Bring Your Own Device: New Opportunities, New Challenges

Published: 16 August 2012

Analyst(s): David A. Willis

The rise of "bring your own device" programs is the single most radical shift in the economics of client computing for business since PCs invaded the workplace. In this roundup of Gartner research, IT leaders will find advice and links that address every part of a BYOD strategy.

Analysis

Bring your own device (BYOD) programs are transforming the economics of client computing. This document summarizes our top-level advice to clients and provides readers with detailed links that can address every part of the BYOD strategy: from planning, to policy, to project management, to cost estimations. We drive deeper into the business case and the question of whether BYOD saves money, and we also assess the state of the art in management and security technologies.

BYOD is an alternative strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data. For most organizations, the program is limited to smartphones and tablets, but the strategy may also be used for PCs. It may or may not include subsidies for equipment or service fees.

As stated in "CIOs' Next-Generation Mobile Strategy Checklist," every business needs a clearly articulated position on BYOD, even if a business chooses not to allow for it. The policy must be easy to understand and follow.

Why Is BYOD Happening Now?

There are many reasons for this sudden shift toward BYOD. The market for mobile devices is booming and has hit the mainstream. Roughly half of U.S. adults own a smartphone, with higher rates among more educated and well-off individuals (data is sourced from The Pew Charitable Trusts, March 2012). Capabilities are at parity: The basic commodity endpoint device used in business versus those used by consumers is converging. In the mid-1990s, a device used in business looked very different from a device used by a consumer, but that is not true today. In fact, the computing power in a mainstream consumer smartphone or tablet is more than sufficient for the needs of a business user, often far exceeding what is needed. Simultaneously, advances in network performance allow the personal device to be married to powerful software that resides in the cloud.
Mobile innovation is now driven more by consumer markets than by business markets. Affordability is not only putting very powerful technology in the hands of consumers, but those consumers are also upgrading at a much-faster rate. Thus, an organization may keep up with mobile technology advancements more effectively by aligning to the consumer, rather than maintaining the much-slower pace of business technology adoption, with its long cycle of detailed requirements analysis, established refresh rates and centralized procurement heritage. Consumers also enjoy equipment and domestic service pricing that often matches the best deals that an enterprise can get on behalf of its users.

As consumer and business hardware comes into parity, the differences between consumer and enterprise endpoints exist only in software, which is fortunately an area in which IT can influence and even control at some degree.

A New Contract

In a BYOD approach, users are permitted certain access rights to enterprise applications and information on personally owned devices, subject to user acceptance of enterprise security and management policies. The device is selected and purchased by the user, although IT may provide a list of acceptable devices for the user to purchase. In turn, IT provides partial or full support for device access, applications and data: In each case, support may be limited. The organization may provide full, partial or no reimbursement for the device or service plan.

The strategy is often intended for a large minority of professional employees and part-time workers, but it is also being considered for the majority of contractors, interns, consultants and other workers not directly employed by the enterprise.

IT’s best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure controls and education in the near term, and with application management and appropriate cloud services in the longer term.

Best practices for BYOD include creating organization-specific BYOD policies, developed in conjunction with legal and HR; guidelines on who is eligible or not for the program; new employee agreements for support, risk and responsibility; adjustments to service levels; service desk training; funding and reimbursement strategies; employee education; and IT publishing specifications on acceptable devices. The approach typically requires customization by country. It may have tax implications for both employee and employer.

BYOD impacts corporate risk, infrastructure and software costs, customer service levels, and total cost of ownership. It typically requires significant technology protections (including authentication, network access control [NAC], mobile device management [MDM] and mobile application management, encryption/containerization, and content protections) and delivery mechanisms (app stores, file-sharing systems and desktop virtualization). It often forces adoption of thinner-client architectures, multiplatform mobile application development environments and frameworks, and HTML5 for mobile applications.

For research on this topic, see:

- "Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices"
The Current State of BYOD in Business

Formal BYOD programs are a relatively new but fast-growing phenomenon. In 2009, it was typical to see no BYOD program whatsoever in business, even though there has always been a substantial amount of "stealth" use of personal devices. But now, formal programs supported by IT are rapidly gaining steam. In a 2011 study, we found that, on average, U.S. CIOs expect 38% of their workforce to use personal devices at work by the end of 2012. Notably, CIOs in Europe anticipate only about half the U.S. rate — so we are seeing different adoption rates around the world (see "CIO Attitudes Toward Consumerization of Mobile Devices and Applications").

Note that these numbers apply mostly to bring your own (BYO) smartphone and BYO tablet programs and that policies supporting employee-purchased PCs are relatively rare, currently estimated at less than 5% of companies.

BYOD Programs Can Reduce Cost, but They Typically Do Not

With the wide range of capabilities brought by mobile devices and the myriad ways in which business processes are being reinvented as a result, we are entering a time of tremendous change.

