



DECISION MAKER'S GUIDE: DEVELOPING A BRING YOUR OWN DEVICE STRATEGY

Giving you a head start in successfully developing and supporting the right BYOD strategy for your organisation

TRANSFORMING COMMUNICATIONS



BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

WHAT'S INSIDE

CONTENTS

THE CHALLENGE	2
BUILDING YOUR BRING YOUR OWN DEVICE (BYOD) STRATEGY	2
WHY YOU MUST ACT ON BYOD	3
So what are the benefits of BYOD?	3
BYOD REALITY CHECK	3
DEFINE YOUR OVERALL BYOD STRATEGY	4
THREE APPROACHES TO TACKLING BYOD: THE PROS AND CONS	4
The liberal approach - Bring your own device (BYOD)	4
The hybrid approach - Choose your own device (CYOD)	5
The zero tolerance approach - Get what your given (GWYG)	7
RECOMMENDATIONS	8

All information contained within this document may not be published or reproduced wholly or in part without Azzurri's prior permission in writing.

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

THE CHALLENGE

The Bring Your Own Device phenomenon (BYOD) has resulted from the union of the unstoppable consumerisation of IT and increasingly blurred line between business and personal life.

A mobile device is an incredibly personal item and as work frequently intrudes into leisure time and vice versa – people want a single device where they can manage their professional and personal lives simultaneously.

More employees are showing up at work with their own smartphones and tablets and asking for access to corporate data, applications and networks. Whether it's your CFO clutching a new iPad or a salesman who prefers his Android device to his IT issued BlackBerry – CIOs have differing positions on whether they are discouraging, allowing or encouraging BYOD amongst employees.

BUILDING YOUR 'BRING YOUR OWN DEVICE' (BYOD) STRATEGY

It is no longer in doubt that an effective BYOD approach can drive employee satisfaction and productivity, and even reduce corporate mobile expenses. However, taking the head in the sand approach to BYOD or implementing a flawed policy will potentially cost you money! CIOs are faced with a significant set of issues and challenges to support consumer technology, while maintaining data security, controlling costs and minimising risk.

This guide is designed to help you successfully develop and implement the appropriate BYOD solution for your organisation.

The tide of BYOD is gathering momentum and it will most likely be the de facto standard in the future. But what the policies, security aspects, benefits and infrastructure will look like is far from clear. There is no clearly defined best practice for tackling BYOD and there is a broad spectrum of approaches. The significant complexities inherent mean each organisation must define their own path and many IT teams are already dealing with a mixed-ownership mobile environment.

It's not just a technology issue either; it's about policy and corporate culture. Even if you don't embrace BYOD, you need to make plans to deal with BYOD.

This guide will run through some of the key considerations and highlight the pros and cons of the three different approaches to tackling BYOD that we've identified:

- The liberal approach – Bring your own device
- The hybrid approach – Choose your own device
- The zero tolerance approach – Get what you're given

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

WHY YOU MUST ACT ON BYOD

Consumer preference, not corporate initiative is driving the pace of change – it's more than likely already happening throughout your business, so you simply have to act.

However, BYOD isn't just driven by your top execs wanting to use iPads in the office. The real driving force is the potential for BYOD to be opened up to your wider workforce to benefit both the organisation and the users. In fact, analysts Gartner have stated that they believe 90% of organisations will support corporate applications on personal devices by 2014*.

So what are the benefits of BYOD?

- **Cost savings** – BYOD can shift the upfront cost of device purchases and connectivity to the users, moving you from full service payments to a predictable monthly mobile allowance for your users.
- **Enhance users' experience, productivity and satisfaction** – Let your users work on their preferred, familiar personal devices (often superior to the corporate-liable counterpart) and carry less by consolidating to a single device for work and personal use.
- **Drive change and business improvements** - Position IT as innovative and ahead of the curve to internal users.
- **Increase personal responsibility** - BYOD leads users to be more aware of excessive usage and savvy employees are more willing to troubleshoot their own devices as a first resort, before calling for IT support.
- **Speed up the rate of technology adoption** - By allowing users to dictate technology choice, you can benefit from more innovation throughout your organisation. This can lead to new ways of working such as tablets being effectively adapted for both front and back office functions, and the latest smartphone apps being modified for business functions.

*Gartner 2011 - "Bring Your Own Mobility: Planning for Innovation and Risk Management."

BYOD REALITY CHECK

Everyone is talking about BYOD but the truth is very few are actually doing it - or at least not in a structured, strategic manner.

Letting users connect their personal liable devices to your network in an ad-hoc manner leaves your data (and reputation) vulnerable. Even where organisations have defined personal device policies and controls in place, users are frequently able to circumvent them and often the policy isn't strictly enforced. An effective BYOD strategy must secure corporate data and networks, minimise cost of implementation and enforcement, control and reduce call and device costs, preserve a high quality user experience, while staying up to date with user preferences and technology innovations.

