

High performance. Delivered.

The journal of
high-performance business

Information Technology II

On the Edge

This time, it's personal . . . and mobile

By Kishore S. Swaminathan, Chief Scientist, Accenture

Popular IT history holds that the introduction of personal computers into the workplace was largely a user-initiated coup d'état. Starting in the late 1980s, corporate employees began using PCs for spreadsheets, word processing, scientific calculations, computer-aided design and so forth, usually outside the ambit of their IT departments.

As the user base increased, IT-savvy employees started demanding access to corporate applications from their PCs. After a few years of standoff, corporate IT departments relented and started integrating PCs in what became known as the client-server revolution in the late 1980s and early 1990s. (For a related article, see "Does your company have an IT generation gap?" *Outlook*, January 2009.)

Is history repeating itself with mobile devices? In most companies, users have already won

the battle against their IT departments with respect to e-mail access, never mind security concerns. Now they want access to CRM, HR and every other corporate application from their BlackBerries, iPhones and soon, perhaps, even their Kindles.

What's the hapless IT department supposed to do? Hold out as long as possible—as it did during the PC era—and then surrender unconditionally? Or assume that the battle will be lost anyway and capitulate now before loss of life and limb?

The good news is that the analogy between PCs and mobile devices is flawed. The bad news is that mobile devices will be a lot more difficult and painful to integrate into a corporate IT ecology than PCs were—both from a technical and a business standpoint.

Flawed analogy

Although personal computers may have infiltrated many companies as a means of supporting personal work, employees did not pay for them out of pocket and smuggle them into the workplace. They couldn't: In the late 1980s and the early 1990s, a well-equipped PC or workstation could cost upwards of \$5,000, or about 60 percent of the price of an entry-level automobile. In fact, business units bought PCs for select employees whose jobs and productivity warranted the investment. So one could infer that those employees who deserved that corporate investment had justifiable business cases for why they needed access to various corporate IT applications.

Further, although integrating thousands of PCs into corporate IT was difficult and expensive, it did not pose a great deal of data or network security risk. PCs then were too heavy and clumsy to be removed from the office, and in those pre-Internet days (imagine!), company networks were isolated islands, safe from global hackers and viruses. Also, the PCs and workstations were company-owned, so employers could impose limitations on how employees could use them.

Mobile devices, on the other hand, are an entirely different matter. In most companies, employees buy their BlackBerries, iPhones and whatever else with their own money and usually shell out the hefty monthly fees as well.

This time, it's truly personal. And that's where the trouble starts.

Anybody—which these days means everybody—who has a mobile device wants the same level of access to corporate applications that they have on their PCs, the lack of a business case notwithstanding. Some like BlackBerries, some like

iPhones, some like Nokia N95-s. Some are on AT&T's network, some on T-Mobile's and some are roaming on Telstra's. More worrisome, perhaps, is that users routinely lose their phones on trains, in taxis, and at your client's or supplier's offices. The devices can pick up viruses from the Internet, and even the wireless signal from the device can be a security vulnerability.

One for me, one for you

Scary as this may sound, there is, in fact, a drastic solution that's not uncommon in government and industries like financial services: Ask employees to carry two devices—a standard, company-issued mobile device for business-related activities and their own personal device for everything else. Technology exists today to control the company-issued one remotely in every way: what is stored on the device and what applications can run on the device; technology can even erase data from a lost device, or if the employee has left the company.

Smart and easy, right?

Maybe. But consider the economics. An unlimited voice-plus-data subscription for a mobile device can average \$75 a month, or \$900 a year. Given the pace of change in mobile devices and networks, a company may need to commit to a replacement cycle of at least 24 months. Assuming a \$400 price for a good corporate-grade device, that's about \$1,100 per user, per year, not including roaming charges. With their tiny screens and less-than-user-friendly keyboards, mobile devices are not yet a replacement for PCs, so your employees will still need their PCs too.

For a company of 100,000 employees that chooses to give each one a corporate-issued mobile device for business use, that's a whopping \$110 million in *incremental* IT costs per year. Fortunately, in many

companies today, employees are happy to pay for both the device and the monthly fee out of their own pockets.

Given this cost, most companies will probably issue these corporate devices to only a select group of employees for the near future. This, however, will put these companies back at square one, since they now have to support two classes of users or face the wrath of the disenfranchised ones.

To be useful, company-issued mobile devices must support Web access, which means they are still not protected from viruses, hackers, phishing and all the perils and vices of the Internet. But unlike PCs, there would be no corporate firewall to protect them.¹

In addition, built-in mobile cameras and streaming videos are increasingly being used for business purposes, such as document scanning and training. When such capabilities are available in corporate-issued devices, personal use is almost inevitable, which will gradually blur the distinction between the corporate and the personal device.

Finally, given the hassle of carrying two devices with two sets of chargers and cables, and of managing two contact lists, two sets of logins and passwords to sites that span both business and personal uses (such as social networking sites), employee compliance with various restrictions is likely to be the exception rather than the rule.

