Bring your own device

Agility through consistent delivery

Advisory Services

Table of contents

The heart of the matter

Information workers today are increasingly tech-savvy and self-empowered. The typical employee owns an assortment of laptops, smartphones, tablets and PCs that are often more advanced than what most information technology departments can offer.

Not surprisingly, many employees prefer to access corporate resources using their own technology because it is familiar, powerful and already an integral part of their everyday lives.

The consumerization of IT has become an unstoppable force. This trend, also referred to as "bring your own device" or BYOD, describes an environment in which employees use personal technology – laptops, smart phones, tablets, and even desktop PCs – to access corporate networks, applications and data. A recent global survey of CIOs found that 28 percent of their workforce is currently using personal devices for work-related tasks, and this percentage is expected to rise to 35 percent by mid-2013.[1]

The benefits of BYOD are undeniably compelling. Organizations that have embraced BYOD have reported improved productivity and employee retention, enhanced mobility, a more flexible work environment and improved IT value to the business. BYOD can enable virtual work environments that provide individual workers the freedom to work when and where they choose. That, ultimately, can help trim operating costs.

Yet for all its promise, BYOD is fraught with risk in the absence of a proper security strategy. Support of heterogeneous devices without the proper forethought makes it very difficult for IT to establish and enforce controls at the endpoints, and that opens the door to potential data breaches and leakage through mechanisms such as malware. Without proper alignment to business needs, IT will face thorny issues implementing the right level of technical support and enforcement of policies among users.

It is not entirely surprising, then, that employee-owned devices have set off security alarms among IT decision makers. In a recent Gartner survey on the consumerization of mobile devices, when asked "Do you believe that the security currently applied to mobile devices, such as smartphones and tablets, used in your organization is adequate and would satisfy an auditor?" only 27% of U.S. respondents believed their mobile security was adequate to pass an.[2]

BYOD is top of mind, yet most businesses have not yet developed appropriate policies. Only 43 percent of respondents to PwC's 2012 Global Information Security Survey said that their organization has implemented a security strategy for use of employee-owned devices.[3]

CIOs must rethink the traditional, rigid approach to governing access to data, applications and networks. What is needed is a device-agnostic strategy that leverages investments in the employee's personal technology to create a more mobile, agile and cost-effective platform for the business.

---

[1] Citrix, IT Organizations Embrace Bring-Your-Own Devices, July 2011
[2] Gartner, CIO Attitudes Toward Consumerization of Mobile Devices and Applications, May 2011, page 5 Gartner surveyed CIOs and senior IT executives attending our U.S. and European CIO forums in March and April 2011. These surveys were conducted during a series of workshops on managing mobile devices and surviving consumerization
[3] PwC, 2012 Global Information Security Survey, September 2011

An in-depth discussion

Tech-centric consumers have become a powerful catalyst for change in the IT environment. As employee ownership and command of technology have eclipsed the capabilities of corporate IT, organizations are beginning to understand that they must modernize IT strategies to accommodate BYOD and mobile computing.

IT has traditionally discouraged the use of personal devices by locking down access to resources to ensure the security of data, applications and the network. Today, however, IT leaders are abandoning this rigid, lockstep approach to security and adopting a new "any device" policy that supports popular mobile operating systems and enables user-owned devices to connect to corporate resources.

This device-agnostic strategy represents a new approach to security that will require a fundamental reordering of IT priorities. New technologies such as virtualization can efficiently lock down applications and their access, allowing IT to securely accommodate employee-owned hardware without regard to the device itself.

The path toward a device-agnostic enterprise has been in the making for years as companies adopted Internet-delivered content and applications that employ standard protocols. Many organizations, for instance, already allow access to browser-based application stores, app stores for smartphones and tablets, and in-browser client-server applications.

Technologies such as desktop virtualization, application virtualization, and HTML5 enable IT to securely deliver content without the need to invest in platform security, the traditional strategy of information security.

Moving lockdown and lockout controls from the desktop and laptop into the network layer makes it possible for IT to allow smartphones and other mobile devices to access corporate resources; it also creates the ability to allow almost any device to connect securely within the organization. A BYOD strategy can effectively consolidate all mobile support with internal application and data delivery infrastructure and support.

We believe that adoption of device-agnostic technologies can allow IT to securely support employee-owned devices and, in doing so, more quickly respond to the needs of the business and its employees to ensure growth and employee retention.

IT organizations that cogently broaden smartphone support and embrace popular consumer technologies such as the iPad can increase employee productivity, mobility and flexibility. Building a solution around a single device or a set of devices is a tactical approach, however. Granting personal devices access to corporate resources on a broader scale is a forward-thinking strategy that can yield game-changing advantages to the business.