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

DEFINE YOUR OVERALL BYOD STRATEGY

There is no well-worn BYOD path to follow. Every organisation will have specific requirements and a unique environment to contend with.

There are a number of key decisions to make which will shape your BYOD strategy including:

- What devices and operating systems will you support?
- Who will own the device?
- Who will own the SIM and the number?
- Who will be eligible for BYOD?
- What about security on the network – VPN authentication, firewall access, VPN to access wifi, guest access, network security?
- Are individuals liable for reimbursement, how much, how frequently and how will this be handled?
- How do you define the boundaries between personal and business usage and liability?
- App management and governance – what apps cannot and can be accessed and how?
- Who in the business is responsible for defining and policing your mobile policy?
- Do you have the tools and resources to support a mixed-ownership estate?

The answers to these questions will have a significant impact on the device choice, sustainability, liability, security, policy and costs of the BYOD programme.

Questions over ownership and management of the device can be a legal minefield – so ensure a policy is signed before the BYOD device is allowed to access the network.

THREE APPROACHES TO TACKLING BYOD: THE PROS AND CONS

We've identified three broad strategies organisations can adopt to successfully overcome the BYOD challenge. It will depend on what type of organisation you are, as to which one you should adopt.

1. THE LIBERAL APPROACH - BRING YOUR OWN DEVICE (BYOD)

Let staff buy the device and pay for the contract. Your people will buy the device of their choice, owning the SIM and the number, with the business compensating them with a monthly allowance (similar to a car allowance).

IT will need to take the necessary measures to secure the corporate data, applications and network on these devices – one option is to create a 'sandbox' environment where users can access corporate applications, but without opening them up to the outside world.

Pros:

Simple to implement – users pay for their own contracts from a monthly allowance and use their own personal devices, removing the burden of procurement, billing and administration from the company.

Potential cost savings – the ability to transfer the upfront cost burden to the employees and replace full service and hardware costs with a predictable monthly spend is appealing.

Superior, familiar and more productive user experience – allowing users to work on their

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

preferred devices can increase satisfaction and productivity, by giving them the tools they want to use for the work they need to do.

Cons:

Cost savings can be less than expected – most businesses currently purchase their hardware and tariffs at highly subsidised rates from the vendors. Paying full consumer prices can prove to be significantly more expensive than a standard business contract.

Excessive calls costs – with no central corporate tariffs and consumer contracts spread across multiple mobile networks, your calls costs between people within the business can soon mount up.

Acceptable usage and liability issues – users owning the device, SIM and contract can give rise to a number of challenges. Distinguishing between personal data usage and calls can be difficult and legally the users don't have to disclose this information if the contract is in their name. This can create challenges in the event of bill shock or excessive roaming charges that the employee is loath to pay.

Securing the unsecure – people use personal devices differently from business devices, which can often result in falling foul of compliance. This can also lead to concerns around privacy vs security. What happens in the event devices are lost for example? Both parties need to clearly understand what data can be remotely wiped in this scenario.

There are two key security issues to consider. Firstly, securing your data on personal devices. All devices must have the fundamental security features required to be viable for corporate use. Additionally if security features prove too restrictive, the users' experience may be damaged and make the whole concept of BYOD unappealing. For example, location monitoring can be viewed as intrusive and will users understand limitations around certain consumer apps or social networking sites?

Secondly, you must secure your corporate network against these BYOD devices accessing it. There are a number of ways to reduce the security risks associated with personal devices (guest access to your Wi-Fi for example), through both applications and written policy.

Support and suitability – just because a person wants to use a device, it doesn't mean it is suitable for the work they need to do. IT must define and clarify what they will and won't support, and during what time periods (for example business hours only?). Consumer preferences tend to shift rapidly, so can IT keep up?

Do BYOD devices get full support, best effort or no support? Depends on your strategy, but it must be agreed upon in advance by both parties. Users will often still expect IT rather than carriers to resolve their issues despite the device being in their name.

2. THE HYBRID APPROACH - CHOOSE YOUR OWN DEVICE (CYOD)

This approach allows people to use the device of their choice for work purposes, but with the organisation retaining ownership of the SIM and contract – a personal device with a company SIM. CYOD still offers users the flexibility to select their preferred device, while allowing the organisation to manage data security and have greater visibility and control around mobile costs. It offers a solution that matches the needs of the company and the employees.

Pros:

Supports device choice – employees are able to select the device that they want to use which

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

offers the user experience and functionality that suits them. A policy that doesn't support the devices users' desire – be it iPhones, Android smartphones, iPads or other tablets– or that has extensive usage restrictions will have limited appeal and impact. A variant on this approach might be to offer a recommended list of devices to users, but sourced through the company, possibly with varying levels of subsidy based upon job roles.

