

# Rising cost of data breaches fuel security spending

By Shamus McGillicuddy, News Writer  
15 Nov 2006 | SearchSMB.com

Organizations are using the rising (and documented) cost of lax security practices to justify investment in data security.

Companies have long understood the importance of information security, but until recently most security investments have been at the perimeter. Justifying additional investments aimed at securing data as it moves through an organization has been a challenge.

But a new benchmark study by Elk Rapids, Mich.-based [Ponemon Institute LLC](#) found the cost of dealing with a data breach rose this year by 30% to \$4.8 million.

For many budget-conscious midmarket CIOs, numbers like this can easily justify an investment in solutions aimed at securing data.

The cost of a breach was derived from an average cost of \$182 per lost customer record and an average number of 26,300 lost customer records per breach.

For his second annual study, institute CEO and chairman Larry Ponemon said he interviewed 31 companies that had reported losing sensitive customer data last year.

Ponemon divided the total cost of data breaches into three component costs. Direct incremental costs, such as legal fees, audit and accounting fees, call center expenses, notification letters, phone calls and email rose 8% to \$54 per lost customer record. Lost productivity, with employees and contractors diverted from other tasks to deal with these activities, rose 100% to \$30 per record.

The biggest impact was felt in the third category: lost customer opportunities cost companies \$98 per lost record last year, an increase of 31%. These lost opportunities included turnover of existing customers and increased difficulty in acquiring new customers.

"When you basically look at a \$4 or \$5 million cost per breach and then look at the solutions that are available, it's usually a cost-positive solution [such as encryption or automated data detection]," Ponemon said. "Some implementations can be hundreds of thousands of dollars, but some can be millions, and there's not as much return on investment. But then again, these breaches can happen over and over again."

Kit Robinson, director of corporate communications at Vontu Corp., said, "The history of IT security has focused on perimeter defense against outside attacks from hackers, spam,

viruses. It's only been relatively recently that people started to look inside the organization and recognized that there is a huge vulnerability in terms of an insider threat. Most of that is innocent -- good people doing bad things." San Francisco-based Vontu, a data loss prevention vendor, sponsored the Ponemon study.

During the past few years, beginning with the [California Security Breach Notification Law in 2003](#), more than half the states in the country have enacted privacy laws that require companies to notify their customers when sensitive customer data is lost or stolen. Before that, companies had almost no incentive to reveal that they lost this data, Ponemon said. And thus, they had no incentive to spend money to correct the problem.

Chris Hoofnagle, a senior fellow with the [Berkeley Center for Law & Technology](#), said security breach notification laws have put data security "on the balance sheet."

"There desperately needed to be metrics for ROI in security," Hoofnagle said. "It was really easy to stay out of the newspapers prior to the California law, and now it's impossible."

"Some of the CIOs I talk to, when they're trying to justify a security investment, I will make a fake press release with the name of their company at the top of it, with a headline that says the company has lost 1 million records and the FTC is set to investigate. It's to convey that security breaches are now unacceptable."

However, Hoofnagle said he was surprised that the costs of data breaches are rising. He assumed companies would see high up-front costs that would decline over time as they develop processes and acquire products for dealing with the issue.

"It could be that companies are just now becoming conscious of it," Hoofnagle said. "I've found that it's not uncommon, as a privacy consultant, to visit a client and find that they do not know about an important privacy law that they need to comply with."

Many companies don't improve their data security practices until after they suffer a breach. Ponemon said companies better assess themselves now because customers won't get any more forgiving.

Ponemon said customers don't just consider terminating their relationships with companies that lose their data. They also change the way they do business with these offending companies. For instance, customers will stop doing their banking online and go to bank branches instead. This costs banks money.

"The general belief is that most people thought actual customer churn rates would go down," Ponemon said. "As people continued to get these data breach notices, no one would read them anymore. Most people would be numb. But it doesn't seem to be true."