BYOD: COST SAVER NOT CURSE

Make "bring your own device" policies part of a broader mobility strategy that IT can manage and secure, and employees can use to be more productive.

At first blush, bring your own device (BYOD) sounds like a gift for budget-minded organizations.

After all, if employees offer to use their personal computers and communication devices for work that's less money for computer gear coming out of an enterprise's capital expense budget. Employees also get to use their preferred hardware, and some organizations report this can result in overall higher employee morale.

But is it really a bargain? What about the IT department, which will have to manage and secure a wide range of new devices, from notebook PCs and smartphones to tablets and even consumer-oriented iPod touch digital assistants — not to mention the many operating systems and applications trying to access sensitive corporate data?

While the concept presents pros and cons, many high-profile organizations are adopting bring your own device to work policies, allowing workers to use the computing machine of their choice. While such policies may require some changes in corporate strategy, they can result in a number of benefits including increased productivity, lower support costs and enhanced employee morale.

BYOD Benefits

Larger enterprises offering liberal device policies include CARFAX, Kraft Foods and Proctor & Gamble, which offer incentives to induce employees to bring their own mobile devices into the workplace.

CARFAX, for example, gives staff interest-free loans for new computers. Kraft plans to let employees buy their own PCs. And Proctor & Gamble is letting several hundred of its employees use their own notebook PCs in the office.

Even the federal government is jumping on this bandwagon. The Veterans Affairs Department has announced plans to begin letting use of iPhones and iPads on its networks this fall.

And last year, a senior White House technology official floated the idea of the government using stipends as part of larger initiatives to reduce IT costs and help agencies migrate more services to cloud-computing environments.

"While gaining acceptance, there's an increased complexity from managing all those devices and versions of software, and complexity is the enemy of total cost of ownership," says Jack E. Gold, president and principal analyst with the consulting firm J. Gold Associates.

The reality is that many IT managers are under pressure to develop BYOD policies that address these security and complexity issues — and to do so quickly.

"Two years ago, device management meant deploying a line of business applications for the field sales group," says Mark Jordan, senior product manager for mobility at Sybase, which includes mobile management solutions within its software portfolio. "Now, organizations may have to manage 20 or 30 apps each, for several thousand users across different departments."

Mobility experts and veterans of BYOD initiatives say the answer is to understand the business needs of the organization and then devise a plan that balances corporate governance and employee choice.

New Thinking Required

How significant is the BYOD trend? One measure to look at is how workplace smartphones are being provisioned. Forrester Research says employees choose their own smartphones 70 percent of the time, with 48 percent of the devices picked without regard for IT support. That means only 23 percent of the smartphones used at work in the United States are delivered as a take-it-or-leave-it device by IT, the analyst firm says.

The consumerization of IT is upending the control IT departments used to enjoy when they could enforce corporate standards for specific PCs and operating systems. But mobile devices change things because employees routinely use the latest and greatest devices outside of the workplace and can become dissatisfied quickly with a corporate standard if they view it as inferior to their options personally.

What's more, some mobile renegades will deliberately flaunt corporate guidelines. They will bring in rogue devices that IT doesn't even know are on the network — or let alone manage.

A well-crafted BYOD policy can help incorporate employee preferences into a sound management policy. But many enterprises are motivated by more than a desire to quell employee uprisings.

Organizations can see some clear business benefits through creation of a workable BYOD strategy, including reduced capital expenses. For example, Forrester reports that more than half of the nation's workforce now pays for all or some smartphone use at work, picking up the cost of all or a portion of associated data plans.

Citrix Systems has analyzed the financial impact of BYOD since it launched its own internal program three years ago. It now pays 15 percent of its employees a $2,100 stipend to buy and use a notebook of their choice. But along with that, employees must purchase a maintenance contract from the device supplier, which means the Citrix help desk does not support these employee-provisioned devices. And that's where Citrix sees monetary savings.

The company estimates that procurement and support costs for notebooks boost the TCO to about $2,600 for equivalently priced systems it requisitions. The bottom line: BYOD saves Citrix about $500 per device over three years, according to Michael McKiernan, vice president of business technology.

With another 10 percent of the staff participating (even without a stipend), nearly a quarter of Citrix's staff now uses BYOD notebooks. That number is likely to increase as new hires are brought into the program and current participants renew their participation after three years. (Stipend recipients are charged a pro-rated fee if they leave the company sooner.)

Citrix provides a BYOD stipend only for the purchase of a notebook, not other mobile devices. "We ran the numbers for smartphones

SMARTPHONES: THE NEW BUSINESS TOOL

Smartphone users handle

36% of work-related calls and

26% of e-mail on their mobile phones.

Source: Forrester Research

AND THE WINNER IS ...

Before enterprises define the specifics of their BYOD policies, they should look at mobility strategically. This means figuring out which applications can take advantage of the small but powerful computing devices that people now have access to virtually anytime and anywhere.

If the organization needs help identifying the top applications, do what a number of companies and government agencies have done: Sponsor a contest challenging employees to design and develop mobile apps.

"Whoever has the best ideas gets a free tablet," says Sean Ginevan, product manager for Mobile Iron. "Who better than the people with boots on the ground inside the organization to tell you what to mobilize?"

and tablets, and because of discounts we receive, it's not economical," McKiernan says.

Some additional BYOD benefits beyond financial savings are rippling throughout enterprises. A large pharmaceutical company reports the volume of Tier 1 help desk calls is less for employee-owned devices, says Sean Ginevan, product manager for Mobile Iron, which supplies a mobile-device management (MDM) solution to the drug company.

