Going Mobile

As laptops proliferate, users are freed from the confines of their desktops. But in order to avoid trouble spots, companies must establish written policies for acceptable use.

Written by Stephanie Wilkinson
Illustrated by Jean-François Martin

EARLIER THIS YEAR, Gartner Inc., a market-research firm in Stamford, CT, announced that sales of laptop computers are growing six times faster than desktop PCs—another computing milestone passed. Funny thing about milestones, though—if you're not careful, they can turn into stumbling blocks. With more and more mobile computers being deployed in businesses today, companies need to be ever more watchful about who gets them and how carefully they are used. Like nervous parents of a teenager, IT managers worry every time a laptop goes out the door—and often with good reason. Theft, damage, loss of data, breach of corporate security—all these risks increase with greater laptop usage. And yet, with more computing power being packed into ever smaller, lighter, and more connected packages, laptops have become an indispensable business tool. Managing how they're used, then, means coming to grips with the classic tradeoff between access and security.

"If we didn't make it clear who the responsible party was, we'd end up with a whole lot of "lost" laptops that would cost the city a bundle."

In the old days, when laptops were high-ticket items, companies thought long and hard about who would be allowed to take them out of the office. But as prices drop and employees spend more working hours out of the office, reining in laptop use is neither practical nor wise. "We're increasing our use of laptops all the time," says Cathy Rex, IS manager for the City of St. John's in Newfoundland, Canada. "We want to make it easier for city employees to be out of the office. It serves our citizens better."

With the line between work hours and off hours blurred, more people are spending more of their waking life on the job. "The wireless revolution has certainly helped to fuel small business demand for notebook computers," says Todd Gold, a writer for Laptopical.com, a laptop aficionado Web site. "Also, the prices for laptops are getting lower."

Gold cites the new Compaq NX6125 from Hewlett-Packard as an example of the kind of affordable mobile technology rivaling desktop performance that small companies are hot for. Priced less than $1,000, this computer comes equipped with a 64-bit AMD Turion processor, a 60GB hard drive, wireless connectivity, and a biometric fingerprint reader for added security. It weighs about six pounds, Gold says, and also features a spill-resistant keyboard and scratch-resistant lamination—welcome protection against the inevitable knocks mobile computers face on the road.

Acceptable Use Policies

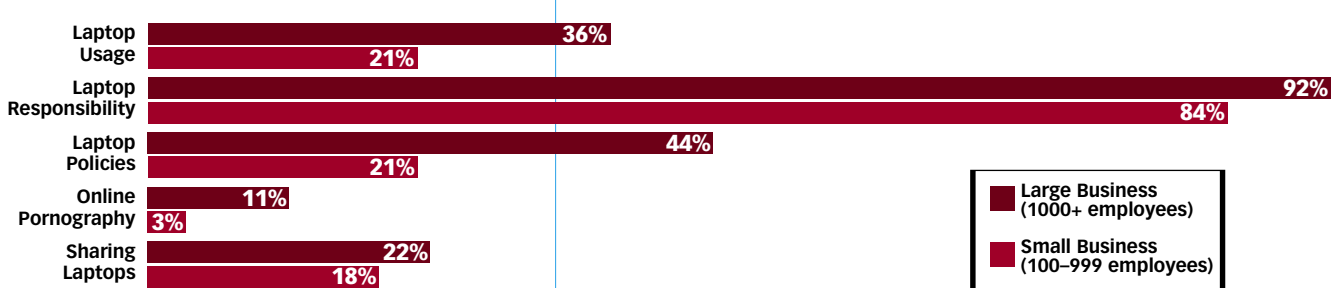
Such protective coatings are nice, but it's how the machines are used both in and out of work that makes all the difference. Interestingly, laptop users in small- to mid-sized businesses have a different attitude toward their laptop or notebook equipment, a new study shows. According to the most recent Web@Work study, a survey of 354 IT managers conducted by Harris Interactive in February 2005, employees at smaller firms are less likely to feel responsible for how the laptop is used outside the office than those at larger firms. In addition, more SMB employees admitted to sharing their laptop with family and friends than employees at large companies. And three times as many SMB users admitted to looking at pornography on their work-owned laptops than those at larger companies.

These disparities might be explained by another of the study's findings: Larger companies are twice as likely as smaller ones to have a written policy outlining acceptable use of company laptops.

