BYOD and the security implications of consumerisation

Key points
- Two-thirds of employees have an option to use personal devices for work
- Personal devices are poorly tracked, often lack basic security measures, and can rarely be wiped by the business
- Even if you haven’t formally allowed BYOD the chances are it’s happening in your organisation
- Mobility of smartphones and tablets makes them particularly vulnerable, and more attractive to thieves
- Users lack the knowledge to protect your corporate data on their device
- Processes, policies and tools to manage mobile devices are immature compared with corporate PC environment
- Legal and liability questions arise in the event of a security breach
- Questions arise over privacy of private data held on a personal device
- Many organisations struggle to adopt a retrospective BYOD policy
- Organisations need to define business objectives, device use cases, and risk profiles in order to understand what data needs protecting
- User training and education are key

One of the main benefits of technologies like cloud and virtualisation is that corporate applications have become more easily accessible via personal mobile devices.

The impact that consumer technology products and services are having on enterprise IT departments is generally referred to as ‘consumerisation’, and there is a growing trend toward this ‘bring-your-own-device’ (or simply ‘BYOD’) approach. Allowing, or even encouraging, the use of personal devices for work could dramatically improve productivity while reducing costs. Cisco, for example, claimed in March 2012 that BYOD has delivered savings of around 20 per cent, with its VP of IT declaring: “We don’t pay for it, and our users are happier.”

But BYOD brings its set of challenges to an organisation’s security. Technology alone cannot solve these, and as with so many other aspects of cyber security it is policy, education and governance that are critical.

This document examines the state of BYOD adoption in the UK in 2012. We’ve augmented third party research with the results of our own survey of 100 UK business users (carried out in February 2012), and we’ve canvassed a cross-section of senior business and IT staff to find out how BYOD is working in practice. We’ve identified five key security challenges for consumer devices and then suggest a way forward in developing your consumerisation security strategy. Finally we take a brief look at how technology can help, and at the challenge of applying policies retrospectively. Most organisations need to take action now, even if that action is merely to prevent the use of consumer devices for work. But for many, consumerisation does offer real opportunities to reduce cost and increase productivity.

Security is not an obstacle. It’s a business enabler. And there are substantial benefits if the rollout of consumerisation is handled well in a corporate environment.
BYOD TODAY

How prevalent is BYOD?

Current evidence suggests that at least two-thirds of employees in corporate environments now have the option to use personal devices for work.

A survey by Aberdeen Group in 2011 suggested that 72 per cent of organisations allow use of personal devices, but that only 27 per cent of these are ‘approved’ by the company. A more recent study by Harris Interactive, primarily focused on users in the US, found that as many as 80 per cent of employees are using personal devices for work while 66 per cent of businesses have not yet implemented a BYOD security policy.

In a global survey published in January 2012, 88 per cent of executives reported that employees were already using personal computing technologies for business purposes. The same survey suggested that 55 per cent of companies had already experienced a security breach as a result of personal technologies being used in the workplace.

Our own survey – conducted among UK users, rather than business managers – corroborates these findings, and suggests the UK is not far behind the US in speed of adoption. 68 per cent of respondents confirming they already using personal devices for work, although a smaller percentage of these are used ‘unofficially’ than in the Aberdeen survey.

How secure are devices now?

Many personal devices used for work appear to lack basic security measures, such as encryption and anti-malware tools. According to our survey, over half are typically unprotected, and control rests in most cases with the user.

The Harris survey warns that a third of employees who use their device for work happily connect to the company via ‘free’ or public networks, that 37 per cent do not use basic security features (such as auto-lock mechanisms), and that employees often let other people, such as family or friends, use their devices.

Generally speaking, organisations do not centrally track and control personal systems. Our user survey suggests that only fewer than one-quarter are centrally tracked, and that only 19 per cent of organisations have the capability to remotely erase data on their personal devices.

What are the most urgent challenges?

It is important to set expectations for employees and the business as early as possible. The increased adoption of cloud has accelerated the adoption of BYOD because the whole cloud model is driven by subscription-based services. This, in turn, is driving user expectations such that the cloud/personal device combination is becoming a default standard for work and leisure.

BYOD has multiplied the headaches associated with granting and withdrawing access privileges. Whereas corporate laptops were typically refreshed over a three-year cycle, consumers may upgrade personal devices as often as once a year.

Does your organisation allow you to use personal equipment for work-related tasks? Source: Company85 Consumerisation Survey, 2012
The use of insecure personal devices is currently commonplace, and from a technology standpoint businesses need to urgently consider ‘context-aware’ security capabilities that adapt access policies to device, user and location. In this way, businesses will be able to take advantage of the evolving generation of enterprise applications now being developed for distribution via consumer-class devices.
FIVE SECURITY CHALLENGES FOR THE CONSUMER DEVICE

Technologies to protect sensitive data on personal devices do exist, but technology is only part of the story. Company85 discussed BYOD with a group of CIOs and CISOs who identified five key challenges they face adopting BYOD.

