STRATEGIC GUIDE TO

BYOD

(The Bring-Your-Own-Device Phenomenon)

Eight Things CIOs Need to Know

The Legal Challenges

Addressing Mobile Security

BYOD's Hidden Costs

How to Write the Policy

FROM THE EDITORS OF

CIO

BUSINESS TECHNOLOGY LEADERSHIP

Table of Contents

Adapted from articles published at CIO.com

BYOD: Eight Things CIOs Need to Know [page 3]

Security: Secure BYOD at MasterCard? Priceless. [page 9]

Legal Affairs: BYOD Stirs Up Legal Challenges [page 12]

The Hidden Costs of BYOD [page 13]

How to Establish a Solid BYOD Policy [page 16]

BYOD, But Don't Drop It [page 18]

EDITOR'S NOTE

Bring It On

Of course, BYOD doesn't just mean "bring your own device," like a beer at a picnic. It really means employees are allowed to connect devices that they already own (like smartphones and tablets) to the corporate network to get work done.

It may have started with some "digital natives" bringing their iPhones to the office, or, just as likely, with the CEO bringing in the iPad he got as a gift. Either way, CIOs have to determine how to deal with this phenomenon. Whereas CIOs historically have been control freaks—providing the specific devices that could get hooked up to the network—now they have to figure out how to say "Yes, but," as in, "Yes you can hook that thing up, but here are the rules of the road."

Only about one-third of CIOs are actually allowing BYOD at the moment, but is there any doubt this will become even more common in the future? It's time to figure out your policies about who owns and pays for what, and how to make sure corporate data isn't compromised.

This report is intended to help guide you along the way.

Mitch Betts

Editorial

Editor
Mitch Betts
mbetts@cio.com

Contributors
Kim S. Nash
Tom Kaneshige
Jonathan Hassell

Editorial Management
Brian Carlson
Maryfran Johnson
Dan Muse

Image Credits
Scanrail/Fotolia [cover]
iQoncept/Fotolia [page 3]
Zimmytws/Fotolia [page 12]
Atlantis/Fotolia [page 13]
iQoncept/Fotolia [page 17]

BYOD: Eight Things CIOs Need to Know

BYOD, or bring your own device, is more than code for "my CEO bought an iPad." BYOD refers to a strategy for letting employees choose and purchase the devices they want to use to do their jobs—everything from PCs and laptops to smartphones and tablets. The machines belong to the employees, who take them along with them if they leave the company.

CIOs who enact BYOD policies are plowing new ground in the consumerization of IT. They seek to cut costs, perhaps — though whether the policy creates hard savings is debatable — and change the way IT and non-IT staff interact. They also expect to improve the productivity of both the IT staff—newly freed from some support tasks—and colleagues who should require less technical training if they use the same machines at home and at work.

Plus, BYOD can boost morale by acknowledging the growing demand from employees to use

the technology they like over what IT wants to support, says Leslie Jones, CIO of Motorola Solutions, which since 2008 has reimbursed employees for one personal smartphone ad allowed them to use the devices at work. BYOD is a "great acknowledgement of reality," she says.

Some CIOs, however, say BYOD is a nonstarter: an empty idea that saves no money but brings potentially expensive security and control problems to corporate IT. Companies that offer full-fledged BYOD programs are still in the minority. In an exclusive survey of 476 IT leaders, we found that 69 percent don't allow employees to buy their own equipment for work while just 24 percent do.

Yet of the 131 companies that allow BYOD, most only suggest which products employees should use, leaving the decision up to the individuals. Just 22 percent require employees to choose devices from a specific list.

Reining in the BYOD Hype

Today, only one-third of organizations are BYOD-friendly

Do you allow access to your corporate networks via personal laptops, smartphones or tablets?

Yes: 33%
No: 67%

Source: Robert Half Technology survey of 1,400 CIOs, May 2012

Another 38 percent let employees pick any devices they want.

Those intrepid CIOs face complex decisions about technology and policy, as well as challenges measuring the true value of BYOD. No one wants to create a BYOD program larded with rules and overhead; it's supposed to simplify work life, after all. Plus, employees are pushing for freedom of choice as consumer devices outpace corporate ones in features and usability. Your mobile workers are tired of carrying around different machines for work and personal use. Whirlpool, for example, doesn't want employees to feel they are taking a step down the technology ladder when they come to work, compared to the technology they use at home, says Daren Fairfield, a director in global information systems at the $18.4 billion appliance maker.

