MOBILE DEVICE OWNERSHIP

How to choose the right mix:
BYOD/COPE/CYOD/COBO

Whitepaper
Until recently, every second story in enterprise IT news seemed to be about the ‘Bring Your Own Device’ (BYOD) phenomenon and its ever-increasing stronghold on the enterprise world. And indeed, recent research suggests that roughly 60% of global businesses may have implemented some form of BYOD already.¹

What tends to get glossed over in BYOD coverage is the degree of penetration within individual organizations. For example, International Data Group (IDG) notes that a majority of organizations that allow BYOD permit only 1% to 20% of their employees to conduct work on personally owned devices.²

So while we tend to think of organizations as either BYOD or not, the fact is that most are running more than one device ownership model. Often, a segment of the workforce is approved for BYOD, while another segment is running Corporate Liable (CL) devices.

What’s challenging for organizations of every type is determining whether to enable BYOD and to what degree. There are many questions that need to be answered. For users who aren’t going to be on BYOD, why not? What ownership model is appropriate for them? Will they remain on the model they may be used to (typically CL – also known as COBO, for Corporate-Owned, Business Only). Or is it appropriate to move them to a Corporate-Owned, Personally Enabled (COPE) or Choose Your Own Device (CYOD) scenario?

BYOD/b-y-o-d/noun
Bring Your Own Device. With this approach to enterprise mobility, workers use devices they own and maintain to conduct work-related computing and communication. There are various flavors of BYOD: employees may or may not be compensated for mobile voice and data costs by the company, for example. And IT may or may not offer support for users’ personal devices.

COBO/köbö/noun
Corporate-Owned, Business Only. In this scenario, organizations own the devices and have a policy that restricts personal use. In these scenarios, employees often own two devices – one for work and one for personal. Also known as CL, for Corporate Liable.

COPE/köp/noun
Corporate-Owned, Personally Enabled. The organization offers employees smartphones or tablets that are owned by the business but configured (via containerization) to allow personal computing and communications activities by employees.

CYOD/c-y-o-d/noun
Choose Your Own Device. Generally, linked with COPE. The organization offers a choice of devices rather than issuing a single phone or tablet.

FREE 30-DAY TRIAL
Interested in trying BES12? Run a trial free for 30 days¹² – with no impact on your existing setup. Head to blackberry.com/bes12 to learn more and sign up.
Three critical questions

In a report called “Beyond BYOD: how businesses might COPE with mobility,” research firm Ovum concludes that:

“It is clear that when it comes to planning and implementing a mobility strategy, there is no one-size-fits-all policy that suits all organizations — or even all roles within a particular organization. Ovum thinks that we will see the majority of firms adopt a mix of BYOD, CYOD, COPE and COBO strategies, applying different rules to different teams and employees depending on their particular requirements, security profile, risk profile and the kind of apps and the type of data that they need access to. Having an EMM solution capable of supporting all scenarios simultaneously would therefore be advantageous to organizations implementing mixed corporate and personally owned device deployments.”

Looking at your overall mobile-user population, what rubric might you use to assess which group should be on which ownership model? What mix of COBO, BYOD and COPE is going to give your business the best balance of security, productivity and user satisfaction? Which approach is going to best advance your workforce mobilization initiatives?

There are a few key questions to weigh up, no matter what you ultimately settle on.

For each user or group:
1. What’s the right security framework?
2. What makes the most business sense?
3. What do employees want and need?

How does your employer provide you with a smartphone to use at work?

For all the press COPE and CYOD have been getting over the last year, few statistics have surfaced on their adoption. Ovum’s research found that CYOD/COPE is being used by approximately 7% of the surveyed workforce. COBO is still at nearly 9%.  

![Current spread of enterprise mobile provisioning strategies](image)

### The three flavors of BYOD (per Ovum):

**Unrestricted, supported BYOD:** Employees are allowed to use any personal device they want for work and the company will aim to support it.

**Restricted, supported BYOD:** Employees are allowed to use a personal device for work as long as it is on a list of approved devices that the company will support.

**Unrestricted, unsupported BYOD:** Employees are allowed to use any personal device they want for work, but it is left unmanaged and unsupported by the company.
1. What’s the right security framework?

As we’ve discussed, at the company level, regulatory compliance issues mean that some organizations will choose to stick with a strictly COBO model.

If your organization is highly security conscious or operates in a regulated industry like finance or healthcare, or in government, you may need features that aren’t readily accessible through most BYOD solutions. The issue isn’t always one of technical capability, but often, one of management effort. If you’re allowing (and attempting to support) a wide range of BYOD devices, you’ve got multiple platforms to attend to and multiple potential areas of vulnerability.