The result? An agile, innovative solution to business needs and security in a device-agnostic environment.

The many benefits of bring your own

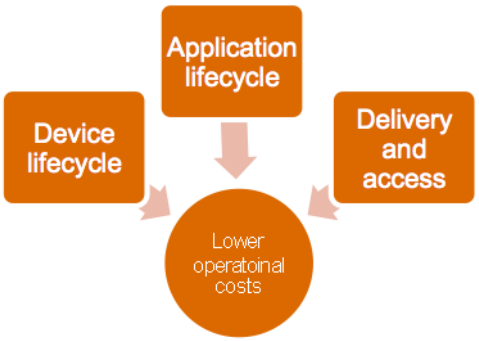
Organizations that have adopted a bring-your-own strategy often cite employee satisfaction and business productivity as key advantages. Other benefits include enhanced collaboration and mobility, expanded mobile access to resources, reduced spending on sourcing and support of devices, lessened responsibility for device lifecycle management, as well as consolidation of infrastructure and tools across many IT disciplines.

An infrastructure that allows access from a large set of device types must be secure. An advantage of a device-agnostic infrastructure is that security is integrated into the design; it is not, as with traditional infrastructure, an overlay. A BYOD strategy requires that organizations apply the controls typically found on endpoint devices to the network layer. As a result, a comprehensive device-agnostic approach can simplify and strengthen security of networks, data and applications.

Allowing employee-owned devices to connect to corporate resources can also save costs when coupled with the right infrastructure and policies. In a BYOD world, IT is no longer responsible for sourcing and procuring hardware such as smartphones, laptops, tablets and even desktops. Instead, employees are offered a stipend to purchase the computing device of their choice, assuming it meets the company's baseline requirements.

Stipends also can be offered to cover all or part of an employee's smartphone data plan, a perk for the knowledge worker who does not use a company-issued handset as a primary device. At the same time, this approach frees the IT organization from procuring, maintaining and refreshing smartphones, and relieves IT of the responsibility of managing service plans.

BYOD also makes telecommuting more feasible and available to a broader set of employees, who often regard working from home as a coveted privilege. For the business, telecommuting enables operations to take advantage of cost-saving options such as the hoteling of office floor space, and can help centralize the IT support organization.



A BYOD strategy that frees application lifecycles from devices and consolidates delivery mechanisms can yield operational savings. In a model BYOD environment, software can be stored on centralized servers; it does not have to be directly installed on individual devices. This obviates the need for IT to support the installation and upkeep of each device's software inventory. It also makes it possible to streamline support of the application's software patches, upgrades and migrations, including the prospect of near-instant rollback upgrade protection. What's more, the use of a secured application development methodology and data delivery mechanisms that employ technologies such as HTML5 and PKI encryption can further separate the device from a corporate data footprint. Developing and delivering of applications on a centralized model enables IT to consolidate development efforts and remove the need for regression testing across multiple devices.

A strategic deployment of a device-agnostic enterprise ultimately will enable IT to realize cost benefits in user-support initiatives. Application support is lessened, since all installations, use and maintenance can be centralized and standardized on a server image; IT will no longer be required to resolve end-user DLL issues or develop multiple delivery methods to allow different versions of the same application to a user.

A device-agnostic strategy also can help mitigate security risks from attack vectors such as malware. Application virtualization and desktop virtualization, coupled with network segmentation, for instance, limit the impact radius of attacks because the device is segmented from direct contact with application servers and business data, essentially quarantined. The device is viewing the network but is not actually interacting with the application.

The challenges of an any-device implementation

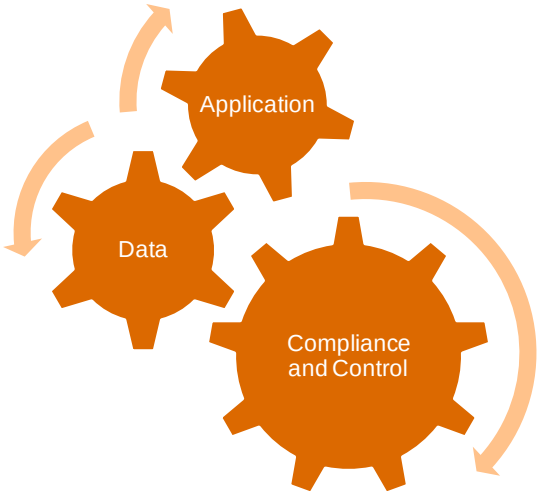
For all its advantages, a BYOD strategy also presents some hurdles that should be considered early in the development of a device-agnostic strategy.