BYOD, ideally, helps merge an employee's home and work life in a way that corporate IT can manage. But Mike Cunningham, CTO of Kraft Foods, says careful planning and methodical testing are necessary to draw conclusions about what needs to be controlled and what can be set free.

Some rules that already govern the use of corporate technology

The corporate network can become a key means of enforcing security policy.

might translate directly to BYOD programs, such as prohibiting employees from using a device used for work to view notoriously insecure sites featuring gambling or pornography. But BYOD requires other nuanced considerations that go beyond the common sense called for in protecting a work-provided device that is occasionally used outside the office.

1. Don't balk for security's sake.

Squashing the BYOD idea because of security concerns is a knee-jerk reaction, says Doug Caddell, CIO at Foley and Lardner, a law firm where 400 iPads are in use as part of a BYOD program that started in February. "You hear a lot about why you can't do something rather than why you can do something," he says. Caddell has users protect their iPads with passwords, which he sets to time out after so many idle minutes. Generally, attorneys working with sensitive material are required to store documents on company servers, not personal devices, through Citrix or VMware. "Security is not insurmountable," he says.

As personal devices get smarter and better able to store and do more with corporate data, they also become a bigger targget for hackers, says Joe Oleksak, a security assurance and consulting manager at consultancy Plante and Moran. "Smartphones and tablets haven't had antivirus and anti-malware programs installed to protect them. You're seeing a big rush in malware writing to take advantage of that."

The corporate network, however, can become a key means of enforcing security policy. For example, the network can detect which devices are running what antivirus and anti-malware tools and deny access to those that don't comply with the company's standards, Oleksak says.

2. Webify, virtualize and mobilize first.

Security concerns do mean that employees using their own laptops, tablets or smartphones for business should not store data locally. In-house counsel would hyperventilate should intellectual property be exposed when someone's kid grabs mom's laptop to Skype his pals about homework. This sort of threat may be equally possible with a work device that is allowed outside the office. But if a laptop is now viewed as personal property under a BYOD program, users may be tempted to forget company policies designed for security. Companies should be

sure to re-emphasize that certain rules still apply, such as those pertaining to sharing a device.

The most secure solution is to permit access to data only through virtual, mobile or Web-based applications on central servers, on a secure network. Users should then also agree not to store data on their devices. The laptop—or tablet or smartphone or netbook—acts merely as an interface allowing a user to work with corporate information.

That architecture has to be in place before a CIO can consider implementing BYOD, says Whirlpool's Fairfield. Whirlpool is testing BYOD with 200 employees and aims to get at least half the company's users working in a virtual environment, regardless of whether they use their own device or one issued by the company, Fairfield says. Many companies are virtualizing applications anyway, to save on server and device costs, among other reasons. Virtualization makes all the more sense in a BYOD situation, Fairfield says. There is no sense in allowing BYOD without first having set up enterprise applications so they can be easily accessed by mobile devices, he adds. That means creating either Web versions—or at least Web interfaces to back-end systems—or purely mobile applications.

VERBATIM

"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."

Source: PricewaterhouseCoopers, January 2012

3. Get infrastructure in top shape.

Whirlpool's pilot quickly showed Fairfield that data storage capacity needed to be upgraded to handle more data now that information that had been stored locally was being moved to central servers, he says. Connectivity interruptions have also occasionally cropped up. That's a critical concern: If people aren't connected to central applications and data, they can't work. To cope, Whirlpool has asked local telecommunications carriers to prioritize their tower upgrades to improve access. "They're cooperating, but can't go as fast as we'd like them to," he says. "Still, they are doing what they can to make heavy-traffic areas better." As the IT

infrastructure is tweaked, Fairfield plans to roll out BYOD to the rest of the company in waves over the next 18 months.

At Kraft, on the other hand, CTO Cunningham has noticed an improvement in network throughput. Because people in the program log in to the network and use their devices to access virtual applications and data stored centrally, there is far less data flowing out from servers than there is in a client-server setup, he says, making the network faster.

Field managers, salespeople and marketing staff are the first and best candidates for BYOD programs.