Sometimes, BYOD won’t see the light of day simply because an organization’s legal team doesn’t want to enter into what they might perceive as higher-risk territory. Personal data is one example, and privacy laws vary from country to country. If a company-owned device is lost or stolen, IT can, through its MDM/EMM solution, wipe the device remotely to safeguard sensitive data. But in a number of countries (including South Korea, Italy and France) it’s illegal for a company to wipe a device it doesn’t own. Legal departments often default, therefore, to the easiest option, which is to insist on corporate device ownership.

But if you’re not in a regulated environment, are there particular users in your organization who should remain on COBO? Let’s assume that security is the critical driver. With a fully locked-down device, organizations maintain control over granular policies to control every aspect of device use.

Disable the camera. Shut off access to web browsing beyond the intranet. Prevent app downloads.

Let’s consider the roles with the highest security needs in any organization. The Chief Executive Officer. The Chief Financial Officer. The VP of Human Resources. Should they be able to access sensitive work data on a device they own personally and use for non-work purposes too?

What are the risks? Where do the liabilities lie if something goes wrong? For IT, this raises a lot of secondary questions. Do you trust the security on the device itself? How secure is your containerization approach? How well protected is data as it travels from the device, behind the firewall to various servers and back again? How solid is your Data Leak Prevention (DLP) capability? How much are you relying on the user to adhere to your usage policies? If you’ve got several systems and solutions at play, where are the weak links in how they interact with each other?

Many senior IT leaders will only feel comfortable in scenarios where those with the highest security needs don’t own the device or use it for their personal lives.

“Being able to identify and remediate vulnerabilities on so many different devices is a gargantuan task. It takes staffing and training to do properly. Any single hardware device is capable of running multiple iterations of the operating system, each with its own unique security issues. Taking the attitude that the end user can and will be responsible for keeping the device current is not feasible for a multitude of reasons. What if a forced OS upgrade breaks a user’s favorite personal app?”

- Jeffrey Brandt, Editor, Law Technology Daily Digest
2. What makes the most business sense?

One of the key business drivers for BYOD originally was, of course, cost savings. You’ll find thousands of articles on this topic, many of which suggest that those savings can be realized. There are just as many that suggest those savings aren’t likely to materialize in the way many predicted. It depends on what you consider and what you value.

The most obvious trade-off to consider is having to pay for devices with COPE versus not having that hardware capital expenditure with BYOD.

On the other hand, when you supply devices and the accompanying voice and data plans, you gain the ability to negotiate bulk rates for these services, known as pool plans. Some pundits suggest that businesses can chop those expenses by up to 70% through negotiation.

Here are a few considerations that sometimes go under the radar when enterprises look at business cases for BYOD versus COPE for specific user segments.

Support costs
For BYOD users, you may be able to hand off support issues to the employee to take up with the carrier. In COPE, that may not be the case. What’s the impact on your help desk?

Consider this anecdote from a Computerworld piece called “Running the ROI numbers on BYOD”: “One client boasted that the average number of tickets its help desk had to handle per month had declined from 0.55 per user to 0.44 with the advent of BYOD. But the client didn’t account for the fact that the BYOD program had expanded the number of users needing support from 10,000 to 23,000. That means the total number of tickets increased from 5,500 a month to more than 10,000 a month.”

Location
BYOD adoption varies widely globally. “So far, BYOD adoption is most common in companies with between $500 million and $5 billion in revenue, but there are significant differences according to geography,” according to a recent Gartner report. “The U.S. adoption rate is double that of Europe, but the highest rates are in India, China, and Brazil.”

What drives these differences? Corporate culture? Regulatory/legal factors? Costs and expectations around compensation? Whatever the reasons, you may find that a BYOD model is a natural fit for employees in one country, while COPE is better suited to those in another.

Key considerations in BYOD vs COPE planning:

1. **COPE VS BYOD**
   - COPE: You’ve got a lot of hardware to buy, deploy, maintain, manage and retire.
   - BYOD: You’ve got a lot of administration to sort out if you’re reimbursing. And no bargaining power on plans.

2. **SUPPORT**
   - Can BYOD lower your support costs? Maybe. But take care in making these calculations. BYOD may mean a lot more employees are now mobile, which can add to the load on your help desks and network.

3. **LOCATION**
   - The U.S. BYOD adoption rate is double that of Europe, but the highest rates are in India, China, and Brazil.
3. What do employees want, and how much do they care?

