DEVICE Du Jour

As the "bring your own device," or BYOD, movement gains momentum in the corporate world, IT organizations rethink their mobile strategies.

When Citrix Systems CEO Mark Templeton met with his CIO to discuss the company's mobile future, he had a vision in mind: Create an environment where personal devices could serve double duty as personal and professional machines.

Thus began Citrix's "Bring You Own" or BYO program for its employees. That was nearly four years ago. At the time, Templeton wanted the IT department to step up its efforts to help employees augment their corporate-issue desktop and notebook PCs with a wide variety of personal mobile computing devices, including netbooks, smartphones and eventually tablet PCs.

The program has been deemed a success, even beyond the original total cost of ownership (TCO) goals, which Citrix did attain, says Michael McKiernan, vice president of business technology at Citrix. "Participants report that their computing experience is better and they feel empowered that their employer trusts their assessment" of the tools they need to do their jobs.

Since the Citrix experiment several years back, many high-profile companies 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.

Citrix Test

The Citrix CEO and CIO weren't interested in some BYO "Kumbaya" technology policy that accepted all types of devices at the expense of corporate management and security policies. Instead, they had clear business goals in mind.

Among them was self-service computing, where employees could mix and match resources to make themselves more productive. The executives also set clear targets for reducing Citrix's TCO for hardware by upwards of 20 percent.

Finally, they sought a showcase for demonstrating how Citrix's own technologies could make other corporate BYOD campaigns possible.

Another benefit of the program has been additional freeing of Citrix's IT department to focus on high-value activities. In addition, McKiernan says the company has even become more secure. This is despite the conventional wisdom that says accepting personal devices inside the firewall can create security vulnerabilities.

"Fewer security issues have been encountered with our BYO devices than corporate devices," McKiernan says. "It's a question of ownership — people typically take better care of their personal assets."

Some organizations acquiesce to the presence of personal devices. Others embrace the idea. Citrix is part of the latter group. Early on, it identified 850 people who would be eligible to receive a three-year, $2,100 stipend to buy personal mobile equipment for the program.

Even without the encouragement of the stipend, an additional 500 Citrix employees gradually started bringing their own devices to work, many doing so on a daily basis. Last year, Citrix expanded their BYO initiative to international workers. Today, 96 percent of all participants say they would recommend a similar program to others, McKiernan says.

BYOD Takes Off

Citrix isn't the only organization that's doing more than just dabbling with strategies to incorporate personal devices into the corporate infrastructure. Reports abound about companies implementing this approach in big ways.

Some large companies in the vanguard included CARFAX, Kraft Foods and Procter & 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 Procter & Gamble is letting several hundred of its employees use their own notebook PCs in the office.

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

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

"There is an overwhelming trend to bring your own device to work," says Paul DeBeasi, research vice president for wireless and mobility at Gartner. "Suffice it to say, I think that BYO is becoming the new normal."

He declines to note any predicted growth rates, adding, "I don't think that I would believe any survey that claims to quantify this trend. It is moving too quickly, and it depends upon who you talk to — end users versus IT folks."

Still, not every organization is embracing the concept. Attitudes about BYOD differ depending on the sensitivity of information mobile workers typically access and whether an organization is heavily regulated or not. For example, regulatory concerns are causing financial services, healthcare and government organizations to move slowly when it comes to adopting BYOD programs, DeBeasi notes.

"BYOD is a business decision," he points out. "A company that decides against BYOD may benefit from an increase in security and regulatory compliance. For those companies that decide in favor of BYOD, they may benefit from increased employee productivity." Each company — perhaps individual units within companies — will need to evaluate business needs against cost factors and security and regulatory demands.

The existing corporate culture and IT infrastructure also will impact these decisions. For example, Citrix found that it needed few changes to its existing IT environment — but only because it had a head start in some areas given its own product base of virtualization tools.

Plus, it already has a virtual private network (VPN) in place to provide secure communications between devices and data centres. And earlier application virtualization efforts stood ready to deliver corporate apps and data to mobile workers.

McKiernan says preventing data breaches was a concern from the start, but the Citrix virtualization implementation was designed to keep corporate data centrally managed in the data centre. A combination of end-user attention to security best practices and corporate security policies also bolstered data protection efforts. In addition, Citrix uses antivirus software and hard-disk encryption technologies.

Step-by-Step Strategies

Other organizations may find themselves having to do more upfront work. This can be especially true when it comes to securing a BYOD environment.

The first requirement is a well-defined policy that identifies which mobile users and devices may access the corporate network and what they will be allowed to view and access >>>>

56%

Users at Citrix Systems who say they have become more productive since being allowed to use personal mobile devices at work

Source: Citrix Systems

once they log on. For example, some organizations may limit employees to e-mail service on their personal devices; others may allow access to internal servers and push out enterprise applications.

Similarly, businesses will need to determine how they will manage highly sensitive data. This includes whether any critical data can be stored on mobile devices. "You probably don't want top secrets and future plans floating around on somebody's mobile device," says Craig Mathias, principal at the mobile consulting firm, Farpoint Group.

Analysts advise organizations to create a cross-functional team of security experts, applications developers, network administrators, end users and business managers to gain consensus on these and other policy questions.