4. Decide who does what.

From the start, IT leaders must convey to BYOD participants that they, not IT, are responsible for learning about and caring for their smartphone, tablet or laptop, says Jared Mittleman, CTO at AG Semiconductor, a privately held company that resells machines for building computer chips. And some devices may be harder for IT to hook up to a corporate network than others.

For example, BlackBerrys are among the most commonly used devices at AG and are therefore some of the easiest to support. But Mittleman's boss purchased an iPhone last year. Mittleman OK'd the purchase—wouldn't you?—but explained that accessing corporate applications may be bumpy because IT was inexperienced with iOS. He also stipulated that his boss had to help work through any technical issues. "I'm a BlackBerry guy. I do my best. But you, as the BYOD owner, have to be willing to contribute. That's the deal."

At Foley and Lardner, employees are advised to purchase an extended warranty for their devices. The company also keeps loaners on hand for when personal machines are being repaired. "Attorneys can't be without a computer," Caddell says.

5. Say no sometimes.

While 800 employees participate in the BYOD program at the $49.2 billion Kraft Foods, not everyone can partake. At factories, for example, workers have to use specific computers to control the making of cereal or macaroni, Cunningham says. "We're not going to have someone showing up at plant and plugging [a personal device] into our production line."

Legal and human resources staff who work with sensitive, confidential information will

likely need to use fully loaded, company-issued machines to protect and store that data. Working with a thin client, such as a tablet or netbook, over a network may not be feasible. Generally, it's your remote and mobile staff—the ones more likely to be using mobile devices and laptops now, such as field managers, salespeople and marketing staff—that are the first and best candidates for BYOD programs.

6. Indoctrinate – politely, of course.

Careful training is a must, either one-on-one or in small groups, before anyone connects a personal device to the corporate network. Users eager to fire up their snazzy new machines must first understand the Dos and Don'ts of the BYOD policy, Mittleman says.

Automated training makes it too easy to breeze through and miss critical security considerations. IT staff should look people in the eyes and know that they get it, he says. Oleksak, the security consultant, agrees a passive approach to training puts your company at risk. "Your users are your weakest link," he says. "They have physical control of the device and logical access to corporate data. They are the front lines against attack."

VERBATIM

"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."

Source: PricewaterhouseCoopers, January 2012

Whirlpool is finalizing its policy as it continues its pilot. The document will stipulate that users keep data on servers and not stored on their devices, Fairfield says. However, in cases where a user may leave data on his smartphone, the policy will advise that it be stored in folders separate from personal information. That way, if the phone is lost or stolen or the employee leaves Whirlpool, it can be wiped clean of corporate data remotely, leaving personal data in place. Motorola's policy includes similar provisions.

Another good practice: State that although the device is personal, the employee agrees not to visit sites known for spreading malware, such as pornography and gambling sites, Oleksak says. And iPhone and iPad users must agree not to jail break their devices to install software that hasn't been vetted by Apple, he advises. "That's how intruders gain access." Likewise, users of Android and other devices should

understand that Flash is a common way for hackers to deliver malware, so avoid Flash-heavy sites, he suggests.

After those sessions, though, CIOs expect to do less training than they did historically when introducing new technology. Fairfield expects a more rapid adoption thanks to people working with a smaller number of interfaces. The company now supports 48,000 different desktop computing configurations. The huge variety is caused by employees frequently downloading software from the Internet. "To get that number down to a standard set of virtual applications administered centrally will be a huge performance and productivity improvement," Fairfield says.

7. Decide who pays and how much.

Whirlpool is contemplating offering a reimbursement of a few hundred dollars for a personally purchased device; the company

Secure BYOD at MasterCard? Priceless.

More than a year into its BYOD program, MasterCard Worldwide continuously assesses the security technology and policies that allow 30 percent of its employees worldwide to use their personal iPhones, iPads and Android devices at work. **"Security is a high priority for us,"** says Edgar Aguilar, group executive of infrastructure and operation services at the $6.7 billion credit card company.

Employees can get work email on their devices and merge their personal and business contacts and calendars. "We are giving them access to their own information in a form factor they feel familiar with," Aguilar says.

For participants in the BYOD program, **MasterCard sets strict conditions of use**. Data stored on or transmitted to or from the device is **encrypted**. MasterCard also requires passwords to lock the smartphone or tablet or to get on the corporate network. "It's essentially a **secure container**," Aguilar says.