BYOD has had so much attention that CIOs have begun to assume that this model is the one employees are clamoring for. In many cases that’s absolutely true – after all, it was employee demand that gave BYOD life in the first place. But it’s unwise to leap to conclusions on this subject. Ovum reports that almost 60% agree that being given a device to use for personal as well as work purposes would be a perk, while only 14.4% disagree with that opinion.3

Some employees, particularly in certain roles, will view the ability to bring their own device to work a real plus. Others will see a lot of appeal in their company providing them with a device. Surveys are a great way to get a sense of where specific employee types stand. Make sure to cover your bases in terms of demographics, role types and regions. It’s easy to assume that the youngest employees in your company will gravitate to BYOD, but your research may tell you they’re just as happy (or happier) to be provided with a device and not have to worry about reimbursement or expense claims. By the same token, just because your senior executives have been on COBO devices for years doesn’t mean they want to continue that way. Some enterprises run a voluntary BYOD program and gauge interest that way.

Employee attitudes to COPE are largely favorable

"If my company provided me with a smartphone or tablet of my choice, to be used for personal as well as work purposes, I would see this as a perk."9

- Strongly agree: 37.3%
- Agree: 25.8%
- No opinion: 22.5%
- Disagree: 6.0%
- Strongly disagree: 8.4%
BlackBerry supports all device ownership models

BES12 provides secure, cross-platform mobility management for organizations of all shapes and sizes and supports all device ownership models. These capabilities are consistent across the on-premise and cloud versions of BES12.

BYOD
To really make BYOD work you need the right strategy and company usage policy, as well as the right cross-platform Enterprise Mobility Management (EMM) solution.

BlackBerry provides effective management of BYOD users alongside corporate-owned device users, from a single management console, on-premise or in the cloud. Whether employees choose a BlackBerry, iOS, Android™, or Windows® Phone device, BES12 perfectly balances user and enterprise needs by seamlessly securing work data and apps while protecting personal usage and privacy.

COPE/CYOD
BlackBerry’s ability to support a COPE environment was documented in a 2014 report from Gartner Inc. entitled “Protecting Enterprise Information on Mobile Devices, Using Managed Information Containers.” The report states that “BlackBerry comes closest to offering a product to support COPE.

BlackBerry® 10 devices running BES12, include a Personal Space that is separate from the Work Space on the device, and policies can be set as to what the user is allowed to do within the Personal Space. Other container products do not support such a model.”

COBO
For those organizations and users who want or need fully locked-down devices: BlackBerry is the only integrated end-to-end smartphone and Enterprise Mobility Management (EMM) platform provider offering a real COBO device and application management option.

Gold level EMM delivers the optimum solution for high-security mobility. When a BlackBerry 10 device is managed through BES12 with the Gold level EMM option, organizations can deploy a corporate-only use model where access to device features and capabilities, including social media feeds and public application access, can be fully managed and, if required, prohibited. Alternatively, a managed Personal Space can be enabled on the device through BlackBerry® Balance™, which allows users to make the most of their device for personal use while the enterprise retains full device control and all work related content is fully protected within the Work Space.
Ovum on COBO

"In terms of data security and management, COBO should be the least risky model. Organizations can install whatever solutions they deem relevant on the devices and keep complete control over what can and can’t be accessed on them – they can lock devices down as much as required.

This means that using COBO devices can be the safest option, but the risk is in providing a poor user experience and restricting access to desired applications, driving employees to find ways around the system and finding other ways to do their job i.e. turning them back to BYOD.

Having an end-to-end EMM solution for COBO – e.g. one that supplies the device, secure infrastructure and the management software – would enable a consistent experience and also allow for newly released devices to be supported easily. BlackBerry is the originator and most prominent vendor offering this all-inclusive hardware and software package for COBO deployments, and remains the leader in terms of end-to-end device security and management.”

The lowest Total Cost of Ownership (TCO)

BES12 has been designed to be flexible to meet every scenario enterprises may choose or encounter. Whatever mix of device ownership models you start with or end up settling on, BES12, on premise, in the cloud or a hybrid of both, provides the lowest cost cross-platform solution on the market.

More specifically, BES12 Cloud is cost-effective, scalable, secure, simple business enablement for organizations of all sizes. There is no hardware or servers to install and low monthly or annual subscriptions means no on-prem data center operating costs.

The Advantage level technical support included with every BES12 subscription comes with Software Assurance so upgrades and updates don’t cost anything and your software is always current with the latest service pack.
To sign up for a free 30-day BES12 trial\(^\text{12}\), head to [blackberry.com/bes12](http://blackberry.com/bes12).