
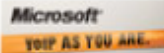


Now you can get the latest technology news & reviews from the trusted editors of eWEEK.com on your handheld device.

mobile.eweek.com

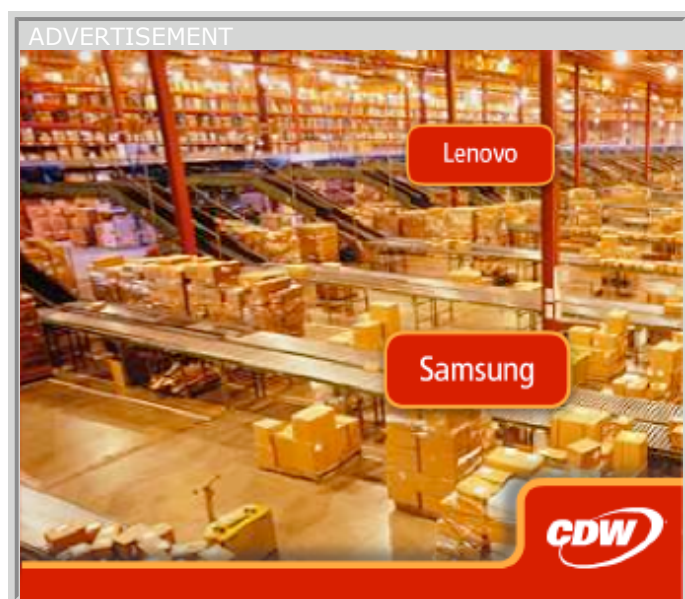
BROUGHT TO YOU BY  SPONSORED BY  YOUR AS YOU ARE.

Data Breaches Cost More Than Ever

November 28, 2007

By Lisa Vaas

The cost of an average data breach is creeping up, but the cost of lost business caused by data breaches is soaring.



A study from the Ponemon Institute—sponsored by encryption software maker PGP and data loss prevention vendor Vontu—shows that the average cost of a data breach has grown 8 percent—to \$197 per data record—since 2006 and 43 percent compared with 2005 costs.

RELATED LINKS

- ▶ [Should We Be Legally Obligated to Fix Vulnerabilities?](#)
- ▶ [Let's Demand Names in Data Fumbles](#)
- ▶ [Police Raid Home of Suspected Botnet Ringleader](#)
- ▶ [Securing Mobile Data](#)
- ▶ [Top of SANS 2007 Internet Threats List: The Gullible](#)

Meanwhile, the loss of business associated with those data breaches is accounting for a much bigger bite of the total cost: It's up 30 percent over 2006, averaging \$4.1 million, or \$128 per record compromised, according to the report, released Nov. 28. Lost business now accounts for 65 percent of

data breach costs, compared to 54 percent in the institute's 2006 study.

The study surveyed the experiences of 35 organizations across an array of 15 industries, each of which has suffered data breaches over the past year that involved from fewer than 4,000 records to more than 125,000 records.

The costs of dealing with a data breach fall into three categories: out-of-pocket expenses such as hiring consultants or lawyers to defend an organization; having public relations personnel devoted full-time to damage control and critical response; and what is called an opportunity cost—lost economic opportunities when customers get annoyed and take their business elsewhere or the costs of attracting new business during the data breach fallout.

[Click here to read more about securing mobile data.](#)

Larry Ponemon, chairman and founder of the Ponemon Institute, told eWEEK that researchers are amazed that the cost of lost business is going up instead of down. "The reason we think that should be the case is that over time, given more and more breaches, people should become immune and be less likely to do something like destroy their credit card with TJX," he said.

On the other hand, customers and partners might expect that companies should have learned by now how to protect sensitive data and could be more harsh in their assessments of organizations post-breach.

The average total cost per reporting company in the institute's survey was more than \$6.3 million per breach and ranged from \$225,000 to almost \$35 million.

Third-party data breaches are also on the rise, and they cost more than internal breaches: Breaches by third-party organizations such as outsourcers, contractors, consultants and business partners were reported by 40 percent of respondents, up from 29 percent in 2006 and 21 percent in 2005. Breaches by third parties averaged \$231 per record.

One example of a third-party breach was disclosed by the Gap in September, after the clothing retailer found that a vendor managing the company's job applicant data lost personal information for some 800,000 job seekers. That third-party vendor in fact violated the terms of the agreement between the two companies by failing to encrypt data on a stolen laptop. That's not surprising, given that some 80 percent of data breaches involve human failing of some sort, the Ponemon Institute has found, with 49 percent of breaches caused by lost devices and an undetermined amount involving failure to hew to security policy.

The only news coming out of the study that might be deemed somewhat positive is that costs associated with a data breach, such as investigation, notification of impacted individuals and services such as free credit monitoring, have decreased 15 percent. That's because businesses are getting well-seasoned when it comes to dealing with multiple breaches: They know how to escalate an incident to upper management, for example. In fact, some of the organizations surveyed have suffered up to 10 breaches, a circumstance that likely reflects the fact that they're better at detecting breaches, Ponemon said, as opposed to the possibility that they haven't learned anything.

Encryption and data loss prevention use increase following a breach: They were the top two technology responses following a data breach.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

Copyright (c) 2008Ziff Davis Enterprise Inc. All Rights Reserved.