If the device is lost or stolen, MasterCard can wipe just the corporate information. "It's up to the users to make sure they protect their personal information."

About 2,000 of MasterCard's 6,700 employees worldwide have signed up for BYOD so far, and that number is growing, Aguilar says. "We keep hiring new employees around the world and we see more requests for BYOD."

Aguilar's next step was allowing access to the corporate intranet on personal devices, a feature he enabled early last year. Whatever new applications it deploys, MasterCard, which does business nearly every country, wants to **do it globally**, not favoring any one country over another, he says. That means knowing how **wildly different data privacy rules** affect the use of personal smartphones and tablets. archiving and usage logs in place and tested before opening other applications to the BYOD program, Aguilar says.

Kim S. Nash, CIO magazine, May 2012

Allowing employees to choose the technology they like may also attract new hires.

hasn't finalized the total amount per employee yet. Also being debated is whether it would be a one-time payment or on a refresh cycle of every few years, similar to a traditional PC upgrade cycle. One of Fairfield's concerns is fairness. "Executives can afford it, but for people in our plants who need laptops, to spend a few thousand dollars is a major purchase for them." Fairfield and his team are also considering offering company-issued netbooks that cost just a few hundred dollars but would remain corporate assets.

Foley and Lardner offers reimbursement of up to $3,800 every three years, rather than a stipend, which is considered taxable income for the individual. "All of a sudden you see something on your W-2 and you're not a happy camper," Caddell says. CIOs should confer with the accounting department about how best to administer the funds for BYOD programs, he says.

There is no set allowance at AG Semiconductor. Mittleman or a system administrator reviews each request, checking that RAM, power and pricing are appropriate for the employee's work. Many companies don't offer any technology allowance at all, according to our survey. Of the 131 companies that said they have some form of BYOD program, a skimpy 4 percent cover the entire cost of a personal device and 36 percent said they provide some financial help. But 60 percent of those surveyed have employees pick up the whole tab.

Kraft offers employees a stipend every four years, the amount of which Cunningham declines to specify. He does offer this advice: Have IT track who has gotten how much as part of the procedure for setting up a new employee and decommissioning people who leave Kraft. The goal is to "make it part of what you're already doing, as opposed to spawning a whole new set of activities," he says.

8. You will change company culture.

More than a year into Kraft's BYOD program, Cunningham says he's seen hardware support costs drop, but it's just as important that the arrangement makes people more productive and improves their work-life balance. Allowing employees to choose the technology they like may also attract new hires, he says. "They think, 'I can work with this company, which has no draconian rules.'"

Mittleman has found that people are more engaged with their colleagues in and out of IT. One by-product of freeing

employees to buy and try their own technology is that they may discover productivity tools that the IT department would otherwise overlook. "Everyone's an IT incubator," Mittleman says.

For example, the director of sales recently used a compact mobile router to access an Ethernet network and use it like a wireless network. It's handy in oddly furnished hotel rooms where the desk sits in an inconvenient place. The sales director had to buy a second router after his boss adopted the first. It was a great idea that the IT group wouldn't have had the time to investigate, Mittleman says. "We're constantly working on pushing large initiatives. But if you can find a lot of things that make someone's life 2 or 3 percent better, those add up," he says.

The more cordial give-and-take between IT and non-IT staff at Mittleman's office has resulted in improved software development, he says. Colleagues understand more about what it takes to make IT work well and are more willing to brainstorm ideas and identify functions they want, he says.

BYOD is not just about changing the procurement process. It changes the relationship between IT and the rest of the company, he says, and spreads understanding of how IT works. Supporting a proliferation of devices may increase support costs, he adds, but "it's more than made up for in the willingness of users to work with us."

Kim S. Nash, CIO, September 2011

VERBATIM

"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 the meet the needs of all users whole carefully safeguarding the organization's data according to its business model."

Source: PricewaterhouseCoopers, January 2012

LEGAL AFFAIRS

BYOD Stirs Up Legal Challenges

What happens if the IT staff needs to get some corporate data from an employee's personal iPad and stumbles across child pornography elsewhere on the device? Did the IT team have permission to conduct e-discovery on personal data? Is the team obligated to call law enforcement? Would the finding be admissible in court? Were the employee's privacy rights violated? Was the company's bring-your-own-device (BYOD) policy clear about which parts of the device could be searched?