IT retains greater control – by owning the SIM, IT can exert much greater control over expenditure, contract negotiation, compliance, security requirements and costs. While shifting device ownership from the company to the individual can still increase corporate liability, retaining control of the SIM eliminates several grey areas around the disclosure of usage information, and also allows the company to retain number control if the employee leaves the business.

Reduce mobile call costs – calls cost are still one of the most significant areas of mobile spend. By retaining the SIM, calls between company mobiles can be offered at greatly reduced rates or even free. You also can deploy an integrated dial plan across fixed and mobile networks with consistent numbering and functionality, with preferential rates for calls between company offices and mobile devices.

Easier to manage - centralised billing from the primary network provider enables billing interrogation (through tools such as Azzurri ITEM) which offers greater visibility of tariff costs and operating efficiency. Using a single mobile network also eases the support burden and offers user familiarity.

Cons:

Personal vs corporate conflicts – while you must take steps to secure corporate data, users are equally protective of their privacy and the integrity of their personal data. IT requires a degree of management and control over the device, which can cause quarrels. For example, if the device is lost can it be fully or selectively wiped? Ensure user policies are signed and understood before allowing devices to access the network.

There are also conflicts around personal calls versus work usage. You need the tools and policies in place to track, define and recover personal call costs from users. This not only helps to ensure compliance with VAT rules around personal call costs but helps you to control and reduce your mobile call costs. Tools like Azzurri ITEM offer a simple interface which allows your people to view costs for their own devices and services and assign calls to personal or business use.

The strain on IT – you'll need resources within your team (or support from your mobility partner) who are experts on the range of devices and operating systems (iOS, Android, BlackBerry etc.) that you are supporting. You must be able to keep up to date with the fast moving consumer market to prevent the CYOD policy becoming obsolete.

Device refresh - users will want regular upgrades to their devices, similar to the yearly upgrades they are used to from consumer contracts. How will these be funded and paid for?

Support, suitability, security, procurement – while retaining ownership of the SIM mitigates a number of challenges, it's still vital to prepare your organisation with a clear policy - understood by users and IT - that protects the company. It's also important to have a personal call policy that outlines guidelines for acceptable personal usage and the ramifications for breaching these.

However, stringent security requirements and restrictions on personal usage can damage the user experience and satisfaction, so must be limited to the essentials where possible. Mobile Device Management (MDM) tools can help you to monitor usage and enforce your policy.

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

3. THE ZERO TOLERANCE APPROACH - GET WHAT YOU'RE GIVEN (GWYG)

The third strategy is to discourage rather than embrace BYOD, prioritising protecting your network and data over user experience and satisfaction. Employees will be issued business owned devices, SIMs and contracts and will be discouraged from using personal devices.

This doesn't mean they can't be issued the latest and greatest devices, but those decisions will be driven by the business and personal usage will be strictly regulated.

Pros:

As you were – this approach is the most comfortable and traditional for IT, as it eliminates a number of the concerns around supporting and securing personal devices and also securing the corporate network against these devices. It also sidesteps several potential concerns around personal vs corporate liability and procurement.

Cons:

Outdated approach – This approach can seem to be ignoring rather than addressing the challenge. Tech savvy users may well still try to circumvent your restrictions and connect to the network anyway, which could easily result in a damaging data breach.

Poor user experience and satisfaction – business-led decisions around devices and usage will inevitably lean towards the conservative, offering a lack of user satisfaction as they can't work in the way they want to, where they want to and on the technology they prefer.

BRING YOUR OWN DEVICE (BYOD) DECISION MAKERS GUIDE

RECOMMENDATIONS

Design, develop and ultimately integrate a best practice, market-competitive mobility program to suit your organisation

Organisations of all sizes and across all industries are investigating how to handle the BYOD phenomenon. The initial success of BYOD adoption will depend on effective preparation, while its long-term sustainability will depend on the ongoing quality of the employee's end-to-end experience.

Ultimately the first step to a successful mobility solution should be to understand how your people need and want to work. So the goal should be to empower staff with the right devices, connectivity options and functionality to do their jobs, at the right cost and in a secure, reliable manner.

BYOD is a complex issue and shifting the ownership of devices has a number of implications affecting technology, policy and corporate culture – many with limited precedent.

The hybrid approach currently offers the best balance between user satisfaction and corporate control – but the right solution for your organisation may be a variant or even a combination of the three highlighted approaches, applied differently to diverse users or groups across your business.

For more information on these issues and how Azzurri can help you define and deliver the right BYOD or overall mobility strategy for your organisation, including the key questions around security, support, liability, acceptable usage, re-imbursement and many more, please get in touch on **0844 324 0000**, email findoutmore@azzu.co.uk or visit <http://www.azzurricommunications.com/challenges/personal-devices.aspx>.

TRANSFORMING COMMUNICATIONS

