

530M records exposed, and counting

Jay Cline

September 9, 2008 ([Computerworld](#))

By my count, over half a billion records of personal information have been exposed or mishandled in the past eight years. And these are only from breaches where a record count has been publicly revealed.

That's more than the population of the [European Union](#), and more than the number of people living in the U.S., Canada, Mexico and all of Central America and the Caribbean combined.

My count of 530 million is more than double the 244 million records cited on [Privacyrights.org](#). So how did I arrive at that figure?

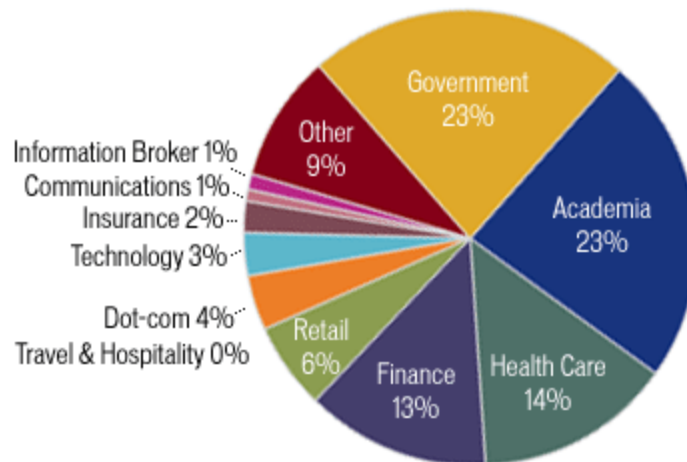
There are a number of Web sites where you can find information about data breaches, including [Computerworld's privacy page](#), [Attrition.org](#), the [Identity Theft Resource Center](#), blogs, government agencies and privacy newsletters such as the International Association of Privacy Professionals' "[Daily Dashboard](#)". For my summer project this year, I tabulated the data from all of these sources. I added them to files I'd been keeping since 2000, which included data on breaches stretching back to 1995. An intern, Emily Prather, Googled the Fortune 500 companies for news of breaches that didn't make these lists. Add to these several dozen notification letters received by friends and family, and we tallied about 1,500 breaches.

What does the data say about the information risks facing your organization?

The biggest surprise to me was the sources of breaches. Many people within the information security profession refer to the insider threat as the primary source of risk, routinely saying that 75% of breaches are the work of employees.

This isn't exactly what breached companies are telling the press, though. The biggest line item we found was hackers, at 20% of all breaches. For

their part, dishonest insiders garnered 3% of the blame. It's possible that a good number of the stolen laptops (19%) and other computers (8%) were taken by employees, but the cases we reviewed appeared mostly to be random criminal acts.



If you add up all of the mistakes employees make — such as losing laptops and backup tapes, improperly disposing of documents, inadvertently sending e-mails and packages, and misconfiguring Web sites — the employee category amounts to 39%.

A whopping 11% of publicized breaches were the result of an errors traceable to vendors.

Have these root causes changed over time? Many of us in the privacy profession know that organized crime is thriving in the stolen-information business and growing in sophistication each year. And maybe they're getting away with it more often. The share of intentional privacy breaches has fallen from 74% in 2005 to 55% this year. Conversely, unintentional data exposures rose from 25% to 40% over the same period, with unspecified causes accounting for the remainder.

There has also been some speculation that breach notification has peaked in the U.S., with more companies encrypting their laptops and doing better overall at applying lessons learned in breach prevention. The numbers

don't support this assumption. From 1995 to 2004, I tracked 186 breaches, with an equivalent number in 2005 alone. In 2006 and 2007, and number of breaches topped 400, and it's on track to do so again in 2008. Each of the past three years has also seen more than 100 million records exposed.

Does risk vary by geography? The mandatory notification of privacy breaches in the U.S. has inflated the appearance of risk in America, with the U.S. accounting for 89% of the incidents we recorded. The U.K. (6%), Canada (3%) and Japan (1%) rounded out the top tier.

Within the U.S., the states with the highest number of breaches tracked closely with their relative populations, with California (133 incidents), New York (68), Ohio (58), Texas (57) and Florida (34) taking top spots.

But if you break down the incidents on a per-capita basis, our nation's capital tops the list at 75 breaches per million inhabitants. Montana (10 per million), Vermont (eight), New Hampshire (seven) and Rhode Island (seven) — with their handfuls of breaches and low populations — rounded out the top tier.

And what about industry sector? Some of the more infamous breaches — such as [CardSystems](#), [ChoicePoint](#) and TJX — may have given the impression that the privacy breach phenomenon is all about credit card number acquisition from private-sector companies.

But in terms of sheer number of breaches, government agencies (23%) and schools (23%) topped the charts. Health care (14%), finance (13%) and retail (6%) companies followed.

There were definitely limitations to our study. We're relying on what companies say or what gets reported about their breaches. Anyone familiar with doing forensics on a breach knows that these facts can be hard to pin down with certainty.

Moreover, many companies, especially smaller businesses, are experiencing breaches but not detecting them. Others are detecting them but not reporting them. And those helping companies in this area say there

is a better-than-even chance that sending out a batch of breach letters will not result in press coverage.

What should privacy and security officers take away from this data? Stay vigilant of suspicious activity on the network, patch known vulnerabilities, train employees, keep locking down laptops and flash drives, and beef up your vendor oversight program. And get ready for mandatory breach notifications across the industrialized world.

Jay Cline is a former chief privacy officer at a Fortune 500 company and is now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.