www.liebsoft.com/BYOD_survey/

30 Can employee-owned devices save your company some money?, Computer World, See also: http://www.computerworlduk.com/in-depth/careers/3331614/can-employee-owned-devices-save-your-company-some-money/

31 Good Technology State of BYOD Report, Good Technology, See also: http://media.www1.good.com/documents/Good_Data_BYOD_2011.pdf

32 Gartner – Bring your own device: New opportunities, new challenges, Gartner, See also: http://www.gartner.com/resources/238100/238131/bring_your_own_device_new_op_238131.pdf

33 Iyogi, See also: http://www.iyogi.co.uk/

34 Geeksquad, See also: http://www.geeksquad.co.uk/services/tech-support

35 Consumerization of IT-survey report, Trendmicro, See also: http://www.trendmicro.com/cloud-content/us/pdfs/rpt_consumerization-survey-report.pdf

36 BYOD and Virtualization, Top 10 Insights from Cisco IBSG Horizons Study, Cisco IBSG Horizons, See also: http://www.cisco.com/web/about/ac79/docs/BYOD.pdf.

37 Google Apps for business, Google, See also: http://www.google.com/intl/en_uk/enterprise/apps/business/pricing.html

38 Microsoft Office 365, Microsoft, See also: http://www.microsoft.com/en-gb/office365/compare-plans.aspx

39 Key Strategies to Capture and Measure the Value of Consumerization of IT, Forrester, See also: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

40 IT performance report, Mid-year update, Intel, See also: http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/intel-it-midyear-performance-report-2012.pdf

41 Tablet typing must leap input gap, replace laptops, Adaptxt US tablet survey. See: http://adaptxt.com/adaptxtlive/tablet-typing-must-leap-input-gap-replace-laptops

42 Key strategies to capture and measure the value of consumerisation of IT, Forrester, See also: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf

43 BYOD policy gives London university users network access flexibility; Computerweekly, See also: http://www.computerweekly.com/feature/BYOD-policy-gives-London-university-users-network-access-flexibility

44 Can BlackBerry Balance Turn RIM's Enterprise Fortunes Around?, PC Mag, See also: http://www.pcmag.com/article2/0,2817,2410246,00.asp

45 The Enterprise App Store: 10 Must-Have Feature, CIO, See also: http://www.cio.com/article/704977/The_Enterprise_App_Store_10_Must_Have_Features?page=1&taxonomyId=3061

46 Mobility: The CISO's New Agenda, Symantec, See also: http://www.symantec.com/resources/articles/article.jsp?aid=20120913-mobility-ciso-new-agenda

47 Apple's B2B App Store: Why it's a big enterprise deal, Techrepublic, See also: http://www.techrepublic.com/blog/smartphones/apples-b2b-app-store-why-its-a-big-enterprise-deal/3179

48 Facebook recodes iOS mobile app to address speed complaints, BBC, See also: http://www.bbc.co.uk/news/technology-19357161

49 FAQ: Wyse EarthSmart Computing™ Initiative, See also: http://www.wyse.co.uk/solutions/technologies/green-computing/earthsmart-computing-initiative

50 XenDesktop Planning Guide: User Bandwidht Requirements, Citrix Knowledge Centre, http://support.citrix.com/servlet/KbServlet/download/24560-102-665134/XD%20-%20Planning%20Guide%20-%20User%20Bandwidth%20Requirements.pdf

51 Medium usage employees are defined as users that generate network traffic of 12,220 KB/day. Such users are estimated to send 10 messages, receive and read 40 messages, delete 20 messages and log on and off twice every day. Average messages size assumed to be 50 kb. Source: Company Network Requirements, Microsoft Online Services, 22 March 2012. See: http://www.microsoft.com/online/help/en-us/helphowto/3dea7174-a521-4442-a7c5-5d540e09b20d.htm

52 2012 Consumerization of IT Survey; InformationWeek, See also: http://reports.informationweek.com/abstract/83/8838/it-business-strategy/research-2012-consumerization-of-it-survey.html

53 2012 Consumerization of IT Survey, InformationWeek reports, See also: http://reports.informationweek.com/abstract/83/8838/it-business-strategy/research-2012-consumerization-of-it-survey.html

54 Jailbreaking: Removing the restrictions put in place by a device manufacturer to limit the functionality of the device. The term is used specifically to refer to such actions performed with Apple devices and mobile devices more generally.

55 Workers worried by BYOD privacy intrusions: survey, Network World, See also: http://www.networkworld.com/news/2012/100112-fiberlink-survey-262940.html

56 BYOD's Phone Number Problem, CIO, See also: http://www.cio.com/article/707405/BYOD_s_Phone_Number_Problem

57 Analyst: Apple could release custom versions of its App Store for enterprise, Tabtimes, http://tabtimes.com/news/ittech-stats-research/2012/10/02/analyst-apple-could-release-custom-versions-its-app-store

58 App downloads to rise 6% in 2012, BCS, See also: http://www.bcs.org/content/conWebDoc/46879

59 New Survey Finds Over Half of Employees Use Unauthorized Consumer Based File-Sharing Apps at Work, Skydox, See also: http://www.skydox.com/company/news-room/new-survey-finds-over-half-of-employees-use-unauthorized-consumer-based-file-sharing-apps-at-work

Contacts

Deloitte Authors

Thomas Struthers
Senior Consultant, Technology, Media and Telecommunications,Strategy Consulting

Tel: +44 (0)20 7303 4203
Mobile: +44 (0)7827 956151
Email: tstruthers@deloitte.co.uk

Paul Lee
Global Director, Technology, Media and Telecommunications, Research

Tel: +44 (0)20 7303 0197
Mobile: +44 (0)7810 756262
Email: paullee@deloitte.co.uk

Designed and produced by The Creative Studio at Deloitte, London. 24126A