BlackBerry

WHITE PAPER

Smart Policies for Personal-Liable Smartphones

When an individual's device selection matches corporate control, policy and security needs, business benefits abound

With sleek designs and a variety of user-friendly features, smartphones have implanted themselves on the public's consciousness—so much so that one leading industry research firm reports that a record 54.5 million such mobile devices were shipped in the fourth quarter last year. With sales rising nearly 40 percent over the same quarter in 2008, the message is clear: **Smartphones are hot, and not just for mobile workers.**

Indeed, consumers have latched on to the smartphone concept. In the third quarter of 2009, for example, about half of BlackBerry® smartphones shipped to consumers. Take a look next time you're going about your weekend activities. Chances are your neighbor, bridge partner or child's soccer coach has swapped out his or her plain old cell phone for a snazzy, sophisticated new smartphone.

From one little handheld device, a smartphone user can zip off an instant message, check e-mail, update a calendar, zero in on a meeting spot using a GPS locator and, of course, make a phone call. Whether these users are consumers going about their daily lives with the help of a fun

CIO
Custom Solutions Group

gadget or mobile employees communicating, collaborating and otherwise enhancing their workdays with a business-productivity tool is of little consequence—except for those safeguarding the enterprise.

Traditionally, enterprise IT has frowned on the use of company-issued smartphones for personal purposes; likewise, it has prohibited the use of personal smartphones on the corporate network. It's a best practice that addresses security concerns and that is widely advocated by CIOs and mobile-computing experts. But smartphone-wielding users have starting pushing back, wanting a single device to handle both the personal and professional aspects of their lives.

security mechanisms including user authentication, data encryption and remote data removal. IT doesn't provide smartphones to deskbound or other employees who do not need to be able to make calls or send e-mails at will, just as it doesn't dole out laptop computers to anyone who asks.

Few organizations allow employees to use their own smartphones on the corporate network. The concern is that these devices—for which the employees, as the owners, hold personal liability—introduce too great a corporate risk. Fundamental security has been the issue, says Craig Mathias, founder of the Farpoint Group, an advisory firm that specializes in wireless communications and mobile

> "You need to treat a smartphone as an endpoint on the network."
>
> —MARK KEATING, DIRECTOR OF PLATFORM MARKETING, RESEARCH IN MOTION

The situation harkens to the early days of the personal digital assistant (PDA), says Roger Beharry Lall, senior manager, Strategic Insights, Business Marketing, at Research In Motion (RIM)—but with one significant difference. "We can look at that classic anecdote that showed that 80 percent of Palm Pilots were used for business but 100 percent were bought through the retail channel," he says. "But PDAs were mainly stand-alone devices, not interacting with the network, and were relatively harmless. Fast forward to today, and smartphones really are part of an enterprise's mission-critical story."

Business Smartphones in a Social World

Within the enterprise, IT organizations typically assign smartphones to mobile employees who need access to voice and data services as well as business applications. IT assumes corporate liability for the smartphones, as the company is responsible for paying the initial and upkeep costs, enabling applications, and securing and managing the devices.

IT establishes secure connections (via a virtual private network or other mobile middleware) for those employees, and deploys a back-end mobile device management system, such as the BlackBerry platform, that allows IT to control smartphone features and functionality while also ensuring

computing. Imagine, for example, the exposure a company might suffer should a non-secured smartphone or its removable memory card with sensitive corporate data be lost or stolen. Likewise, consider the outcome if corporate data are manipulated by a malicious intruder who has gained access to the company network via a weakly authenticated smartphone.

Data ownership and uncontrolled application use are other sticking points. These come up whether IT is considering allowing personal-liable use of a smartphone or sanctioning the personal use of a corporate-liable smartphone. One of the last things any CIO wants to discover is that a departing employee's personal smartphone contains contact information for the company's premier customers—and that the data can't be wiped from that device. Or that an employee using a corporate-owned smartphone for personal purposes has lost the device, which also happens to host content that counters corporate guidelines.

In the face of such possibilities, a "just say no" policy has been the responsible choice. But the growing popularity of smartphones and an increasingly demanding employee population now make such stringency a bit trickier.

"What we're saying is, 'Everybody has a personal phone. Does everybody really need a corporate phone too?' The answer is, there don't seem to be any hard and fast restrictions that need to be in place any longer," Mathias says.

Alternatives to a Corporate-Liable Approach

Admittedly, Mathias says, such thinking required him to do a 180-degree turnaround. He encourages CIOs to do the same. Personal-liable smartphone use is possible with the right policies and technologies, he says. And, given the market momentum, the time to implement those policies and technologies is now.

Mark Keating, director of Platform Marketing for RIM, agrees that CIOs would be well served by easing restrictions on smartphone use.

Rest assured, Keating says, IT executives are not ignoring the significance of the smartphone's socialization on its enterprise use. But nor are they rushing headlong into a complete strategy change from corporate- to personal-liable smartphone use.

"Increasingly, in the conversations I have, customers tell me they know that 'just say no' policies will only last so long and that frustrated users will try to find a way around the controls," he says. "They know they have to put their arms around this, embrace it, and figure out how to do so in a controlled fashion that makes everybody happy."

Staving off a smartphone uprising at Freeth Cartwright LLP, one of the U.K.'s leading regional law firms, has been a matter of airing out usage rules a bit, says IT manager Chris Nicholson. The firm has standardized on BlackBerry smartphones, used by approximately 160 employees primarily for phone calls, e-mail, calendar functions and digital dictation.

