



Search:

News Magazine

[Home/News](#) | [Subscribe](#) | [Editorial Calendar](#) | [Links](#) | [Contact Us](#) | [Partners](#) | [Forums](#)



Current Issue

- [News & Views](#)
- [Speed Thrills](#)
- [QuickSpins](#)
- [Made in Taiwan](#)
- [New Arrivals](#)
- [Bluetooth](#)
- [HardWear](#)
- [Profiles](#)

Archives

2001

[Jan](#) [Feb](#) [Mar](#)
[Apr](#) [May](#) [June](#)

2000

[Apr](#) [May](#) [June](#)
[July](#) [Aug](#) [Sept](#)
[Oct](#) [Nov](#) [Dec](#)

Mobile Labs

ARCHIVES

Steal This Laptop!

By Cassimir Medford, February 2001

A notebook is a small, high-priced package that is easily stolen. Users must learn to keep their systems and their data safe and secure.

Who can you trust? That is the question IT managers are asking in the wake of several high-profile notebook thefts. Qualcomm Inc.'s chief executive Irwin Jacobs' laptop disappeared in September when he turned away for about 20 minutes to talk to a small group of reporters after a speech at a Southern California hotel. According to published reports, Jacobs said the laptop contained sensitive information that could compromise the company's competitive position.



Illustration by Douglas Fraser

officials, the New Zealand contingent reported five laptops stolen. In what police believe was a crime of opportunity, three notebook computers and a personal digital assistant were stolen from the Democratic National Committee's finance office in New York; the computers taken were those closest to the office door.

While bad news for the victims, these incidents served as a wake-up call to IT managers and security specialists. For years, IT managers have complained about poor notebook security but found the corporate

Last year, a notebook containing top-secret information on arms proliferation disappeared from the State department. The CIA also had to grapple with lax security when former Director John Deutch was found to have copied sensitive files to his notebook. And even in the Olympic Village in Sydney, Australia, where access was restricted to accredited athletes and



Index

- [Page 1](#)
- [Page 2](#)
- [Page 3](#)
- [Go Directly to Jail](#)
- [Six Things to Remember](#)
- [Steal These URLs](#)

Options

If you prefer a **Single Page** for reading this article, [click here](#)

For a page specially formatted for **printing** this article, [click here](#)

purse strings pulled tight when they appeared for money to combat notebook theft.

[CLICK HERE](#)

"When I go in and say I need \$300,000 for data security, people look at me like, 'No you don't,'" says Chris Apgar, data-security officer for Providence Health Plan in Beaverton, OR. Apgar advises that when faced with opposition to a security proposal, "You need something more than just strong powers of persuasion to get the attention of corporate management."

Most managers wince at the thought of having the names of their companies publicly associated with a breach of computer security. Apgar's concern with security was heightened by a federal law that imposes penalties, including fines of \$250,000 and 10 years in jail, when the confidentiality of a health-care system's patient is compromised by a breach of security, including data security (see accompanying sidebar "Go Directly to Jail" at left).

In explaining his struggle to get the funding he needed for security, Noah Groth, president and CEO of PC Guardian, a San Rafael, CA-based vendor of security products, says: "We were fighting from the bottom up. But when a chief executive's notebook gets stolen, it gets plastered all over the papers. Every chief executive all of a sudden adopts a sense of urgency."

Crime Costs

Experts say computer theft is a severe and growing problem. For instance, Columbus, OH-based Safeware Insurance Agency Inc., a company that insures computer equipment, reports that notebook losses from thefts and accidents have grown significantly. In the past three years, thefts accounted for 29 percent of all claims made to Safeware, and annual claims rose more than 11 percent to nearly \$1.75 million. Claims for personal computers in 1999 totaled approximately \$1.9 million.



Compaq's PC Card Biometrics ID device

319,000 laptop computers stolen in 1999, representing \$800 million in losses.

The Federal Bureau of Investigation reports that more than 300,000 notebooks, about 3 percent of those in use, were stolen in 1999.

Safeware says that its clients reported

"People are hesitant to call it an epidemic, but notebook thieves are getting bolder," claims Brian Haase, Safeware's commercial-marketing manager.

"Corporations are concerned about the asset itself, but the data on the notebook hold a lot of value to the

company."

The irony is that in most cases the data on the machine is worth far more than the notebook itself. "There is uncertainty on the value of data residing on mobile devices," says Anthony McMahon, marketing manager of Hewlett-Packard Co.'s business unit for OmniBooks. "And that makes it very difficult for them to have a sense of urgency, [but] shareholders and corporate managers are beginning to attach dollar values to the data."

[GO TO: Page 2](#)

Read more great articles in *Mobile Computing*

SUBSCRIBE

[Home/News](#) | [Subscribe](#) | [Subscriber Services](#)

[Editorial Calendar](#) | [Links](#) | [Forums](#) | [Contact Us](#)

[Partners](#) | [Media Kit](#) | [Privacy Statement](#) | [Legal](#)

Mobile Computing logo and all contents of this site
are copyright 1998-2000 by [EMAPUSA Inc.](#)
All Rights Reserved.