

December 31, 2007

Data Breaches Of Personal Info Soar

Mark Jewell, Associated Press

The loss or theft of personal data such as credit-card and Social Security numbers soared to unprecedented levels in 2007, and the trend isn't expected to turn around soon as hackers stay a step ahead of security and laptops disappear with sensitive information.

And while companies, government agencies, schools and other institutions are spending more to protect an ever-increasing volume of data with more sophisticated firewalls and encryption, the investment often is too little too late.

"More of them are experiencing data breaches, and they're responding to them in a reactive way, rather than proactively looking at the company's security and seeing where the holes might be," said Linda Foley, who founded the San Diego-based Identity Theft Resource Center after becoming an identity theft victim herself.

Foley's group lists more than 79 million records reported compromised in the United States through Dec. 18. That's a nearly fourfold increase from the nearly 20 million records reported in all of 2006.

Another group, Attrition.org, estimates more than 162 million records compromised through Dec. 21 - both in the U.S. and overseas, unlike the other group's U.S.-only list. Attrition reported 49 million last year.

"It's just the nature of business, that moving forward, more companies are going to have more records, so there will be more records compromised each year," said Attrition's Brian Martin. "I imagine the total records compromised will steadily climb."

But the biggest difference between the groups' record-loss counts is Attrition.org's estimate that 94 million records were exposed in a theft of credit-card data at TJX Cos., the owner of discount stores including T.J. Maxx and Marshalls. The TJX breach accounts for more than half the total records reported lost this year on both groups' lists.

The Identity Theft Resource Center counts about 46 million - the number of records TJX acknowledged in March were potentially compromised. Attrition's figure is based on estimates from Visa and MasterCard officials who were deposed in a lawsuit banks filed against TJX.

The breach is believed to have started when hackers intercepted wireless transfers of customer information at two Marshalls stores in Miami - an entry point that led the hackers to eventually break into TJX's central databases.

TJX has said that before the breach, which was revealed in January, it invested "millions of dollars on computer security and believes our security was comparable to many major retailers." With wireless data transmission more common, hackers increasingly are expected to target what many experts see as a major vulnerability. Eavesdroppers appear to be learning how to bypass security safeguards faster than ever, said Jay Tumas, the

head of Harvard University's network operations, at a recent conference for information security professionals.

"Within a year or two, these folks are catching up," Tumas said.

The two nonprofit groups' 2007 data also show rising numbers of incidents in which employees lose sensitive data, as opposed to cases of hacking.

Besides TJX's problem, major 2007 breaches include lost data disks with bank account numbers in Britain, a hacker attack of a U.S.-based online broker's database and a con that spilled resume contact information from a U.S. online jobs site.

"A lot of breaches are due to inadequate information handling, such as laptop computers with Social Security numbers on them that are lost," Foley said. "This is human error and something that's completely avoidable, as opposed to a hacker breaking into your computer system."

Attrition.org and the Identity Theft Resource Center are the only groups, government included, maintaining databases on breaches and trends each year. They've been keeping track for only a handful of years, with varied and still-evolving methods of learning about breaches and estimating how many people were affected.

Despite those challenges, the two nonprofits say it's clear 2007 will end up a record year for the amount of information compromised because of greater data loss and increased reporting of breaches.

Both groups acknowledge many breaches may be missing from their lists because they largely count incidents reported in news media that they consider credible. Media coverage has risen in part because of the growing number of states requiring businesses and institutions to publicly disclose data losses.

Because of proliferation of such laws, "it may take a year or two before things stabilize and we can see what's really happening," Foley said. "If that's the case, then we'll know whether businesses are practicing better information-handling techniques."

Some records losses in 2007

- Discount retailer TJX Cos. reports hackers broke into its computer systems and accessed at least 46 million customer records, primarily credit-card data. Banks later sue TJX and estimate the breach involved at least 94 million records.
- Britain's tax and customs department loses two computer disks containing personal information such as addresses and bank account numbers for about 25 million people. The disks were sent via internal government mail to the government's audit agency but never arrived.
- Dai Nippon Printing Co., a Japanese commercial printing company, says a former contract worker stole nearly 9 million pieces of private data on customers from 43 clients.
- A check-authorizing subsidiary of Fidelity National Information Services says information on 8.5 million consumers was stolen, allegedly by a former employee.
- Online brokerage TD Ameritrade Holding Corp. said one of its databases was hacked and contact information for its more than 6.3 million customers was stolen.
- The online job site Monster Worldwide Inc. discovered that con artists had grabbed contact information from resumes of 1.3 million people.

© 2008 The E.W. Scripps Co.