Security Breach Costs Jump 30%
November 28, 2007

By Deborah Gage

The cost of recovering from a single data breach now averages $6.3 million-that's up 31 percent since 2006 and nearly 90 percent since 2005, according to the Ponemon Institute, which studies privacy and information management.

Two-thirds of that cost is spent recovering business that's lost after a breach, a cost that has risen 30 percent since last year. More customers stop doing business with a company after their information is exposed, and it's getting more expensive to replace them.

"As consumers and end users get more educated, I think there's less tolerance," says John Dasher, the director of product management for PGP, which, along with Vontu, co-sponsored the Ponemon study. Companies known to have suffered a breach were contacted by Ponemon, and 35 agreed to respond.

The companies surveyed were from 16 industries and lost anywhere from 4,000 to 125,000 records. They spent an average of $197 per lost record investigating the breach, notifying customers, restoring security infrastructures and recovering lost business.

Breaches by third parties-outsourcers or members of a company's supply chain-were the second biggest cause of security compromises and are more expensive. Companies spent an average of $231 per lost record on third-party breaches compared to $171 per lost record in 2006.

The only costs that got cheaper were those associated with investigating breaches and notifying customers. Notification costs were down 40 percent, to $15 per customer, suggesting that companies are learning from each other, Dasher says. Also, more than 30 states now have laws requiring companies to notify customers which tend to guide companies' behavior.

Dasher says when PGP sells its software, which encrypts data, more people inside a company are now involved in purchasing it. CEOs, presidents, chief operating officers, legal, and marketing departments all want a say, in addition to the usual folks in information technology, "especially if your function touches customer or employee data," he says. "They all have different concerns." Marketing, for example, doesn't want to spend precious dollars restoring a damaged brand.

But data encryption software doesn't protect against breaches if it's not properly deployed, Dasher says. And companies should choose their business partners carefully. One company which did encrypt its data lost it to an accounting firm which loaded it onto a laptop, which

was stolen from a car.

This is Ponemon's third survey of data breach costs since 2005. Lost laptops are a growing problem and now account for 49 percent of breaches, compared to 35 percent in 2006. Third party breaches were down to 16 percent of breaches, compared to 21 percent in 2006, although more companies—40 percent—reported third party breaches this year.