InformationWeek
:: analytics

By Grant Moerschel

4 Ways To Lower Mobility Risk

Employees want their own phones, and managers want them using apps for productivity. Your problem: Secure all this.

Look around, and you'll likely agree that end-user computing is taking its most radical turn since, well, the introduction of end-user computing.

Smartphones and now the iPad and tablet computers (which create similar challenges for mobile security) are growing like mad. To put some numbers on that growth: Smartphones accounted for 46% of global mobile phone revenue in the second quarter of last year, Infonetics research finds. It estimates that two out of three mobile subscribers in developed countries will use smartphones by 2014.

Mass-market smartphone ownership is creating new expectations from employees. Apple's and Google's offerings trump the BlackBerry platform, the enterprise standard, because people think they can be both serious (for business) and fun (for me).

2010 also brought the first truly practical hyper-mobile computer—something larger than a smartphone but smaller than a PC. The iPad and its tablet followers have obvious appeal to people, many of whom are wondering if they can replace their work computer some of the time, feeding those work-anywhere, play-anywhere fantasies. This month's Consumer Electronics Show illustrates the tablet frenzy Apple ignited with its wildly successful iPad, introduced only a year ago. New tablets are promised from Motorola, Research In Motion, Samsung, Dell, and even newcomers such as TV maker Vizio. Verizon has had the iPad on its network, and now has the iPhone 4 as well.

So the competition for mobile hearts and minds and pinch-and-tap fingers is in full swing, which means your employees will be showing up with more and more new devices. Employees want access to corporate resources and data via these new devices, many of which they personally own. Of utmost concern to any compliance-minded CIO should be: Are these new computing methods putting my data at risk? The answer is likely "yes" if you're leaving device settings up to the users. As we'll discuss, the risks of both smartphones and tablets can be managed in much the same way; it's just a matter of defining your requirements, picking a capable management product, and moving forward. We'll offer four frameworks for managing the risks of these mobile devices.

But first some important context. The megatrend is a shift beyond simple e-mail on these mobile devices. First driven by the iPhone, and now by the iPad, apps are the new frontier, with enterprise examples that include CRM, virtual desktop access (check out VMware's VDI infrastructure), and specialty apps.

Apps fall into two big categories, says Ojas Rege, CEO of mobile device management (MDM) vendor MobileIron. They're either task-oriented with broad

4 Mobile Security Strategies

>> Basic device management Use Microsoft Activesync for simple policy management.

>> Enhanced device management Use mobile device management software for more sophisticated control of company-issued devices.

>> Walled garden Allow corporate access from personal devices, but wall it off from the device's personal content.

>> Risk based management Set policies that restrict corporate access of phones with high risk factors, like unauthorized apps or out-of-date policies.

appeal, such as those for time sheets, expense reports, and conference room scheduling; or they're specialty apps for a niche audience. Some of those specialty apps are custom-coded for a company's specific business processes.

For example, Customedialabs, an interactive media agency, produces a digital sales app for the medical device and diagnostics industry. Using a client app that regularly syncs with a back-end data repository, the mobile app helps clients cover sales territories using CRM components, while trying to ensure that reps show prospects only the latest medical information. This cuts the risk of providing out-of-date material, a violation of stringent FDA Part 11 rules.

It's just one example of how, with apps, we've left the safe confines of e-mail far behind.

Their Phone, Your Problem

Another problem for the CIO is who owns the device. It's possible for companies, particularly highly regulated and deep-pocketed ones, to insist that employees use only company-issued smartphones by issuing only authorized and tested BlackBerry models backed by the trusted BlackBerry Enterprise Server.

However, taking that approach hasn't kept employees who don't qualify for a BlackBerry—and even those who do—from knocking on IT's door brandishing their own shiny iPhone or Droid device and saying, "I want to use this to access the company's network." And who's to argue, really, if an employee is asking to be more available and more productive? Look for companies to continue migrating away from issuing standard smartphones. Instead, they'll provide smart management of enterprise data that's housed within personally owned mobile devices, regardless of platform.

Again, the compliance-minded CIO who allows the use of personal devices for business purposes must have a plan to mitigate the risks of sensitive company data, from personally identifiable customer data to proprietary technical information, being disclosed. This holds for any mobile device that's permitted access—whether to e-mail, a VPN connection to the internal network, access to an internal app or Web app, or access to remote desktop servers.

There's a big sticking point, though, in providing security for personal devices accessing work information. The amount of control you exert may cause problems. If, for example, you enforce a device wipe policy after 10 failed authentication attempts, and someone's 9-year-old tries to guess her dad's password 11 times, guess what? That phone or tablet just got wiped. So when evaluating mobile device management, we recommend flexible policies that safeguard enterprise data while not necessarily affecting personal data.

