



THE ASSOCIATED PRESS

Jim Stickey, chief technology officer at Trace Security Inc., holds his son, Gannon, 5, at their home in San Diego. When Stickey recently registered his son for karate classes, the form asked for the 5-year-old's Social Security number and driver's license number. Stickey said safekeeping of customer data that could be used by thieves should start with not asking for information a business doesn't really need.

Businesses careless with personal data

By Ellen Simon
THE ASSOCIATED PRESS

NEW YORK — Stealing Social Security numbers and other sensitive data isn't always a cloak-and-dagger, ultra-sophisticated operation: It's often a low-tech job made easier by carelessness and flimsy safeguards.

Plenty of inexpensive measures can protect data from the large-scale theft that big banks, data merchants and other companies have recently disclosed.

But "security and privacy, for a lot of large organizations, are an afterthought, not a priority," said Evan Hendricks, who publishes the newsletter *Privacy Times*.

Consider the latest headache for some large banks.

Wachovia Corp. and Bank of America Corp. say they have notified more than 100,000 customers that their accounts and personal information may be at risk after former bank employees allegedly sold account numbers and balances to a man who then sold them to data collection agencies. Nine people have been arrested in New Jersey in the case.

Or consider MCI Inc.'s privacy problem.

An MCI laptop containing the names and Social Security numbers of 16,500 current and former MCI Inc. employees was stolen

last month from the car of an MCI financial analyst in Colorado. The car was parked in the analyst's home garage. The computer was password-protected; the company would not comment on whether the data were encrypted.

Encryption, which is relatively inexpensive, would make all those records all but impossible to access.

After a previous embarrassment, Bank of America is testing different encryption methods. It lost backup tapes in December containing the Social Security numbers and account information for 1.2 million federal workers, including senators and 900,000 Defense Department employees.

Such losses go to the heart of information technology security, whose importance is magnified as more data are concentrated in ever-smaller packages.

That the backup tapes in the Bank of America case were shipped as commercial air cargo shows the bank didn't understand their worth, said Jim Harper at the *Cato Institute* think tank.

"That's like shipping stock certificates in an envelope," he said.

One simple measure many companies can start with is collecting less information, said Jim Stickey, chief technology officer at TraceSecurity Inc., a Louisiana security company.

"Personal data is cash money. If you leave it sitting out on a sidewalk, you're making a mistake."

Greater scrutiny of clients could have spared ChoicePoint Inc. considerable grief, analysts say.

After ChoicePoint said in February that thieves using stolen identities had created 50 dummy businesses that pulled data including names, addresses and Social Security numbers on as many as 145,000 people, its stock dropped precipitously from \$48 a share the day before the announcement to the current price of about \$39.

A simple Google search on some of those company names came up empty, but ChoicePoint "never had a system in place for really checking them," Hendricks said.

One simple measure many companies can start with is collecting less information, said Jim Stickey, chief technology officer at TraceSecurity Inc., a Louisiana security company.

When Stickey signed his son up for karate recently, he was asked for his Social Security number, home address and drivers' license number.

"There's no reason for that," he said. "The security at the karate shop is not like a bank."