"If this is my phone, and I tweaked it just the way I want it within organizational security bounds, I'm going to be more willing to try and fix it before I call the help desk," he says. "This isn't a corporate laptop where as soon as there's one little hiccup I throw up my hands and say 'IT, this is your device. Figure out how to fix it.' "

Personal responsibility may extend to security practices as well. "There are fewer issues with personal devices than with corporate laptops," McKiernan says. "People better take care of these devices when they own them."

Manageable BYOD

How can the IT department assure that the enterprise sees these benefits instead of watching an unmanageable mobile environment arise to create chaos for the existing IT environment?

"You have to address what end users want in terms of personal choice — but don't start there," Gold says. "Think about what your business needs first, then retrofit the technology that works the best to achieve those goals."

That means seeing BYOD not as an end game. It's one component in a robust mobile strategy that addresses all the areas where mobility makes sense and creates a long-term roadmap for delivering the appropriate applications and services.

"You don't want to do BYOD with a series of short-sighted projects," Jordan advises.

Enterprises also should update their existing mobility policies, which may have been tucked away in three-ring binders or file cabinets since their initial creation a decade ago. "Organizations really need to re-evaluate all these policies in light of the latest technologies and the most recent regulatory issues for information management that apply to their industries," Ginevan recommends.

For security and management ease, BYOD rules should address five core considerations:

- Which workgroups can bring in their own gear?
- Should groups be segmented by job function, organizational unit or region?
- To what data will BYOD devices be granted access?
- What kinds of mobile devices will be allowed?
- What will be allowable minimum capabilities of the devices and operating systems?

Answering the last question will be complicated because security and management capabilities of some hardware and OS combinations are still a work in process, experts say. For example, some Android smartphone manufacturers, including Samsung, Motorola and LG, are customizing the Android OS with proprietary management capabilities, such as enhanced password controls, hardware-based encryption and hardened e-mail security.

These extensions are a security plus for IT managers, but the lack of standardization means the enterprise will need to develop alternative management policies for other Android smartphones that run more basic versions of the OS. But what kind of alternative policies?

For example, IT may decide to force users of the basic OS to access corporate e-mail through a security application. By contrast, the IT department may decide it is safe for devices with proprietary security extensions to connect directly to the corporate e-mail server. Or it may decide that some systems or data are off-limits to all BYOD devices.

For added security, and an absolute necessity for organizations in highly regulated markets, IT shops may want to issue an authentication certificate for each BYOD device. A step up from password security, the certificates confirm that both the users and their individual hardware have been authorized to access the network.

Cool Tools

Fortunately, a variety of tools are available to help IT administrators implement and enforce the BYOD policies they create. Mobile-device management software can act as a kind of command center, letting IT managers centrally configure access authorizations and business applications.

MDM solutions also let the IT department track devices, confirm device security settings, and create virtual private networks (VPNs) that establish protected communications links between uses in the field and the enterprise network. An MDM application can also check that each device is running an updated version of its OS and scan for malware before a user device connects to the corporate network. If the hardware is lost or stolen, IT administrators can go to the MDM command center to wipe the data.

"MDM can push down a variety of settings to individual devices, but just as importantly, it enables IT managers to take all those settings back," Ginevan says. "So when someone leaves the enterprise, I can delete all the corporate e-mails, corporate applications and any security certificates that identify the device to the network."

Because MDM tools can streamline or automate so many basic device-management tasks, IT isn't scrambling to service hundreds or perhaps thousands of individual devices. "That gives IT administrators more time to focus on strategic tasks, such as building and mobilizing applications inside their enterprises," he says.

Role for Desktop Virtualization

Another important mobile-management technology is desktop virtualization, which lets IT create individualized desktop environments tailored for each notebook, smartphone or tablet. With virtualization, staff members use their mobile devices to send screen images and keyboard clicks over wireless networks to applications centrally stored in the backend data center, which also houses all corporate information. Because data doesn't reside on mobile devices, there's less risk of a security breach if portable hardware is hacked or stolen.

For its BYOD strategy, Citrix enhances each device with its own commercial technology, Citrix Receiver. It connects end-user hardware to virtual desktops created by central IT administrators. To protect the messages flowing back and forth between users and data center systems, Citrix establishes VPNs that support data encryption.

McKiernan says members of the Citrix staff that are part of the BYOD program accept client virtualization in part because data and applications stored in a central location makes those resources accessible from any one of the multiple computing devices they may own.

"If the data is stored on a C drive in one computer, they may not always have access to it," he says.

And what about the potential for greater security risks if IT doesn't have complete control over the devices that each person uses? "The rubber hits the road with our results after three years. We have not seen our exposure increase," he says. "If you provide the right incentives for people to protect corporate data, they will. Just because someone chooses to use their own MacBook, they don't suddenly turn into a deviant." ■

IS BYOD WORTH THE RISK?

Consider these five risks when starting a "bring your own device" program:

- **Network security:** Be ready to defend against unauthorized access in addition to controlling uploads and downloads.
- **Device security:** Enterprise protection should extend to each authorized device.
- **Burgeoning support requirements:** Wikis and other passive tools can help your organization manage multiple device platforms without getting buried.
- **Growing costs:** Carefully consider how to implement security protections, additional access portals and wired/wireless infrastructure before jumping in.
- **Compatibility:** Evaluate your network architecture to determine if a range of platforms and OSs can easily and safely connect.

Ask how CDW can help augment your professional technology staff, whether you're looking for permanent, semi-permanent or temporary placements.