There are instances where current-state mobility costs can be cut, such as in the common case of replacing an existing BlackBerry device that provides mobile email and calendaring. To take an example, moving a 500-person mobile workforce running corporate-supplied BlackBerry devices at a cost of $90 per month to personally owned devices results in a 29% reduction in hard costs, using a standard $50-per-month reimbursement rate, while investing roughly $360 per user in new infrastructure, software and support (see Figure 1).
Figure 1. One Common Situation Where BYO Saves Money: BlackBerry Replacement

Before
$1M

$90/month/user

After
$1.08M Over Two Years

$780K

$15/month/user software and related costs
(likely to increase with time)

$50/month/user service fee
(might decrease with time)

$300K Savings in Two Years

Source: Gartner (August 2012)

Just as we saw with home broadband in the past decade, the expectation that the company will supply full reimbursement for equipment/services will decline over time, and we will see the typical employer favor reimbursing only a portion of the monthly bill. We also expect that, as adoption grows and prices continue to decline, employers will reduce the amount they reimburse.

But as businesses look to drive ever more capability to the mobile device, the costs of software, infrastructure, personnel support and related services will increase over time. Once we start including file sharing, business applications and collaboration tools, the costs to provide mobile services go up dramatically.

However, BYOD does not reduce costs in other common situations, including when an organization has:

- Frequent international travelers, where devices and plans are complex and best centrally managed. Employees are often confused and undisciplined in their use of international services.
- Employees located in countries where remuneration for device usage is considered taxable income.
Situations where custom mobile application integration using specific device platforms is required, and where the business has an urgent need for a specific strategic set of mobile applications.

Heavy use of hosted virtual desktop (HVD), especially where application software licenses will increase.

Low acceptance of the BYOD model. A certain critical mass needs to be hit, or the program will not reach a sufficient scale to warrant support.

But there are other strong drivers besides cost reduction, where BYOD delivers both tangible and intangible benefits to an organization. These include:

- Improving employee satisfaction and attracting and retaining staff. Gartner clients commonly report that the perception of IT improves substantially among users who opt into the BYOD program.
- Expanding the number of mobile users in the workforce and presenting new opportunities for mobile applications. Whereas opt-in programs typically move 40% of currently qualified mobile workers into the BYOD program, BYOD could also expand the total number of mobile users substantially — by 50% or more. Thus, for many organizations, the number of workers in the employee-liable program will be double that of the corporate-liable program within two years' time.
- Offloading the management of nonstrategic devices from IT, allowing limited fixed-cost resources to be applied elsewhere.
- Adopting new technology at a greater speed.

Costs to Consider — And the Critical Technologies

There are many potential costs to be considered, many of which are substantial. A BYOD program typically requires strong isolation methods, including security protections (such as authentication, NAC, MDM and mobile application management, encryption and containerization, and content protections) and delivery mechanisms (app stores, file-sharing systems and desktop virtualization). It often forces adoption of thinner-client architectures, multiplatform mobile application development environments and frameworks, and HTML5 for mobile applications. User self-support tools also require some investment.

For research on this topic, see:

- "Choose the Right Tools to Securely Support Consumer-Driven Smartphones and Tablets"
- "Magic Quadrant for Mobile Device Management Software"
- "Critical Capabilities for Mobile Device Management"
- "Enterprises Can Apply an App Store Approach to Support Employees' Smartphones and Tablets"
Other substantial costs include HVD and software licensing fees, which can often break the economics of the program. In "The Cost of Connecting Apple’s iPad and Other User-Owned Mobile Devices to the Corporate Network," we illustrate how shifting to an HVD model increases the one-time costs per device by more than $600. In "Ensure Apple iPads Are Licensed Correctly to Use Microsoft Products to Avoid Problems," we help clients navigate the complicated task of ensuring that their licenses are in order. Another factor at play is the lower rate of user satisfaction with HVDs on non-PC devices that do not use a standard keyboard and large screen. Organizations should view HVD as a tactical approach to providing applications and not the ultimate solution to the need for native applications or browser-based HTML5 applications.

**International usage fees** are another major factor to consider. In general, employees who roam frequently between countries may incur significant costs, and we advise that businesses continue to manage these costs on behalf of their most active international travelers. Almost daily, we hear of horror stories, where a day trip incurred a multi-thousand-dollar bill because the employee was unaware of the charges being incurred. Companies need to be prepared for these surprises and plan an approach that holds employees and managers accountable for unusually high fees.

**Taxation.** Corporate reimbursement policies must be developed in conjunction with legal and HR departments, focusing on under what conditions a subsidy for device usage can be taxed. The tax implications can be quite complex, varying by tax jurisdiction. Tax laws are often vague on the distinction between various device types, such as mobile phones, tablets or PCs. They may also change year to year. The safest general position is to avoid a fixed stipend and instead favor reimbursement. For example, the U.S. Internal Revenue Service ruling SBSE-04-0911-083 specifies that reimbursement of normal personal mobile phone usage is not taxable, but it applies to the current tax period only; it may change in time. Note that other tax rules may still apply, such as at the state level.