Data security, of course, is paramount. Security should be baked into every aspect of access to the network, data and applications. Protection of the corporate data through isolation from personal data should also be addressed.

Transitioning to a device-agnostic infrastructure will require new skills from network engineers and security teams, as well as up-to-date network access controls. Before a BYOD strategy can be implemented, IT must gain a comprehensive understanding of how these technologies are applied.

A fundamental security component of a BYOD infrastructure is the addition of an MDM (mobile device management) solution. These solutions limit or resolve IT policies against traditional mobile devices. They do not address the more strategic considerations necessary to create a BYOD infrastructure, however, and should be considered tactical in nature when not a part of a comprehensive strategy.

The weakest link in mobile device security is often the user. Liability often originates at the top: C-level executives often muscle exceptions to use personal devices, but these leaders pose the greatest risk because they have access to the company's most important information. A BYOD strategy will demand that CIOs implement and enforce a very strong set of policies to govern employee use of devices and access. Policies should be carefully designed to meet the needs of all users while safeguarding the organization's data according to its business model.



Device support should be meticulously designed to meet the needs of users while ensuring that IT is not unduly burdened with hardware and device on-boarding issues. A careful balance between employee satisfaction and access to IT resources is critical. Organizations should involve human resources and legal departments to ensure that the policies are acceptable to employees and also meet requirements for data security and compliance mandates.

Employees who participate in a BYOD program should be required to sign binding agreements before being allowed to access resources using a personal device. Participants must understand that they may be required to relinquish some rights to control of the device, such as requirements to install a mobile device management client, encryption of email or the device itself, and use of strong passwords. A clear understanding of these stipulations should be articulated to the employee to ensure a successful BYOD transition.

At a minimum, BYOD policies should require installation of the organization's security profiles on the equipment, assert the right to wipe the device if it is lost or stolen, and spell out the support and repair policies for the equipment. Employees also should be required to back up personal information stored on the devices because the organization cannot be responsible for loss of personal files should the hardware require a data wipe.

One particularly thorny issue can arise if an organization initiates a legal hold against a BYOD user and IT is required to temporarily confiscate the device to capture its state and data. Similarly, when an employee leaves the company, voluntarily or otherwise, IT should be entitled to legally wipe corporate data and applications from the device. This typically requires up-front permission from the user.

Another challenge for BYOD programs arises from costs associated with use of devices. If, for instance, the company retains management of a smartphone service plan, employees must understand that they will be responsible for costs associated with excessive data use, copious 411 calls or selection of smartphones that are more expensive to use in some circumstances.

Finally, a BYOD strategy will represent a huge cultural shift for most organizations. To ensure that all possible implications are considered, CIOs must involve business leaders, as well as HR, auditors and legal staff, in the earliest phases of developing a BYOD strategy.

A new approach to delivery, access and packaging

When compared with legacy approaches, a device-agnostic BYOD strategy offers more efficient methods to deliver, access and package data and applications. At its core, a BYOD infrastructure relies on virtualization and segmentation techniques, but it also requires a clear strategy for audit, user support and on-boarding.

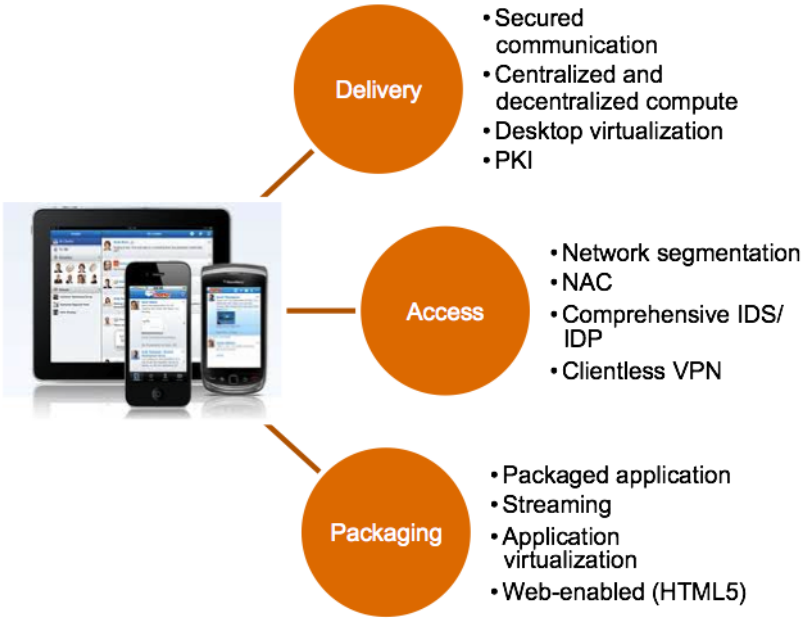
A typical BYOD infrastructure employs desktop virtualization, application virtualization or a security-enriched application development to deliver a secure package to an unsecured platform. This approach, which enables IT to retain security of the package regardless of the device, can represent a vast departure from traditional methods of application and data delivery that transport an unsecured object to a secure platform.