Welcome to the foggy world of BYOD, where the blending of personal and work lives on a single device opens up a host of legal issues. "It's a slippery slope" that lacks clear legal guidelines, says Ben Tomhave, principal consultant at LockPath, a vendor of governance, risk and compliance software. He's also incoming co-chairman of the American Bar Association's information security committee.

Tomhave offers another scenario: Suppose the employee is terminated and the company remotely wipes his iPad, which **deletes personal data. Is the company culpable?** "You've got to make sure policies and legal agreements clearly articulate the expectation," Tomhave says.

Brian Jackson, an attorney at Fisher and Phillips, a law firm that represents employers, says **the BYOD policy needs to be clear about who owns the device and what information the company can search, view and wipe**. For example, the policy could require employees to back up personal data (such as on a home PC or cloud storage) and then explicitly state that the company will wipe those areas clean if the device is lost or stolen.

If a BYOD dispute goes to court, the company should be able to show that **the "employee walked in with eyes wide open,"** Jackson says, so the employee can't say, "I had no idea they'd erase my baby pictures."

Companies also need a policy for disciplining employees who don't comply with BYOD rules, Jackson says. The discipline might range from ending the employee's participation in the BYOD program to termination.

Tom Kaneshige and Mitch Betts, CIO magazine, July 2012

The Hidden Costs of BYOD

While CIOs might gloat at BYOD's perceived cost savings—no more BlackBerry purchases!—they'd be wrong to do so. Aberdeen Group found that a company with 1,000 mobile devices spends an extra $170,000 per year, on average, when they use a BYOD approach.

"Organizations that simply say BYOD is about productivity and have completely ignored the cost structure are playing with a blank check," says Aberdeen analyst Hyoun Park.

This is a splash of cold water on the hot BYOD trend.

Mobile BYOD was supposed to get CIOs out of the vicious hardware-buying cycle, or at least offset costs.

Case-in-point: Cisco's cost savings from BYOD is in the neighborhood of 17 percent to 22 percent. "We don't pay for it, and our users are happier," Lance Perry, Cisco's vice president of IT, customer strategy and success, told attendees at the Consumerization of IT in the Enterprise Conference and Expo. "Isn't that a beautiful thing?"

But Cisco is the exception, not the rule. BYOD's dirty little secret is that most CIOs aren't seeing cost savings. In fact, mobile BYOD often costs more in the long run than company-owned mobile devices.

So where's the money going? Here are five hidden costs in mobile BYOD.

Hidden Cost: The Monthly Premium Hit

Traditionally, CIOs haven't had much to do with mobile devices. But mobile devices have become strategic lately and thus have fallen into the CIO's purview. This means many CIOs are probably not familiar with a wireless

expense management cost structure, which is extremely complicated.

"They approach BYOD from a limited perspective," Park says.

A company can purchase hundreds or thousands of smartphones and receive a volume-discount rate, including some free replacements. Under a BYOD program, a company doesn't get these benefits. However, this isn't a big deal since employees are paying out of pocket for the hardware anyway.

The problem really comes into play with the wireless service. A company that chooses to own mobile devices can buy services in bulk from a single carrier and increase its discounting power, whereas a consumer signing up for a two-year plan pays a much higher rate.

Aberdeen's research shows that a company seizing a volume-discount rate and optimizing plans for certain employees spends an average of $60-per-month for a smartphone's wireless voice and data services. Whereas the average BYOD reimbursement for a smartphone is $70-per-month.

Hidden Cost: Expense Reports

As mentioned earlier, many CIOs aren't on the wireless management ball. These companies spend an average $80-per-month for a company-owned smartphone, or $10 more than a BYOD smartphone. At first glance, this seems to prove BYOD's cost savings, right? Wrong.

You'll have to tack on the hidden cost of reimbursing BYOD employees. Typically, an employee files a monthly expense report for their wireless bill. A single expense report costs about $18 to process, says Aberdeen. Suddenly, the cost of a BYOD smartphone bill runs around $90 per month.

It should be noted that an employee who files an expense report with multiple expenses, including the wireless bill, will still only cost the company $18 to process. That is, mobile BYOD expense reporting will incur this hidden cost only if the expense report was filed solely because of the wireless bill.