1. Increased mobility

While many of the risks aren’t new (printed documents and laptops leave the office all the time) smartphones and tablets are typically much more mobile. They accompany their users on holiday, go to the pub to watch the rugby, go to that dodgy nightclub, after the office party, fall asleep on the train and wake up in Cornwall.

Users also connect them to the many unregulated wireless networks in restaurants, bars and cafés all over the world. If your corporate data is on one of these devices it's potentially exposed at all these places.

2. Likelihood of theft

Compared with the traditional corporate laptop, smartphones and tablets are far more desirable and therefore more likely to be stolen and traded.

If you’re lucky the thieves will just re-use the device and wipe the data. If the thieves decide to have a rummage around and get access to something interesting, you could end up facing regulatory fines, damage to your reputation and loss of intellectual property.

3. Lack of user awareness

Many users lack the knowledge to protect your corporate data on their devices.

Generally, your employees do not understand how the data could be compromised or, indeed, the value of the data itself. Even if you think you’ve secured basic access to email/calendar you could still be exposed. Consider these examples:

- The user takes a photo of a whiteboard containing your strategic plans, forgetting it automatically gets synchronised and published in the cloud.
- The user makes a note of all your passwords in a single notepad file on the device. And the file is probably unencrypted.
- The user backs up or syncs the device to the home PC, which is unlikely to be encrypted.

4. Lack of maturity

Corporate IT departments have had many years to perfect the management of the PC and laptop. Policies, processes and tools to manage mobile devices are relatively immature by comparison, and require constant review and enhancement.

5. Questions of liability

A BYOD device blurs the boundaries of liability. Will your insurance firm cover you in the event of a breach from a personal device? If you wipe personal data following a theft are you liable in some way?

Legal and liability risks, which vary by territory and open up another set of challenges for businesses operating internationally. In the US, for example, ‘reasonable security’ for personal devices needs to be demonstrated for a data breach case to be legally defensible.

With BYOD, organisations lose the consistency, scalability and efficiency of being able to directly install security software, to apply patches and to encrypt data in a standardised environment. According to one legal expert, if employees are unable or unwilling to implement specified security controls then in the event of a security breach the company becomes liable simply because it did not comply with its own security programme.

The good news is that there are some problems that get easier. For example, keeping traditional systems and applications up to date and patched with the latest security fixes is not a small task for many firms. Consumer products are typically much better-designed to allow end users to manage this process themselves, thus reducing cost.
FIVE KEY CONSIDERATIONS FOR YOUR SECURITY STRATEGY

Productivity and accessibility are the main benefits for introducing consumer devices, so burying them under too many layers of security is likely to be counter-productive. The best solution is one that provides adequate control and a reduction in risk without impacting usability.

1. Drive requirements from business objectives

A clear definition of the business objectives you are looking to achieve will allow you to put the cost and effort of security into context, and will help you decide whether you are willing to accept some risk to realise the benefits.

2. Understand use cases and the value of data within each case

What applications need to be available and therefore what data will they have access to? And what's the value of that data? Think about the following aspects:

- **Regulatory** For example, your internal address book or client contacts are commonly stored on consumer devices and covered by the Data Protection Act.
- **Reputational** As any government minister will tell you, there are some emails and documents you don’t want going public.
- **IPR** Legal or commercially-sensitive documents could be valuable to a competitor.
- **Access** Information allowing an attacker to gain further access to your data (passwords, conference call numbers and access codes), and information on your systems and security.

3. Create a service model aligned with your risk profile

From the risk profile determined in the use case analysis discussed above, define your service model. It's possible you may require a layered model with different levels of security to account for the different risk profiles/data. For example, use of multi-factor authentication may only be required for certain types of data.

Your solutions need to address all areas where data needs protecting. In-transit to the device? In-use by the applications themselves? Stored on the device? Even cloud-based apps may cache data locally on the device; what's in the cache? Does it need protecting and how?

4. User education

Security awareness training is as critical as defining policies and implementing tools. Building a user community who are aware of the risks, who understand how they are likely to be compromised, and who have been educated in best practice is a vital building block to a successful strategy.

5. Bake BYOD into your system design life cycle

Finally, it's more effective to build in security as systems are being designed, so update your system design lifecycle to incorporate consumer devices and their security.
ADDITIONAL CONSIDERATIONS FOR A BYOD STRATEGY

Privacy, legal and security definitions

These are a key part of the BYOD acceptable use policy, e.g.

- What devices can/can’t be used for
- What rights does the company have in the event of a device being lost; can it wipe all the data (including the personal data) for example?
- Clarification of legal liability on both sides

This is where the organisation can build in protections, and it’s suggested that employees should formally sign/acknowledge the policy prior to connecting a device.

Consider legal and HR regulations unique to each country

Employer/employee regulations differ significantly by country, so this also needs to be taken into account when defining policies.

