

# Employee-owned Smartphones: Seize the Opportunity

As more employees desire to use their personal smartphones for work, IT managers must leverage the opportunity, or risk their organizations missing out on an emerging business trend.



**Consider this scenario:** An employee is at his son's soccer practice, which is dragging on much longer than he thought it would. If he could access his work email on his new smartphone, he thinks to himself, he could track those projects he's been working on. So why won't IT let him have access to the corporate network?

In increasing numbers, employees are clamoring to use personal smartphones for work-related duties. According to IDC, employee-owned smartphones will represent more than half (56%) of the business smartphones shipped in 2013, for a total of 56.7 million devices going into the hands of individual workers in the next three years.

It's no longer feasible for an IT department, regardless of company size, to ignore the smartphone push from the majority of the employee population. IT management must attempt to channel the chaos and determine ways to embrace the personal mobility wave while maintaining effective security and management measures, especially in relation to the corporate network.

## 64% of IT organizations say that maintaining the appropriate level of security for mobile devices/mobile data is their highest priority.

SOURCE: survey by CIO and Computerworld

This new environment calls for innovative mobile strategies, new policies, and a fresh approach to allowing smartphones access to corporate resources. IT management must take a leadership role in setting those strategies and policies.

### The Consumerization of IT

Until recently, smartphones were something of a corporate status symbol. Organizations provided them for a small, but increasing, percentage of the corporate population, and supported the voice/data plans of those devices directly through what was known generally as corporate-liable smartphone policies.

While expensive, the efficiency gains of mobile access to email and company information paid back in months, if not days. In addition, these policies enabled organizations to impose strict limitations and stringent controls. They limited not only who had access to corporate resources, but also how those resources were accessed: what devices could be used, including which features on those devices were enabled and which disabled. IT provided users with secure network connections and controlled the devices using sophisticated management systems.

However, smartphones have undergone the same transformation as other electronic devices, dropping in price and adding sophisticated features while promoting a tech-culture sizzle that makes them appealing to the majority of Internet-surfing, text-messaging, GPS tracking consumers. According to research firm Gartner, 172 million smartphones were sold last year.

And increasingly, employees want to use their bought-and-paid-for personal smartphones in the business context. Some want to use their smartphones for simple work-related tasks, such as checking email or calendar appointments. Others want to access corporate resources, like customer-related data. Also, some of those with

corporate-supplied smartphones are balking at the clumsiness of having to lug around two separate devices, one for work and the other for personal interactions.

The fact is, there's no stopping the employee-owned smartphone trend and its overlap with the work environment. Consulting firm Yankee Group says 54% of employees already use their own mobile devices for business purposes, whether sanctioned by their organizations or not. IT executives must craft a mobile strategy that incorporates employee-owned smartphones and accommodates these workers as they embrace extended mobile responsibilities, or the workers will figure out a way to do it for themselves.

### Ownership Rules

There are several good reasons why organizations should open up their mobile strategies to incorporate employee-owned smartphones.

- 1. CONTROL COST.** Having employees take over the expense of their smartphones, both the initial cost of the devices and their ongoing voice/data contracts, benefits both sides of the equation. By being more efficient and effective at work, an employee can leverage an expense that he or she would be making anyway. And the employer saves the significant cost of an ongoing budget commitment to an ever-expanding circle of corporate-liable smartphones.
- 2. EMBRACE TECHNOLOGY ENTHUSIASM.** The second good reason for organizations to open up their smartphone agendas is to capitalize on employees' enthusiasm for the technology. That enthusiasm translates into commitment that will help make an organization's mobility strategy a success.
- 3. MULTIPLY THE BENEFITS OF MOBILITY.** The benefits that come with a mobile workforce—real-time communication, faster decision making, extended data access—multiply as the connections proliferate. And controlling costs while proliferating productivity technology across the enterprise makes for a strong return-on-investment argument.

Cost is a factor almost everyone understands. Ira Levy is chief performance officer and chief information officer for Maryland's Howard County. The county recently switched from a "corporate-liable" smartphone policy for a designated group of county employees to a more inclusive employee-owned smartphone policy. The primary reason for the change, says Levy, is that the county went through

a “very challenging budget time period” and needed to cut expenses. The smartphone strategy switch was part of that budget downsizing.

Employees “embraced” the new agenda because they understood the circumstances. “We did a lot of education on budget savings and why it was important,” Levy says. The reasoning was effective, especially when it was laid out in terms of “fewer furloughs” and not having to “go down a more drastic budget-cutting path,” he says.

That does not mean Howard County doesn’t support its smartphone users. The county provides the 600-or-so employees who have smartphones hooked into the

Howard County’s didn’t wait. The county’s official smartphone policy was made available in March, at the same time the changeover was taking effect, but had been in the works for a while. “We had been working on the policy for months,” Levy says. After the policy was made available, county officials made sure employees were aware of the changes. “We held internal town-hall meetings in different facilities where employees could ask questions, go over parts of the new policy, what [platforms] we support and what we can’t support.”

Since smartphones first entered the enterprise environment, the priority for IT has been pretty straightforward

**Employee-owned smartphones will represent more than half (56%) of the business smartphones shipped in 2013, for a total of 56.7 million devices going into the hands of individual workers in the next three years.** SOURCE: IDC

organizational network with stipends that range from \$15 to \$105 a month, depending on their use of the technology and their place in the organization. That’s a smart move. By offering a stipend to employees who use their bought-and-paid-for personal smartphones for work, organizations still can save a considerable amount of money over expanding corporate-liable policies while engendering loyalty and favor among their workers.

