

The New Face of Identity Theft

As scams become more sophisticated, companies of all kinds find themselves at risk.

[Peter Krass](#), CFO IT

March 15, 2005

In January 2004, the MyDoom computer virus proved so malicious that Microsoft and other companies offered hundreds of thousands of dollars in reward money for information leading to the arrest and conviction of the virus author. Is it possible that those were the good old days?

As this year began, computer security vulnerabilities again made headlines, but the nature of the attacks was far different. A hacker stole the Social Security numbers and other personal data of thousands of students and employees at George Mason University, home of the Center for Secure Information Systems, a project that involves the U.S. Department of Defense.

Sensitive personal information was also at issue at T-Mobile, which said in January that it had cooperated with authorities that had made an arrest in a case involving security breaches in 2003 and 2004. Those breaches reportedly involved not only the names and Social Security numbers of 400 customers but also Secret Service information and even photos taken by celebrities with their camera phones.

And, of course, the theft of the personal data of 145,000 consumers from ChoicePoint Inc., which was made public last month, made the reality of identity theft front-page news yet again.

Virus attacks remain a threat, of course, but far more worrisome is the trend toward identity theft and theft of data. Unfortunately, a new *CFO IT* poll suggests that CFOs may not be adequately focused on this emerging threat. ID theft, dubbed the fastest-growing white-collar crime in America, is not just an issue for consumers and their financial institutions. It also poses a very real danger to any company that uses computers and the Internet.

Armed with the user name and password of an employee in your company, an ID thief can access your company's computer systems with virtually no risk of detection. "Getting a person's password is actually an elegant way of attacking a corporation," says Peter Firstbrook, a program director at Meta Group. "It's like starting a car with a stolen key — there's no shattered glass, no alarm set off. It's entirely possible that nobody will notice."

Stealing user names and passwords is relatively easy, but a would-be criminal doesn't even have to do that. Security experts and studies indicate that there are possibly thousands of Websites that exist solely for the purpose of stealing, buying, and selling IDs. In fact, ID theft has become a big business, big enough to attract international organized crime.

The potential damage goes well beyond the value of the data stolen. Jonathan Penn, a market analyst at Forrester Research, maintains that because of the fear of ID theft, consumer confidence in conducting business online is now eroding. "People are moving off online banking because of security concerns," he says. "Suddenly this is becoming a trillion-dollar problem once you look beyond fraud loss to consumer E-finance adoption and retention."

While few people regard the CFO as the front line of defense on computer security, the potential damage to corporate reputation, the threat of fines for failing to protect sensitive data, and the actual hit that corporate coffers could take make data protection a major facet of risk management. Some CFOs get the message, yet while companies do continue to spend heavily on computer security, awareness may still lag in reality (see "[Security by the Numbers](#)").

Security vs. Convenience

Thieves employ several simple, straightforward techniques to steal personal information. They snatch documents containing Social Security numbers and other personal data from the mail. They steal computers on which ID information is stored. They hack into corporate databases. They buy IDs from other thieves. They bribe company insiders to provide printouts of customer and employee data. They fish through trash bins, looking for human-resources documents. They trick consumers (and employees) into providing their user IDs and passwords via E-mail or links to phony Websites, a process known as phishing (see "Gone Phishin'," at the end of this article). And they use spyware that captures keystrokes, essentially a high-tech way to peer over someone's shoulder as he enters personal data.