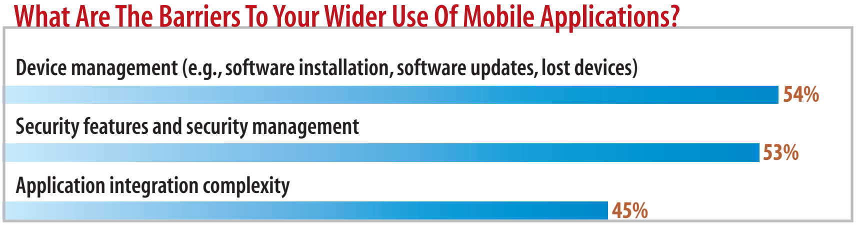
This is an entirely different story if it involves company-owned devices, where you can be as draconian as you want to be. Below, we offer four broad strategies CIOs can use to build a mobile device security strategy, covering basic device management, enhanced device management, walled garden, and risk-based management.

Approaches For Lowering Risk

Basic device management includes rudimentary security such as device wipe, lock, and authentication policies. You can push basic policy settings through Microsoft's ActiveSync, the most ubiquitous one-stop shop for basic control. But if you want enhanced control options, you need to pick a mobile device management vendor that supports all the popular platforms. Enhanced options vary widely depending on the MDM vendor and the platforms you intend to control, but all offer finer device control settings than one gets with the platform basics.

A third option can be described as a walled-garden approach, which builds a hard barrier between personal data and enterprise data. Veteran MDM provider Good Technology does exactly that, for such security-conscious organizations as the U.S. Army. If a company uses Good's software, anytime an employee interacts with the corporate system, it runs through Good's FIPS 140-2 encrypted applica-

What Are The Barriers To Your Wider Use Of Mobile Applications?



Data: *InformationWeek Analytics* Application Mobilization Survey of 563 business technology professionals deploying or planning to deploy mobile applications on smartphones, August 2010 tion container, explains Dimitri Volkmann, Good's product management VP. With a similar look and feel across mobile platforms, the walled garden for business data includes corporate e-mail, calendar, and contacts, with other capabilities in development. Users enter the container that is "owned" by the enterprise, leaving all other device functions personal. Should the company decide to revoke container access, IT can flag the container for deletion next time it connects. Problem solved.

It's the fourth option, however, that is most interesting: risk-based device management. A strict device lockdown policy doesn't work as well on smartphones and tablets as it does on laptops because people expect a certain amount of freedom to use the phone or tablet as it was intended, MobileIron's Rege says. Instead, IT should monitor device risk levels—if the device is jailbroken, unauthorized apps are installed, policies are out of date, or data protection is disabled. The consequence: Enterprise data access is limited or revoked.

MobileIron's risk determination system can look at whether the hardware itself meets certain cryptographic standards. For example, iPhone 3G units aren't encrypted at the hardware level, whereas 3GS and newer version are. Knowing whether devices are encrypted could be important because, if not, data cached on the phone could be disclosed if a phone is lost and falls into the wrong hands.

This risk-based approach interests us more than the walled garden one in part because of the rise of customized and specialty apps. The risk-based approach doesn't change how the phone operates, and it permits the installation of specialty apps, whether they're generally available or available only from an enterprise's own private app store. Being able to allow app installation is highly valuable if you have custom apps, since they don't need to integrate with the walled garden. Also, if a user exceeds the device risk standard by changing a setting, the custom app can be prevented from working until the user reverses the change.

Most of the mobile device management approaches rely on centralized policy. The risk-based approach is no different. Authorized devices receive a software agent that communicates periodically with its management system. The policies defined centrally are implemented at the device via the agent. Therefore, it's the agent determining whether access to the enterprise data will be permitted if the user has made a change.

Real-World Risk Scenarios

Here are a few operational scenarios for a risk-based system. Let's assume that your company maintains two device groups, employee-owned and company-owned. IT sets different policies for each:

>> If any device is jailbroken or rooted, it immediately loses access to e-mail, and IT is notified to make a decision on whether to wipe. This is an extreme situation warranting a decisive response.

>> If a company-owned device has certain applications on it that violate acceptable use policies—for example, games, inappropriate content, even music—the user and IT are automatically notified, and the employee is given a chance to back out the change. Until then, the device can't access corporate resources.

>> If an employee-owned device has the same apps or content on it, perhaps no action is taken. But these devices may have less access to data than the company-owned devices.

>> If the device (let's assume it's based on iOS) has a passcode and thereby has enabled data protection, apps with proprietary information are made available for the user to download from the private enterprise app storefront—for example, an app that lets the user review specs for the latest engineering project. If there's no data protection enabled, then that app doesn't even appear in the user's app catalog.

Mobile device management is a challenge as our perimeters become harder to define. The innovative CIO will turn this challenge into a business opportunity—show that IT can help people be more connected and collaborative, regardless of location. When executed correctly, letting employees use their own devices, regardless of platform, to securely access enterprise data saves money—and wins friends and allies. And if safeguards are built in, conversations with auditors come much easier—you're able to prove that risks are addressed appropriately.

Grant Moerschel is co-founder of WaveGard, a technology consulting firm. Write to us at iwletters@techweb.com.