## Inclusive vs. Exclusive

When it comes to organizations opening up their smartphone strategies, given the rapidly expanding market for such devices and the explosion in models, a fair question to ask might be: How inclusive is inclusive? In other words, should IT management allow any and all smartphone devices and platforms onto corporate networks?

It may be a fair question but it’s backward logic, according to mobile strategy experts. That’s because an organization’s choice of smartphone platforms—which to support and which not to—should be dictated by the mobile strategy and policies already in place, not the other way around. IT management should take their cues from corporate mobile strategy and policy guidelines. Unfortunately, too many organizations are leaving smartphone strategy and policy decision making until after the demand from employees is threatening to overwhelm them.

regarding mobility and mobile strategy. According to a recent survey by *CIO* and *Computerworld*, almost two-thirds of IT organizations (64%) say that maintaining the appropriate level of security for mobile devices/mobile data is their highest priority (and biggest worry) in the mobile environment.

Because of the ad hoc, bottom-up nature of employee-owned smartphones, appropriate security and manageability are even more critical in this new inclusive mobile environment. What is needed is a way to add employees to the corporate network easily and cost-effectively while maintaining the most important security measures and management capabilities that an exclusive corporate-liable strategy would provide

Only a limited number of smartphone platforms offer that type of management control. Research In Motion’s (RIM’s) BlackBerry Enterprise Server is the gold standard among organizations with corporate-liable policies. BlackBerry Enterprise Server provides sophisticated security, management and application development capabilities to support the use of BlackBerry smartphones in the enterprise environment.

Responding to the demands of the employee-owned smartphone imperative, RIM recently introduced BlackBerry Enterprise Server Express, a free version of its enterprise-level management system. BlackBerry Enterprise Server

Express maintains the same encryption and many of the advanced security features of BlackBerry Enterprise Server, allowing for comprehensive yet simple management of BlackBerry smartphones. Some of the management functions IT admins can perform include setting and resetting passwords, deploying and managing applications over the air, locking and wiping devices, and updating device software wirelessly. And because it's free, BlackBerry Enterprise Server Express allows organizations to exploit their employees' use of those smartphones cost-effectively.

For example, employees who express a desire to use their personal smartphones for work-related duties must ascribe to corporate mobile security policies that include, at a minimum, password protection, but also likely encryption, remote lock and data removal, and auditing controls. The security features of BlackBerry Enterprise Server Express include password, encryption and remote-wipe capability, and its management controls delineate limited access to corporate applications and data.

## More than a Smartphone

When is a phone more than a phone? IT management must make employees aware that when a smartphone is added to the corporate network, it transforms into more than a simple telephone or text-messaging machine.

"It's more than just a smartphone," says Roger Beharry Lall, senior manager, strategic insights, at RIM. Unfortunately, many employees pushing to have their smartphones "corporatized" are downplaying or ignoring the complex implications that stem from adding a new device to the enterprise IT architecture. "People have forgotten about the complexity," Lall says.

That's why IT management must delineate for employees, as part of a comprehensive employee-owned smartphone mobility policy, all the implications and outcomes of allowing their devices to interact with company resources on the corporate network. These include the following:

**DATA OWNERSHIP:** Who owns the data on an employee-owned smartphone—all the data, including personal contact lists and calendar entries, family photos and vacation video? Employees with smartphones connected to the corporate network must be aware that if their devices are reported misplaced or stolen, even if they're recovered later, all data could be deleted from them, including personal data. The same goes when an employee leaves the organization, no matter what the circumstances.

**APPLICATION ACCESS:** Management controls will limit the applications and network resources that employ-

ees using their personal smartphones can access. Also, controls may limit the Web sites users can access on their bought-and-paid-for phones, such as gaming sites.

**MULTIMEDIA CAPABILITIES:** For security reasons, some organizations block certain smartphone features, such as cameras and video capability. Also, some organizations limit the use of smartphones as detachable digital storage devices.

**REIMBURSEMENT:** How, and how much, will employee-owned smartphone users be reimbursed for corporate use of their personal devices?

**IT SUPPORT:** What level of support will IT be obligated to provide to employee-owned smartphone users—Tier 1 (help desk)? Tier 2 (service desk)?

There are legal implications to an inclusive smartphone strategy that suggest IT management might want to consult with corporate legal counsel. For instance, hourly workers who email with managers after work hours may be able to claim overtime benefits. A clear policy must be in place that delineates work-related functions and their proper execution, including appropriate work hours.

Be strict, but not too strict. It's important to be consistent, so that if you limit the Web sites corporate-liable smartphone users can access, the same should be true for employee-owned smartphone users. But is this limitation really necessary? Or is it a holdover from an antiquated Internet policy?

## A Leadership Role

Incorporating smartphones into the business environment is not an either/or proposition between a stringent corporate-liable strategy and an inclusive employee-owned smartphone strategy. Some organizations, particularly large ones, will benefit from a hybrid model, where a large percentage of workers access email and limited data on their employee-owned smartphones, while a smaller set of executives or specialists has deep access to corporate resources over company-owned smartphones controlled by a strict management system.

The most important point is to be proactive and plan ahead. "IT has the potential for a leadership role in all of this," says Mark Keating, director of platform marketing for RIM. Unfortunately, Keating says, IT managers have a "limited time to get ahead of the curve before they are inundated by demand they're not prepared for."