BYOD is typically considered a mobile strategy, but we believe a forward-thinking strategy transcends the tactical approach of securing mobile devices and becomes a comprehensive device-agnostic strategy. A BYOD infrastructure blurs the line between internal and external network access, obviating the need to delineate between the two. All devices are treated with the same rigor, and applications and access to resources are delivered in a consistent manner. That results in a consistent and common infrastructure for support of desktops, laptops, smartphones, tablets or employees' personal computers. An effective BYOD strategy can help you achieve the ultimate operational goal: consolidation of the infrastructure and delivery of data and access using a common, secured methodology

As discussed earlier, a device-agnostic network typically delivers content via technologies such as virtual desktop infrastructure (VDI), application virtualization, virtual appliances, and application streaming across segmented and secured networks. Of these, application virtualization is perhaps the most essential. Application virtualization allows IT to operate more efficiently because the technology precludes the need to install and maintain software at the endpoints over its life cycle. The application resides on a centralized server and is streamed as a single executable file to users, who simply click to use. In other words, the application is "run" from a device without being "installed" on it. Delivery of applications can be Web-based, provided through an app store or via client-based software such as Citrix Receiver or VMware View.

Application virtualization also simplifies use. Employees need only click a link or shortcut to launch the executable file; they can run multiple versions of an application on one device without prior installation and without version or DLL conflicts. For example, an employee can simply click a link in a Web browser to seamlessly run Microsoft Word 2007. Should the employee require Word 2010, the application can be delivered with equal ease and without conflicts.

For the on-the-go worker, virtualization technologies offer offline modes that allow the applications or operating system to be accessible when the device is not connected to the corporate network.



Virtualization addresses aspects of data and application access and leakage, but is not necessarily the frontline security checkpoint for access of the device onto the network. To secure corporate resources, a BYOD infrastructure typically employs existing access solutions such as network access control (NAC) to govern secure access by operating system, application and hardware. When added to a device-agnostic infrastructure, NAC can unify antivirus signatures, baselines requirements, network connection type (VPN or bridged, for instance) and access to application resources. These controls can be applied *before* the device is allowed to connect to the network. Additionally, conditional access can be granted to a subset of resources based on the results of a NAC audit.

One of the core concepts of a BYOD strategy is moving the access controls traditionally found in the desktop into the network layer. By segmenting network resources into silos of service and using firewalls and intrusion detection/prevention solutions to monitor and control communications between these silos, the device's ability to access corporate resources is limited, audited and controlled.

Coupling network segmentation with the data segmentation that can be achieved through desktop and application virtualization grants an organization unprecedented control while freeing IT from the need to directly support devices.

A BYOD strategy should be instituted in a manner and timeframe that fits an organization's unique culture and capabilities. BYOD aims to consolidate the tools, infrastructure, policy and governance regarding the delivery of applications, services and data so that both personal and corporate-supplied devices are interchangeable and supported in the same manner.

A BYOD infrastructure is typically introduced as an opt-in program, which requires the organization to continue to provide traditional provisioning of desktops and laptops. The BYOD strategy requires proper forethought and due diligence for success. It is also best to implement BYOD in a phased approach, which allows for proper and timed investments for long-term operational efficiencies and cost/risk aversion.

Supporting users in a BYOD world

The issue of user support inevitably arises in BYOD discussions – and rightly so. For many CIOs, the notion of supporting a freewheeling mix of consumer devices initially seems dangerously open-ended for IT.

Yet that's not necessarily the case.

In a BYOD model, the need for widespread application support is greatly reduced because virtualized applications can be centralized and therefore standardized across devices. Applications are packaged with little or no integration with the device or the operating system, essentially moving IT functions to application hosting in lieu of device support. When application support is required, it can be provided by a separate group that works tightly with the application delivery teams rather than the traditional general-purpose help desk.

Device support becomes minimal; in fact, it may be limited to verification of baseline requirements such as appropriate computing power, up-to-date browsers and client software that meets infrastructure requirements.