On-boarding/off-boarding

- Ensuring devices meet your standards prior to connecting
- Ensuring access and data is removed for leavers and lost devices
- Keeping an accurate inventory of devices authorised to connect

Compliance

Compliance is a major consideration. The company is responsible for protection of personal data regardless of who owns the device, so in the event of a breach you need to be able to demonstrate to an external regulator that you took due care.

Data retention

The ability to access data to comply with legal requests is important. Do you have a copy of all the data you need to retain from a device? Do you have the ability to efficiently and effectively search it? When something goes wrong, it may be difficult or impossible to actually obtain access to or possession of the device.
WHERE CAN TECHNOLOGY HELP?

Keep the data in your data centre
Web applications, cloud apps and virtual desktop infrastructures can ensure your data stays in the data centre but that it is accessible anywhere from your consumer devices. That way, although you still need to make provision for access and authentication, you have a simple solution that will protect critical data assets with minimal disruption. The drawback is that information is not available offline, meaning that this may not be a practical solution in many common situations.

Manage device and application inventories
Mobile device management (MDM) software can provide some core security functions such as an accurate inventory of devices granted access, control over application and access provisioning, logging/auditing functions and so on.

Manage access, authentication and compliance
Device certificates can be used to uniquely identify a device and provide a mechanism for establishing encrypted communications. Protect data in-transit to the device, as well as on the device itself.

Encryption of data stored on the device provides protection if the device is stolen. Without the key or passphrase the data is unreadable even if someone gains access to the device.

Protect the device from malicious attacks
Anti-Malware protection operates in a similar way to anti-malware on a PC. As these devices grow in popularity they will become a bigger target for hackers, and stopping and cleaning up infections is an expensive business.

Sandbox and ringfence corporate data
For many, the whole point of BYOD is being able to combine work and personal tools on a single device. Personal devices owned by employees contain information on a host of private activities and content, from chat histories to bank account numbers. So where do you draw the line? What’s business, and what’s personal?

Usefully for BYOD, some tools give you the ability to ringfence corporate data from personal data. This means you won’t need to upset your employees by deleting their holiday snaps or iTunes libraries when they leave the company. But if an organisation intends enabling remote wiping, brick or blocking on personal devices, then employees also need to be aware of, and to consent to, potential damage, loss of use and personal data loss.

RETROSPECTIVE POLICY ADOPTION
Arguably, most organisations adopting a BYOD policy are doing so out of necessity, and trying to apply protection to data that’s already out in the field. Typically, employees are already using their personal devices for work, and sensitive company information is already being stored on them.

This creates a particular challenge in trying to manage the rollout of a BYOD policy in a deliberate and structured fashion. The sheer speed at which personal devices tend to be upgraded does create opportunities to enforce new security technologies, but it also raises its own questions about data security on the discarded device.

The challenge of applying a retrospective policy only serves to underline why the most critical aspect of BYOD is to inform, educate and train employees, so that business risk, productivity and cost savings are balanced with personal privacy.
IN CONCLUSION

The BYOD phenomenon is being driven top-down as well as bottom-up. In the past, technology was typically adopted bottom-up, beginning with technically-literate employees using the latest gadgets. Now, however, ease of use and the cachet of having the latest device means C-level executives are often setting the tone. When the CIO demands that mobile devices be introduced into the organisation there’s a risk that security and privacy due diligence could be rushed or even overlooked altogether.

Our focus group, and other clients we’ve spoken to, have common experience of dealing with CEOs making up their own rules. One explained that his company’s existing Blackberry policy was thrown into chaos because the CEO insisted he wanted to use his own iPad. A similar “you’re the IT people – you fix it” mentality led to one senior executive buying a new device to replace one he’d broken; and because the new device had no security certificate his company had to break its own protocols in order to grant him access.

Responsibility for security inevitably rests with the board, but in practice this is often abdicated and picked up by the IT department. If the board does not understand the risks and consequences of BYOD, the IT department needs the skills to push back and educate it. In some cases specialist consultancies may be needed to ensure due diligence and to demonstrate to the board that the CIO is managing the situation effectively.

HOW COMPANY85 CAN HELP

Company85’s security practice provides independent advice, project support and managed services, and is not tied to any technology or software vendor. Our Security Governance Framework combines deep information security skills with an enviable breadth of cross-sector experience at both operational and management levels.

Our GRC methodology incorporates frameworks such as ISO/IEC 27001:5, Information Security Forum Standard of Good Practice for Information Security, COBIT, HMG Security Policy and assessment frameworks to embed good security practices in the organisational technology, processes, culture and appropriate governance structures.

Our services provide standard build blueprints that integrate security and data privacy requirements into enterprise architectures – including cloud computing and applications – as well as operational security for data centre and storage management, incident management and resilient architectures for business continuity and disaster recovery.

Our consultants hold full security clearance to work in policing and government sectors in the UK. Clearances are processed and held by Warwickshire Police, and staff cleared include security specialists, solutions architects, project managers, and backup/storage specialists.

References