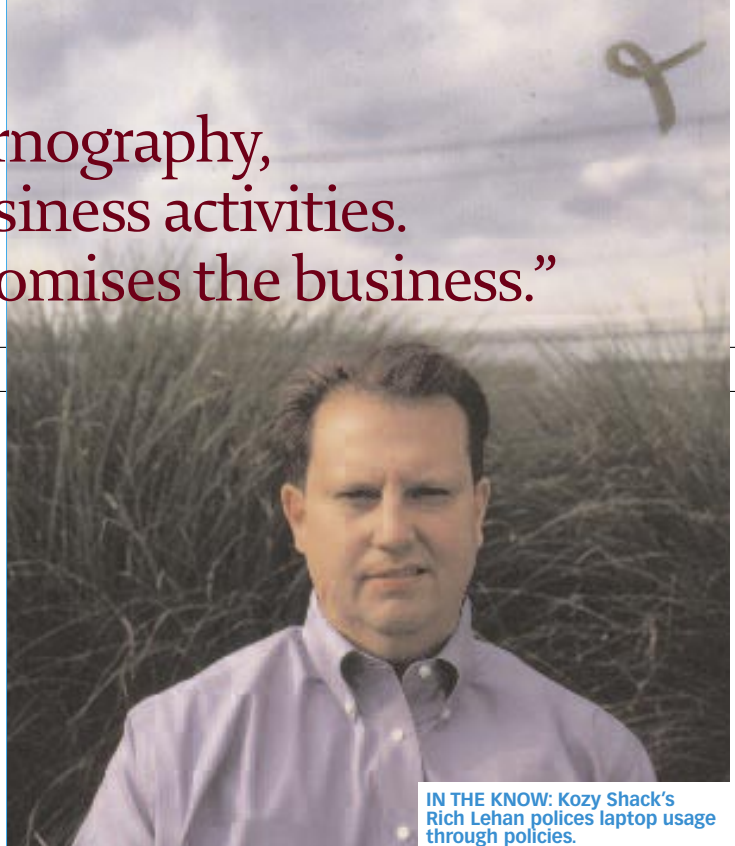
The city government of St. John's has one. According to IS Manager Rex, the policy was created two years ago, just as laptop deployment among city officials began to rise. It's modeled in part on policies suggested in a book called *The E-Policy Handbook* by Nancy Flynn. St. John's policy spells out who is responsible for the laptop (the

Laptops in the Workplace

Companies of all sizes are flocking to laptops, but employees at smaller firms tend to feel less responsible for how their company-issued gear gets used outside of work. SMB users are more likely to share their laptops with others and partake in non-sanctioned activities like surfing porn while off the job. Maybe that's because SMBs are less likely to put policies in place to restrict laptop use.



"No gambling, no pornography, no inappropriate business activities. Nothing that compromises the business."



IN THE KNOW: Kozy Shack's Rich Lehan polices laptop usage through policies.

KEN MISSBRENNER

employee), who can use it (the employee only—no friends, no relatives, no random tablemates at Starbucks), what kinds of software or peripherals can be installed on it (only what's put there by the IS division), and what happens in case of theft or breakage (the employee and/or the employee's department must replace or repair it). Laptop users at St. John's all undergo a day-long orientation session covering proper care and handling of the machines. If requested to do so, the employee must return the laptop to the IS division within 24 hours.

Besides the acceptable use policy, city employees who are issued laptops are heavily restricted in their Internet access—they can only access the Web through the company's firewall—and they are required to come into the office each morning to physically plug into the network to download the day's software patches and virus updates. If they neglect to do it, the patches are pushed out to them the next time the user connects to the network remotely.

Requiring laptop users to take personal responsibility for their computers is prudent for several reasons, Rex says. "Our city's insurance policy has a $10,000 deductible. We were concerned that if we didn't make it clear who the responsible party was, we'd end up with a whole lot of 'lost' laptops that would cost the city a bundle."

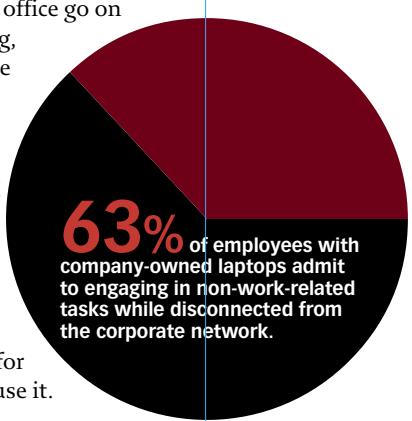
Rich Lehan, director of IT at Kozy Shack, a pudding manufacturer based in Hicksville, NY, points out the importance of tying laptop policies into a company's overall employment policies. With a third of his 250 computer users equipped with laptops, Lehan's biggest concern is that nothing those laptops pick up on the road infects the corporate network. So he's careful to remind users that rules that apply in the office go on the outside as well. "No gambling, no pornography, no inappropriate business activities," Lehan says. "Nothing that compromises the business."

Some rules are more tempting for employees working outside the office walls to skirt than others, he says. "For a certain contingent, their laptop is the only computer in the house," Lehan says. "It's really tempting for them to let their spouse or kids use it. But they know we're always doing software audits and we will find out what they've been up to."

Since Internet access presents the greatest misuse temptation and the biggest risk to corporate network security, Kozy Shack uses Web filtering software to block some Web sites entirely, allow restricted access to others, and provide a daily per-person quota on another class of site, such as sports or shopping sites.

Lehan thinks having such policies and tools out in the open has fostered good behavior among users. "We're a small company, and they know if they break or lose that laptop, it will affect the bottom line," he says.

Stephanie Wilkinson has been writing on high-tech and business issues since 1986.



On The Clock

Curious to know how your company laptop is used off hours? Here are the most common tasks:

- **Personal surfing (56%)**
- **Managing digital photos (28%)**
- **Sharing laptop with family & friends (19%)**

SOURCE: Web@Work Study, February 2005.
Conducted by Harris Interactive for Websense, Inc.
NOTE: Results are not broken down by company size.