BYOD employees often expense their entire wireless bill rather than itemize it. "There's absolutely no visibility into what's personal and what's corporate," Park says. "Even though companies may say they take care of this by putting in a ceiling or fixed expense amount, it doesn't mean they've optimized the cost structure. It just means employees know how high they can go."

Hidden Cost: Security, Management, Data Loss, Oh My!

When a company buys mobile devices in bulk, it can set up a process to automate deployment and management in a scalable way. In a BYOD scenario, an IT person has to input each

individual device into a system, punching in phone numbers, IMEIs (international mobile equipment identity), and employee information.

Aberdeen doesn't provide a cost to this labor-intensive practice. Nevertheless, "It's a pretty realistic pain-point for a company dealing with BYOD on an ongoing basis," Park says.

Then there's a boatload of security and compliance costs associated with mobile BYOD. Typically, BYOD brings iOS iPhones and iPads into BlackBerry shops. This means CIOs will have to invest in a multi-platform mobile device management solution and other software, maybe even a VPN (virtual private network) layer.

"The cost of compliance—ensuring governance, risk management and compliance—is also more difficult when devices must be chased down individually," Park says.

One can see how BYOD could become a nightmare for CIOs. Avanade, a business technology services firm, which surveyed more than 600 IT decision makers late last year, discovered something rather alarming: More than half of companies reported experiencing a security breach as a result of consumer gadgets.

Hidden Cost: Who's Helping the Help Desk?

Then there's the hidden cost in help desk support.

With BYOD, IT departments are caught between the proverbial rock and hard place: IT doesn't control the actions of the carrier or the devices, yet is still being held responsible to support BYOD employees, even if IT isn't getting additional resources to do so.

The flip side is to unload BYOD support onto employees. The thinking goes, they are on the hook to repair their own personal devices. Got a problem with your iPad? Head to the nearest Apple Genius Bar.

As BYOD becomes more pervasive and mission-critical, this kind of self-service won't hold up. "You don't really have control of the device and data if employees are solely responsible for managing the device," Park says."At that point, the company has abdicated control of some of its assets."

Bottom line: CIOs will have to invest in help desk support for BYOD.

All tallied, BYOD doesn't look pretty from a cost perspective.

A typical mobile BYOD environment costs 33 percent more than a well-managed wireless deployment where the company owns the devices, according to Aberdeen.

"Despite all the talk about BYOD being cheaper, that's not what is actually being deployed," Park says.

Tom Kaneshige, CIO.com, April 2012

How to Establish A Solid BYOD Policy

The number of smartphones in use across the globe will reach 2 billion by the end of 2015, according to many estimates. If you haven't been encouraged to establish a program to allow employee-owned devices to access, at the very least, corporate email, calendar and contact systems, it's a virtual certainty you will be now. (In fact, in many companies, your hand is forced by the C suite, because CEOs and other executives often find tablets and smartphones useful in their frequent travels and meetings.)

This pressure might leave you wondering the keys to developing a BYOD policy and how best to implement it. These seven core ideas should be a part of any good BYOD program. Each idea comes with many important questions to ask yourself, your IT associates and your executive team while developing a BYOD policy.

1. Specify What Devices Are Permitted

It was simple and clear in the old days of BlackBerry services—you used your BlackBerry for work, and that was it. Now there are many device choices, from iOS-based phones and tablets and Android handhelds to Research in Motion's Playbook and many others.

It's important to decide exactly what you mean when you say "bring your own device." Should you really be saying, bring your own iPhone but not your own Android phone? Bring your own iPad but no other phones or tablets? Make it clear to employees who are interested in BYOD which devices you will support—in addition to whatever corporate-issued devices you continue to deploy—and which you won't.

2. Establish a Stringent Security Policy for all Devices

Users tend to resist having passwords or lock screens on their personal devices. They see them as a hurdle to convenient access to the content and functions of their device. However, this is not a valid complaint—there is simply too much sensitive information to which phones connected to your corporate systems have access to allow unfettered swipe-and-go operation of these phones.
If your users want to use their devices with your systems, then they'll have to accept a complex

password attached to their devices at all times. You need a strong, lengthy alphanumeric password, too, not a simple 4-digit numerical PIN. Check with your messaging administrators to see what device security policies you can reliably enforce with your software.