"At present we don't allow non-BlackBerry devices on the network. The same applies for personal BlackBerrys," Nicholson says.

However, Nicholson does allow the staff to use a company SIM card in a personal BlackBerry device and attaching to the network. "That way, using the BlackBerry Enterprise Server, we get control over the handset and can set security policy while letting them link to their mailboxes within the firm and make phone calls," he explains.

It's a nice perk: "If employees put our SIM card in their phones, those become part of the corporate bill," Nicholson adds.

Freeth Cartwright can use the policy to fend off different connectivity requests as well. "A lot of people are using the BlackBerry as their only phone. If I say, 'You can't use that for work calls,' that may bring in a whole problem about allowing access to other personal mobiles," he adds.

Of course, the firm doesn't allow employees to use their corporate-enabled personal BlackBerry smartphones sporadically. Nicholson says that the firm doesn't restrict access but does monitor usage and is able to apply security policies where necessary.

Smart Policies for Personal-Liable Smartphones

Indeed, any IT executive considering alternatives to a 100 percent corporate-liable strategy need strong, enforceable acceptable-use policies, Mathias says. "You need a policy that says, 'Hey, if you want to use your personal smartphone on our corporate network, here are the rules: You'll observe security policy, you won't do these certain things that will compromise network integrity or capability, and, in many cases, you'll allow this software agent or applet to reside on your phone so we can control the enterprise data on it,'" he says.

In other words, Keating adds, "you need to treat a smartphone as an endpoint on the network."

As they weigh smartphone options, CIOs must at least consider the ability to do the following:

- Establish and enforce passwords.
- Encrypt data on the device.
- Remotely lock down and wipe a device clean of data. (Depending on the device, this might mean taking the personal with the enterprise.)
- Control network access.
- Allow or disallow application use, including corporate-mandated programs for filing expense reports and such.
- Control interactivity with Bluetooth, Wi-Fi and other wireless systems.
- Restrict use of the smartphone as a USB flash drive.
- Restrict use of a media card on the device.
- Enable compliance mechanisms, such as audit logs.
- Assure high availability.

Keating advises CIOs to pick and choose among that list to establish the right level of security for their needs and to match the decisions they've made for other corporate-liable devices.

He sees two primary organizational challenges: being able to enforce the policy via technology, and establishing clear roles and responsibilities for each party. For the former, that's where a platform such as BlackBerry® Enterprise Server and BlackBerry® Enterprise Server Express

fits in, giving IT control over smartphones, in this case BlackBerry devices. For the latter, CIOs must engage the legal department in the front-end, personal-liable process.

"End users must clearly understand that when they agree to allow their personal devices to connect to the corporate network, they're also agreeing to certain restrictions and controls on it that will be imposed by the company, and that may impede the use of that personal device as they'd like," Keating says. "That's the quid pro quo of connectivity."

A stringent acceptable-use policy, plus technology controls, accompanies Howard County, Maryland's recent decision to allow employees to use personal-liable smartphones and other handheld devices for work, says Ira Levy, director of technology and communication. Howard County is particularly careful, he adds. "We require through our policy that we have control over the data so that if there's a reason to wipe something clean, lock it out or apply our policies, we can do that," Levy says. Howard County has 350 BlackBerry device users, the majority of whom have stayed with those devices since the county switched to the personal-liable plan.

The tricky part comes once you start evaluating smartphone options against your required controls. "That's the real problem right now," Mathias says. "You have so many different platforms out there today and different implementation of those platforms, that it's kind of hard to say we're going to support any arbitrary phone. We'll get to that point eventually, but it'll take a while. So, for right now, you'll end up saying, 'There's a certain restricted set of phones that we'll be supporting and that will include the BlackBerry® and possibly others."

In Howard County's case, use of the BlackBerry Enterprise Server as well as Microsoft Exchange Server's ActiveSync functionality of other non-BlackBerry devices, ensures IT control of the personal-liable smartphones, Levy says.

Benefiting from Personal-Liable Smartphones

No doubt, with strong policies in place and smart use of technology, enterprises can benefit from adopting a personal-liable smartphone strategy. Improved employee relations and increased productivity are two advantages; cost control is another. Enterprises spend a good chunk of the IT budget on smartphone costs, considering capital and operational expenses, Mathias says. Plus, they have to contend with a variety of accounting and tax issues relative to corporate-liable smartphones.

With personal-liable smartphones comes the ability to offset some of those costs. For example, some firms (like Freeth Cartwright) ask employees to pay for their personal smartphones while the firm covers the expenses. In other cases, the company picks up the cost of the phone but has the employees pay for service. Other options include having the employee pay for both the device and the services used or providing allowances or stipends to defray some of the user costs.

> "You need a policy that says, 'Hey, if you want to use your personal smartphone on our corporate network, here are the rules.'"
>
> —CRAIG MATHIAS, FOUNDER, FARPOINT GROUP

Regardless of approach, "it's clear there will be some significant cost savings that come with this model," Mathias says. For example, in Howard County, Levy expects the new personal-liable device policy to save between $350,000 and $500,000 annually.

No doubt, Keating adds, "personal-liable presents a great opportunity for companies."

BlackBerry

CIO Custom Solutions Group