In some countries, the cleanest way to manage tax issues is to renegotiate the employee agreement and state that the salary is set, reflecting that the employee pay for certain IT devices and services. This way, employees may deduct the cost in their personal tax returns.

**Soft costs.** A variety of hidden costs are also worth considering as side effects. Will productivity be affected by user self-support? Should highly paid professional workers with limited technical expertise be spending time diagnosing problems with their devices, rather than using a lower-paid expert within IT who might be able to solve problems more quickly? In the main, these issues have not surfaced as major problems in early BYOD deployments for smartphones and tablets, but we suggest that organizations monitor user incidents and retain a corporate-liable program for workers who need or prefer higher levels of assistance.
Getting Started

A comprehensive project plan is essential, and there are many steps involved, as noted in detail in "Checklist for Determining Enterprise Readiness to Support Employee-Owned Devices" and "Media Tablets and Beyond: The Impact of Mobile Devices on Enterprise Management."

A New User Contract — What the Policy Looks Like

The BYOD approach means that the business and the user need to reach a new understanding. The organization gives the employee the freedom to choose any appropriate device; in exchange, users agree to give up at least a minor level of control over their personal devices. Users take on a responsibility that their devices are appropriate for the job; to maintain these devices, including backing up their own data; to support themselves; and, critically, not to circumvent the policy. They accept the risks of a remote device wipe, which might include the erasure of personal information, and the possibility that the device could be seized as part of an e-discovery process. These are just a few of the issues addressed in detail in "Creating a Bring Your Own Device (BYOD) Policy" and "Seven Steps to Planning and Developing a Superior Mobile Device Policy." A toolkit that clients can use to start their own policy can be found in "Toolkit: BYOD Mobile Device Policy Template."

Pull in the right people into the team. These policies must be built in conjunction with legal and HR departments for the tax, labor, corporate liability and employee privacy implications. Start with a standard policy that would apply anywhere, and create customized versions by country if necessary.

It's Not for Every Company, or Every Employee

There will be wide variances in BYOD adoption across the world — by geography, industry and corporate culture. Most BYOD programs are opt-in programs; a 40% take rate is good, although we occasionally see much-higher acceptance. For the vast majority of companies, it is not possible to force all users into a BYOD program without substantial financial investments — and considerable support from senior management. Legal and employee relations/union issues are likely to surface with forced BYOD programs. We anticipate that corporate-liable, corporate-specified device programs will stay in place for nearly all large organizations.

Lessons From the Field

In "Field Research: Mobility in the Age of Consumerization," we study 15 different organizations and distill their experiences with their BYOD policies. We find a variety of different responses to the program. Likewise, a number of examples are cited in "Choose the Right Tools to Securely Support Consumer-Driven Smartphones and Tablets."

Occasionally, an organization will take a bold step into a program that encompasses all devices: not only smartphones and tablets, but PCs as well. Suncorp, an Australian financial services firm with approximately 20,000 deployed PCs, has made just that move — as analyzed in "Road Notes on BYO Computer: Revolution or Evolution?" Some industries are more highly affected by BYOD, and controls vary widely by industry. As noted in upcoming Gartner surveys, transportation and banking
organizations tend to have more restrictions limiting BYOD than others, such as education, retail or healthcare.

For more research on this topic, see:

- "As the Mobility Movement Gains Momentum, Healthcare Delivery Organizations Must Prepare to Adapt"
- "BYOD in Education by Design, Not Default"
- "Address the Risks of BYOD Within Higher Education"

What Does the Future Hold?

We are likely to see highly successful BYOD programs in the coming years. Many businesses will expand beyond smartphones and tablets and embrace BYOD for PCs. The rise of Ultrabooks, convertibles and other form factors will put new pressure on the PC program, because many of these devices carry a premium and are unlikely to be quickly embraced by IT for its users — even as they become popular in the market. For an analysis of the costs of BYO PC, see "The Impact of BYOC on Management and Support." Beyond PCs, it is likely that users will discover new uses for emerging devices not initially understood by IT planners, much like we saw with the iPad. For more adaptive organizations, "try it and learn from it" will be the new approach to testing the applicability of new devices to the business.

It won't stop with BYO PC. "Bring your own IT" is on the horizon. Once these new devices are in the mix, employees will be bringing their own applications, collaboration systems and even social networks into business.

Despite the opportunities, we should expect developments that will force some companies to move more conservatively. We are highly likely to see reports of significant data leakage through employee-owned devices. Employees and unions will be increasingly concerned about the implications of having access all the time, anywhere — does this mean the employee is expected to be on call at all times? They will also raise the issue of employee privacy as personal data and even individual location could be visible to employers. As employers increasingly attempt to get more workers into the BYOD program, employers may see it as a bare-faced move to cut costs at the employee’s expense. The hidden costs of shifting from efficient IT support to messier user self-support may lead some to question the savings. The issue will remain at the forefront for IT planners for some time.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp