

# Lost BlackBerry Could Open Security Breach

---

*Source:* <http://newsgroups.derkeiler.com/Archive/Comp/comp.dcom.telecom/2005-07/msg00556.html>

---

- *From:* Yuki Noguchi <[washpost@xxxxxxxxxxxxxxxxxxxxxx](mailto:washpost@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 25 Jul 2005 19:08:27 -0500
- 

By Yuki Noguchi, Washington Post Staff Writer

The ability to carry vast amounts of data in small but easily misplaced items such as computer memory sticks and mobile e-mail devices has transformed the way Americans work, but it has also increased the risk that a forgotten BlackBerry or lost cell phone could amount to a major security breach.

Worried that sensitive information could ride off in the back of a taxicab or be left in a hotel room, companies are peeling back some of the convenience of mobile devices in favor of extra layers of password protection and other restrictions. Some are installing software on their networks to make it impossible to download corporate information to a portable device or a memory stick, which is a plug-in device that holds data for use on other computers. Wireless providers are developing weapons to use against their own products, like digital "neutron bombs" that can wipe out information from long distance so one misplaced device doesn't translate into corporate disaster.

It's a nightmare that individuals and corporations fret about when their mobile e-mail or handheld devices go missing or fall into the wrong hands. With the swift stroke of a keypad, someone's e-mail, corporate data and business contacts can be laid bare for others to see — and potentially abuse.

Personal devices "are carrying incredibly sensitive information," said Joel Yarmon, who, as technology director for the staff of Sen. Ted Stevens (R-Alaska), had to scramble over a weekend last month after a colleague lost one of the office's wireless messaging devices. In this case, the data included "personal phone numbers of leaders of Congress. If that were to leak, that would be very embarrassing," Yarmon said.

A couple of years ago, David Yach and all other workers at his Canadian company woke up to an e-mail full of expletives from an otherwise mild-mannered female employee.

But it was not sent by the woman. A thief had broken into her home, commandeered her BlackBerry wireless device and sent the note, said

## Lost BlackBerry Could Open Security Breach

Yach, vice president of software at Research in Motion Ltd., the company that makes the BlackBerry, a device that allows e-mail to be sent and received.

"It's terrifying," said Mark Komisky, chief executive of Baltimore's Bluefire Security Technologies Inc., who recently lost his iPaq 6315 Pocket PC in a cab or at O'Hare International Airport in Chicago. The device, a small pocket phone with a miniature keyboard, contained his e-mail, details of his company's strategy, Social Security numbers of his wife and son, and phone numbers for high-level executives at companies with which Bluefire does business, such as Intel Corp.

"I got off the plane in Baltimore and did the pat-down, and didn't have it," he said. "It's bad," even for the head of a firm that sells security services for companies and government agencies trying to secure their wireless devices. At 10:30 p.m., he called a technician at Bluefire, who erased the information on the iPaq remotely. Luckily, it was also locked with a password, he said.

Companies are seeking to avoid becoming the latest example of compromised security. Earlier this year, a laptop computer containing the names and Social Security numbers of 16,500 current and former MCI Inc. employees was stolen from the car of an MCI financial analyst in Colorado. In another case, a former Morgan Stanley employee sold a used BlackBerry on the online auction site eBay with confidential information still stored on the device. And in yet another incident, personal information for 665 families in Japan was recently stolen along with a handheld device belonging to a Japanese power-company employee.

To combat the problem, security companies have come up with ways to install layers of password protection and automatic locks on devices. Others market the ability to erase data over the air once the device is reported lost. In Japan, cell phone carrier NTT DoCoMo Inc. started selling models that come with fingerprint scanners to biometrically unlock phones.

Some companies suffer only embarrassment from such incidents. But for public companies or financial firms, a lost device could mean violation of the Sarbanes-Oxley Act, which requires strict controls over disclosure of financial information. For doctors and health care companies, the loss of customer data compromises patient confidentiality, protected by the Health Insurance Portability and Accountability Act.

Potential security breaches are made scarier by the greater reliance on mobile devices. Smart phones, such as the Treo or some BlackBerry models, come with enough memory and high-speed Internet access to function as small computers. In some cases, accompanying memory cards allow users to store even more data, including client lists and contract information.

## Lost BlackBerry Could Open Security Breach

"I hear less about the cost of the devices, because it really is a pittance, but I really do hear more about the potential cost of someone gaining access to corporate data," said Kenny Wyatt, a vice president for Sprint Corp., which helps some of its business customers manage the security of wayward devices.

Three years ago, Wyatt lost a cell phone containing phone numbers of co-workers and clients. Sprint now can delete information by sending a signal to a phone over the air, he said, although if the device is turned off, the kill signal won't work.

Without the kill service, losing his phone would be a bigger deal today than it was three years ago because the device contains so much more information, he said. "It'd be like I lost an appendage."

In Chicago, 160,000 portable devices are left in taxicabs every year, according to a survey earlier this year by Pointsec Mobile Technologies, a security software firm. Fifty to 60 percent of those are reunited with their owner, according to the firm, which polled cab companies.

According to another survey sponsored by software maker Symantec Corp., 37 percent of smart-phone users store confidential business data on their phones. Only 40 percent of those surveyed worked at companies that have corporate policies about wireless security.

Yarmon, the staffer for Sen. Stevens, said he sends an e-mail every few months reminding colleagues to install passwords on devices. "That is my worst fear," he said, "for a user to have it fall into the hands of somebody who disseminates it or uses that information against my boss."

Copyright 2005 The Washington Post Company.

NOTE: For more telecom/internet/networking/computer news from the daily media, check out our feature 'Telecom Digest Extra' each day at <http://telecom-digest.org/td-extra/more-news.html> . Hundreds of new articles daily.

- 
- Prev by Date: [\*Yahoo Buys Information 'Widget' Company Pixoria\*](#)
  - Next by Date: [\*AOL's Steve Case Finds Lime Twist in Wisdom\*](#)
  - Previous by thread: [\*Yahoo Buys Information 'Widget' Company Pixoria\*](#)
  - Next by thread: [\*AOL's Steve Case Finds Lime Twist in Wisdom\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)