In a device-agnostic infrastructure, the majority of help desk calls will shift from application functionality issues toward assistance in connecting the device to the network. Once the device is attached to the network, remaining issues can be supported from a centralized application position. In this model, applications and infrastructure are delivered to, not installed upon, end-user devices, and the source of troubleshooting will be a centralized set of resources.

Over time, a BYOD infrastructure can enable IT to pare its front line support responsibilities to core network access. Achieving this simplified level of support will not be easy, nor will it be achieved overnight.

Many organizations will grapple with the level of support offered to different types of workers across the enterprise. Tiered support policies may be necessary to define varying levels of support, ranging from limited assistance to full IT support. Policies and delineations for support should be prudently segmented to provide the right level of assistance to ensure employee satisfaction and productivity.

There is no doubt that a BYOD infrastructure will demand new support processes and new skills from IT. It will also change the way support budgets are spent. While cost savings may not be realized immediately, over the long term most organizations that implement smart support policies may see significant operational savings.

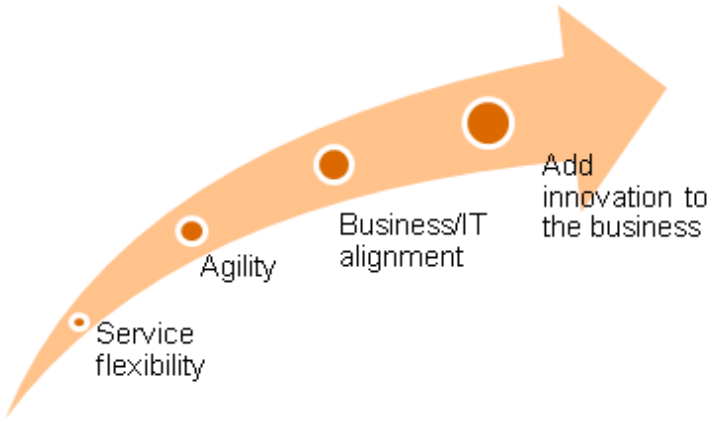
What this means for your business

One thing is certain: Consumer obsession with technology will intensify as manufacturers design and deliver progressively more capable and compelling devices. It is inevitable that employees will bring these products to the workplace or use them to access corporate resources from home.

Among CIOs, denial of this trend is no longer an option.

We believe that CIOs should respond with a forward-thinking BYOD strategy that encourages use of consumer devices in the workplace as a means to drive employee productivity, innovation and retention. This strategy should carefully balance the demands of employees with overall business objectives, using rigorous, informed planning to ensure network and data security.

When crafting a BYOD strategy, CIOs should first determine if the organizational culture and the company's unique operating environment are appropriate for use of employee-owned devices. Each organization will have varying levels of readiness to adopt a device-agnostic operating model.



Assessing the current state of IT services, capabilities, and support structures and aligning possible BYOD requirements can a daunting challenge. Beyond an understanding of current consumer technology, the CIO should spearhead a comprehensive assessment of the people, policies and technology that drive current growth and prepare the business for future expansion. A comprehensive BYOD strategy can strategically align IT and the business, delivering the innovation necessary to thrive in tomorrow's competitive market. Deployment need not be enterprisewide. Instead, we believe that a BYOD strategy is most effective when implemented in a phased approach.

None of this will be easy.

Understanding the confluence of technologies, governance, policies and processes necessary to successfully transition or institute a BYOD infrastructure will very likely test the expertise of most IT organizations, which have long operated in a very structured, inflexible environment.

PwC can help you assess your unique business needs and your IT infrastructure to assist in building a comprehensive device-agnostic strategy and infrastructure. Our expertise in IT infrastructure and strategy, in combination with a mature mobility and risk-management practice, provide a rich source of experience in planning and implementing a BYOD strategy.

Done right, a BYOD strategy can empower users while increasing IT agility and efficiency. But the shift to a device-agnostic environment will be nothing short of a revolution for many IT organizations.

Getting there may not be simple, but for many organizations a BYOD strategy will be essential for driving growth and realizing competitive advantages. We can help you make the move with confidence.

Contacts

To have a deeper conversation regarding the industry or any of the topics mentioned, please contact:

David Edelheit
Principal, New York
david.l.edelheit@us.pwc.com

Dave Stuckey
Principal, New York
david.a.stuckey@us.pwc.com

Jeff Sage
Director
jeff.sage@us.pwc.com

Stephen Singh
Director, Boston
stephen.singh@us.pwc.com

pwc.com