In addition, IT managers may need to roll out some essential technical resources. As Citrix demonstrates, a standard practice for securing mobile environments is to encrypt data when it resides on personal devices or as it's traveling across networks.

Secure VPN tunnels further protect in-transit data. To bolster security even more, data-cleansing applications let IT managers wipe information from devices that end up missing in action. Together, these safeguards lower the risks that lost or stolen hardware will give up corporate secrets or that hackers will intercept messages as they're traversing communication links.

Some organizations are exploring technologies that let IT managers create dual profiles — one for business, another for the user's personal life — on the same device. Desktop virtualization is one way to make that happen.

"We are starting to see some chipsets designed for mobility that support virtualization," Mathias says.

Desktop virtualization treats hardware, operating systems, data and applications as separate components, and that can make it easier to manage data. For example, one form of client virtualization, similar to what Citrix uses, lets business applications and data reside securely on data centre servers. Users see images of the resources on their devices and send keystroke commands to manipulate the information.

Citrix uses its own virtualization technology, the Citrix Receiver, to deliver applications to mobile devices. Other desktop virtualization options create

HOW TO
KEEP TABS ON MOBILE DEVICES

Mobile device management (MDM) applications provide central management consoles that add a layer of security and control to mobile environments.

By using software agents downloaded to mobile devices, MDM applications help authorize whether a device is allowed to tap into the corporate network.

MDM programs can also scan devices for viruses when they log on to the network or download enterprise applications. They can also centrally set up e-mail and other types of business accounts.

In short, "MDM allows you to extend IT services into disconnected worlds," says Mark Jordan, senior product manager for Afaria, an MDM solution from Sybase that supports multiple mobile-computing environments.

For example, Afaria can check to see which version of an operating system an individual device is running to make sure it's current and conforms to the organization's security policies. "So if you're still running an outdated version of an operating system and that's against the security mode, you won't be allowed to access corporate e-mail," Jordan says.

Similarly, Microsoft offers System Center Mobile Device Manager, server-based software that performs management and security services for mobile devices. It complements versions of Microsoft System Center designed to manage notebook systems.

Additional features to consider when evaluating MDM applications include the ability to:

- **See the big picture:** The best MDM consoles provide a central place where IT managers can monitor and manage all devices and applications under their control. This includes downloading software updates to devices while they're in the field or disabling features, such as smartphone cameras, depending on corporate policies.
- **Protect data:** Look for utilities that allow data to be backed up or wiped clean from a device if hardware is reported lost or stolen.
- **Scramble information:** MDM programs should automatically encrypt sensitive data as it is downloaded to devices to assure it stays secure when users roam outside corporate walls.
- **Accommodate growth:** "Bring your own device" initiatives and mobile implementations in general are on a growth trajectory. Make sure a prospective MDM system can scale easily to handle from dozens to thousands of users.

individual work environments with specific business applications targeted for each mobile worker.

Work is ongoing to adapt virtualization to the constraints of mobile screens. But eventually virtualization could offer a standard way to create separate personal and professional environments that let enterprises protect sensitive information and keep malware and other threats from invading the professional workspace.

No matter the tool, the good news is that security isn't an insurmountable obstacle in mobile environments, Mathias says. "Security is always a moving target, and adding a user-owned element to this makes it a bit more complex," he says. "It is certainly possible to be secure enough if you are eternally vigilant. But that's true whether you are mobile or not."

Take Control

IT shops can get some much-needed help in managing all the moving parts of BYOD programs with mobile device management software. Mathias calls this an important component in any long-term mobile plan.

Technological considerations aren't the only factors that contribute to BYOD success. Although "the technology is fairly simple," Citrix's McKiernan advises managers to create a phased implementation plan that also focuses on people and communications.

Companies shouldn't "get bogged down in the hypotheticals of what could happen and whether policy can be used to dictate behavior and 100 percent compliance," he says. "Keeping the program simple and creating an internal portal for 'how-to' questions were influential in creating momentum and resonance at Citrix."

Changing cultural attitudes was also necessary. "The IT department had to accept that BYOD users were better at judging their needs and providing self service," he says. "This program goes against years of work spent standardizing and optimizing the efficiency of enterprise computing offerings."

End users also need to understand that BYOD isn't a do-what-you-please option. The support policies of some organizations exclude devices that aren't authorized or directly managed by the IT department. And although stipends may promote purchases of hardware that straddles professional and personal worlds, corporate largesse has its limits.

"If users value a wide-screen, juiced-up CPU and a bling-bling keyboard, then they must pay for those features," McKiernan says. "Often that means paying more than the company would be willing to pay." ■

BYOD: THE FOUR TRENDS

According to the experts, there are currently four major trends that are encouraging companies to try bring your own device policies. These trends include:

1. **Employee Satisfaction** — Workers, especially younger staff, see the brand of notebook or smartphone as a conspicuous part of their identity or lifestyle. Thus, they get more satisfaction and may be more productive using that particular device.
2. **Technology Advances** — The rise of cloud computing and desktop virtualization means that more devices are compatible in office settings.
3. **Mobile Workers** — Technological advances also enable more workers to work remotely from home or from different locations.
4. **Cost** — Over the past several years, the price of technology has dropped dramatically. Today, dual-core processor notebooks and the Apple iPad start at about $500. And netbooks are often similarly priced to smartphones.