

December 18, 2006

LINK BY LINK

## An Ominous Milestone: 100 Million Data Leaks

By **TOM ZELLER Jr.**

ON Thursday, Kevin Poulsen, senior editor for Wired News, noted in his blog ([blog.wired.com/27bstroke6/](http://blog.wired.com/27bstroke6/)), a milestone in the number of records that have been compromised in data breaches since the ChoicePoint breach nearly two years ago:

“Rapid-fire announcements this week by U.C.L.A. (800,000 records) and Aetna (130,000) moved the total to the threshold, when Boeing revealed yesterday that a laptop recently stolen from an employee’s car contained names, Social Security numbers and other data on 382,000 current and former employees of the aerospace giant — bringing the total to a grim 100,152,801 records (as of this post).”

One might at least hope that the thief in the Boeing incident was simply after the laptop, rather than the data. And the Aetna case, well, that data was stored on backup tapes that were in a lockbox, which thieves lifted — along with DVD players, cash and other items — in a routine burglary.

But in the incident involving the University of California, Los Angeles, announced last Tuesday, there was really no question about the motive and the quarry. A hacker, or hackers, had been entering the restricted database — which contained the names, addresses, Social Security numbers and other private information of current and former students and faculty — for over a year before the breach was discovered.

A commenter at the Wired News blog, giving only the affirmative “yea” as a name, had this to say:

“I was a U.C.L.A. student that got my info lifted. I think it’s horrible not only that these companies are so sloppy and careless about our data but that we have such a weak link in the chain of our security. Congress has let companies use SSN in ways they were never meant to be used and now we are paying the price for it. Add a debt-happy culture to the mix and you have a truly toxic brew of misery if someone gets a hold of your SSN.”

As it turns out, educational institutions have a particularly acute problem when it comes to the nation's leaky data issue.

A study by the Public Policy Institute for [AARP](#) last July, using data compiled by the Identity Theft Resource Center, determined that of the 90 million records reportedly compromised in various breaches between Jan. 1, 2005, and May 26, 2006, 43 percent were at educational institutions.

•

In fact, educational institutions were twice as likely to report suffering a breach as any other type of entity, with government, general businesses, financial service and healthcare companies pulling up behind.

"College and university databases are the ideal target for cyber criminals and unscrupulous insiders," said Ron Ben-Natan, the chief technology officer of Guardium, a database security and monitoring company based in Waltham, Mass. "They store large volumes of high-value data on students and parents, including financial aid, alumni and credit card records.

"At the same time," Mr. Ben-Natan continued, "these organizations need open networks to effectively support their faculty, students and corporate partners."

But the bigger picture here may be that we are now slicing and dicing the niceties of data breaches against a running tally so large, that it has lost nearly any meaning at all.

Another commenter at the Wired News blog complained that the 100 million mark "is arbitrary and a significant underestimate because it does not include breaches before the ChoicePoint breach."

He's right, and he pointed to other tallies, like that maintained at [attrition.org/dataloss](http://attrition.org/dataloss), which keeps a global tally and reaches back as far as 2000. They put the number of records compromised at 136 million and counting.

But whether we're at 100 million or 136 million or something on the order of the entire population of the United States, the question is, what does it matter?

Some have argued not much. "The threat of identity theft from data losses is being greatly exaggerated," Fred H. Cate, the director of the Center for Applied Cybersecurity Research at [Indiana University](#) in Bloomington, told this newspaper not long ago. "And that's because a lot of people have fallen into the trap of equating data loss with identity theft."

Whether or not that is true is open to debate, but what all this data loss does represent, however, is the potential for identity theft — one that will never go away. Sure, it's a game of odds. There is only so much a crook can do with a few hundred thousand names and Social Security numbers. But once they are out there, they are out there for good. Names don't change. Neither do Social Security numbers or dates of birth. And as long as it remains easy enough to fashion that trifecta into a car loan, a home, a credit card, work papers, that would seem to be a bit of a long-term problem.

Indeed, Julie Ferguson, a vice president at Debix, an identity protection firm, and a board member of the Merchant Risk Council, an antifraud trade group, says she has begun seeing premiums placed on “aged” data at some online black market sites where stolen consumer identity and account information is traded.

“At some point organized crime is going to get real organized and actually figure out what to do with the millions of identities and user accounts sitting on these thieves' computers,” Ms. Ferguson said. “Right now, there is just too much data, and the criminals simply have not figured out a way to commit crimes against a million individuals all at once.”

•

For its part, Congress has failed, despite the introduction of numerous data security bills, to agree on any legislation. States have picked up some of the slack, passing many breach notification bills. And 18 states now permit citizens to freeze their credit lines, preventing would-be thieves from opening new accounts. Seven more states make the freeze available to citizens only after they have become victims of identity theft, according to the National Conference of State Legislatures.

Meanwhile, the [University of Colorado](#) at Boulder announced on Friday that the names and Social Security numbers of 17,500 former students may have been exposed in an attack on a server. Those students will be receiving letters notifying them of the breach.

“When it comes to identity theft, there's only one victim that counts — you. The rest are just numbers,” said Mr. Ben-Natan. “When it happens, it takes over your life, and you feel betrayed by the organization that didn't protect you.”

Copyright 2006 The New York Times Company

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)

---