3. Define a Clear Service Policy

It's important for employees to understand the boundaries when questions or problems creep up with personal devices. To set these boundaries, you'll have to answer the following questions.

What level of support will be available for initial connections to your network from personally-owned devices?

What kind of support will IT representatives provide for broken devices?

What about support for applications installed on personal devices?

Will you limit Help Desk to ticketing problems with email, calendaring and other personal information management-type applications?

What if a problem with a specific personal application is preventing access to the apps you have delineated previously that you will support?

Is your support basically a "wipe and reconfigure" operation?

Will you provide loaner devices for employees while their phone or tablet is being serviced?

4. Make It Clear Who Owns What Apps and Data

While it seems logical, on the face of it, that your company owns the personal information stored on the servers that your employees access with their devices, it becomes more problematic when you consider the problem of wiping the device in the event it is lost or confirmed stolen. When you wipe the phone, traditionally all content on the phone is erased, including personal pictures, music and applications that in many cases the individual, not the company, has paid for. Sometimes it's impossible to replace these items.

Does your BYOD policy make it clear that you assert the right to wipe devices brought onto the network under your plan? If so, do you provide guidance on how employees can secure their own content and

back it up so they can restore personal information once the phone or device is replaced?

5. Decide What Apps Will Be Allowed or Banned

This applies to any device that will connect to your environment, whether corporate- or personal-issued. Major considerations typically include applications for social media browsing, replacement email applications and VPNs or other remote-access software.

The question here is whether users can download, install and use an application that presents security or legal risk on devices that have free access to sensitive corporate resources. What if the latest Twitter app has a security hole in its integration with the Mail app on the iPhone that allows spammers to access relay mail through your organization? (This is purely hypothetical, of course.) What if a poorly written instant messaging client steals your organization's address book?

BYOD, But Don't Drop It

Most companies that have a BYOD program require employees to handle repairs on their devices

If an employee's personal device breaks, who is responsible for fixing it?

82%: Employees are responsible for having their devices fixed themselves and for paying for the repair

12%: Employees are responsible for having their devices fixed themselves and our organization pays for the repair

5%: Our organization assumes responsibility for fixing employee-owned devices

2%: Not sure

Source: CIO survey of 131 companies with BYOD programs, August 2011; percentages do not add to 100 due to rounding

These are serious questions to address in your policy, not to mention a starting point for BYOD policy development. Moreover, the technology for preventing downloads of questionable apps or copyright-infringing music and media on personal phones is immature at best, so manual screening of eligible users into a trusted group may be warranted.

6. Integrate Your BYOD Plan With Your Acceptable Use Policy

If your company is on the ball, chances are corporate-issued phones are already covered and treated like notebooks, desktop computers, and other equipment on your network. On the other hand, allowing personal devices to potentially connect to your VPN introduces some doubt about what activities may and may not be permitted. Discussions about an acceptable

use policy are required to fully cover your rear.

If you set up a VPN tunnel on an iPhone and then your employees post to Facebook, is this a violation?

What if your employees browse objectionable websites while on their device's VPN?

What if they transmit, inadvertently or not, inappropriate material over your network, even though they're using a device they own personally? What sanctions are there for such activity?

What monitoring strategies and tools are available to enforce such policies?

What rights do you have to set up rules in this arena?

7. Set Up an Employee Exit Strategy

Don't forget about what will happen when employees with devices on your BYOD platform leave the company. How do you enforce the removal of access tokens, e-mail access, data and other proprietary applications and information?

It's not as simple as having the employee return the corporate-issued phone. In this case, many companies choose to rely on disabling email or synchronization access as part of the exit interview and HR checklists, while more security-conscious companies choose to perform a wipe of the BYOD-enabled device as a mandatory exit strategy.

Have a clear methodology for backing up the user's personal photos and personally-purchased applications prior to this "exit wipe."

You should have a clear methodology for backing up the user's personal photos and personally-purchased applications prior to this "exit wipe.

Proactively reach out to affected users to help them take part in this process—all while making it clear that you reserve the right to issue a wipe command if the employee hasn't made alternate arrangement with your IT department prior to his or her exit time.

Jonathan Hassell, CIO.com, May 2012