In a nutshell, for most people, work and personal lives have become so intertwined in their mobile devices that trying to segregate

them artificially is unlikely to be a viable long-term solution.

Is there a better way?

Game theory can help us understand and analyze the situation. Essentially, here are two players—the corporation and the employee—with different objectives. The corporate objectives include standardization, controlling processes, protecting against data loss or theft, and keeping IT costs low. The employee's objectives include convenience and personal choice.

While the employee is not opposed to the corporate objectives and the corporation is not opposed to the employee needs, factors beyond both players' control (such as the human tendency to lose things or the technological challenges of supplying the same corporate application on the various devices employees might choose to use) put the corporation and the employee at odds. It may seem like a zero-sum game in which one player has to lose for the other to win.

A game theory analysis of such situations (generally referred to as "repeated prisoner's dilemma") holds that the best strategy for both players is not to play against each other but to cooperate and play against the game itself. What if one player does not cooperate? In that case, game theory suggests that the best strategy is "tit for tat": Start by cooperating in good faith, and if the other player defaults (fails to cooperate), then swiftly retaliate to make him or her fall in line. Then cooperate but hold no grudge.

What does that mean in practical terms? First, corporate IT departments have to recognize and accept that

¹ Technically, this problem can be solved by making the users use only VPN (virtual private network) technology to connect to the Internet through the corporate Internet backbone. However, this will dramatically slow down the employees' Internet access to potentially unacceptable levels while dramatically increasing the Internet support cost for a company.

mobility is perhaps the biggest technological wave sweeping the world today: Approximately 60 percent of all people have a mobile phone, and projections are that this will increase to about 80 percent by 2013. Third-generation, or 3G, phones and networks have already deeply penetrated Japan and South Korea, while their adoption in Western Europe, the United States and even in many emerging markets is growing.

Among other things, new devices and networks provide new capabilities—Near Field Communications, or NFC (which enables a mobile device to communicate with the environment), location- and context-sensitive services, video streaming and better user interfaces, to name just a few examples. As such, mobile phones are likely to become perhaps the single most important and ubiquitous communication and service channel between the corporation and its employees, among the employees, and between the employees, customers, suppliers and other business partners.

Accepting reality

By accepting and embracing this reality, companies can reap the advantages of these new capabilities. Specifically: ready and real-time access to customer and sales data for the mobile sales force; on-the-go video-based training; accepting customer orders or payments through NFC-equipped phones; and so forth.

Second, recognize and accept your employees' realities—their mobile devices (irrespective of who pays for them) are, and will continue to be, at the intersection of their personal and professional lives. If you disable cameras, MP3 players and other entertainment features on their mobile phones, they will simply download any number of free software programs (which are

often bundled with viruses, spy-ware and other beasts), potentially compromising the very objective of installing such security controls in the first place.

Third, in the spirit of cooperation, educate employees on the realistic everyday dangers of data theft and loss and on the regulatory requirements and penalties for the violation of data privacy and protection. Then explain the precautions, tools and processes the corporation and employees can deploy together to protect against data theft and to meet the regulatory requirements.

Fourth, to reduce device and network heterogeneity, segment your employees into groups based on their likely preference of features in devices. Perhaps the younger ones want more entertainment features; the executives, uninterrupted global access to voice and data communication; the salespeople, access to high-fidelity audio and video brochures that they can show to customers.

Based on this segmentation, choose a small number of devices and carriers and negotiate bulk, corporate discounts with them. By doing this, the corporate IT department reduces the number of devices it has to support and the employees get to use a device they prefer at a discounted rate.

Fifth, even if the device is employee-owned, bind them contractually to accept a small, mutually agreed-upon set of controls (for example, remote wipe of data and encryption software) established by a representative committee of average end users, business executives and IT executives as a condition of access to corporate data and applications. Don't make these conditions so onerous that even reasonable and cooperative employees will be tempted to disable or subvert them.

Finally, devise your policies in good faith to maximize the productivity of the majority of employees rather than control the potential transgressions of a few bad apples. But in the spirit of tit for tat, don't hesitate to retaliate swiftly when abuses do occur.

Risk and reward, it's said, are two sides of the same coin. Clearly, mobile devices entail both. But as mobile technology advances, the rewards are likely to outpace the risks. Companies that recognize this and plan effectively to reap the rewards while managing the risks will outpace those that focus exclusively on the risks and ignore the rewards.

Kishore S. Swaminathan is based in Chicago.

k.s.swaminathan@accenture.com

Outlook is published by Accenture.
© 2009 Accenture.
All rights reserved.

The views and opinions in this article should not be viewed as professional advice with respect to your business.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

The use herein of trademarks that may be owned by others is not an assertion of ownership of such trademarks by Accenture nor intended to imply an association between Accenture and the lawful owners of such trademarks.

For more information about Accenture, please visit www.accenture.com