SearchDataManagement.com Pocket E-Guide

Data Breach Dangers: Learn to How to Protect Data and Lower Security Spending

While most organizations today acknowledge the importance of information security, justifying additional investments aimed at securing data as it moves through an organization has proved to be a challenge. At the same time, the cost of dealing with a data breach and lost customer records per breach continues to rise. Read this E-Guide and discover three specific actions for your company to take to protect and promote brand trust. Explore how important factors such as stock performance and customer loyalty are directly affected by security breaches.

TechTarget
The Technology Media
ROI Experts

SearchDataManagement.com Pocket E-Guide

Data Breach Dangers: Learn to How to Protect Data and Lower Security Spending

Table of Contents:

Data breach dangers loom, companies remain unprepared

Barney Beal, News Editor

Personal data protection has become a major concern in recent years as high-profile data breaches, coupled with a rise in identity theft, have left consumers nervous about who is handling their information.

The names alone should keep anyone worried about their corporate brand up at night -- ChoicePoint, LexisNexis, Marriott, Bank of America, the U.S. Department of Veterans Affairs -- all have found themselves in the headlines when customer data they were responsible for went missing. It is becoming apparent that data breaches are not just a problem for IT and customer service but should be a major concern for marketers as well.

Yet while marketers see information security as an important marketing and business concern, few are taking steps to prepare for it, according to a recent survey from the CMO Council, a private, nonprofit research firm.

"Obviously, marketers and business people are concerned about security," said Scott Van Camp, editorial director with the Palo Alto, Calif.-based organization. "We feel perhaps they could do a lot more to prepare. There's a disconnect there."

For example, 76% of marketing executives surveyed believe security breaches negatively impact company branding. Yet 60% said that security has not become a significant theme in their company's messaging and marketing communications and only 29% said their company has a crisis containment plan for security breaches and failures. Another 27% don't even know if such a plan exists.

The CMO Council research, sponsored by Symantec and Factiva, surveyed more than 2,000 consumers and conducted in-depth interviews with 25 leading marketing executives.

According to the Federal Trade Commission, more than 52 million account records were placed in jeopardy last year because of security breaches, leading to 9 million Americans becoming the victims of identity theft, with losses adding up to $54 billion. There have been an additional 30 million cases of compromised data in 2006.

However, many marketers remain unconvinced that a data breach significantly affects the bottom line.

"In about a third of our interviews, at some point marketers said, 'I have no evidence that these breaches erode brand trust,'" Van Camp said. "A couple said point blank, 'I don't think I'll lose that many customers.'"

Research is emerging, however, to show that a data breach can be quite costly indeed. A privacy study by the Tucson, Ariz.-based Ponemon Institute found that costs for a single data breach can range from $5 million to $50 million and average $140 per lost customer record.

Security breaches can also directly affect stock performance, according to researchers at Emory University's Zymand School of Brand Science. They found that a company loses, on average, 0.63% to 2.1% value in stock price when a data breach is reported.

The CMO Council survey also found that consumers are worried and agitated. Of the 2,000 consumers surveyed, 65% said they have experienced some kind of computer security problem, and more than half would either strongly consider taking or definitely take their business elsewhere if their personal information were compromised.

The study recommends three actions for companies to take to protect and promote brand trust.

"First and foremost, they need to begin establishing good strong policies for customer data right from the outset," Van Camp said. "They need to start with what they do with security inside the company -- opt-in programs and strong policies internally."

Companies should also have a containment plan in place that deals not only with actions but with marketing response in the event of a breach.

"Being up front is probably the No. 1 thing a company could do," Van Camp said. "A quick measured response and then a plan of restitution."

Finally, companies should be prepared to offer some sort of restitution or monitoring, be it a dedicated Web site or an offer of free credit monitoring.

Data breach costs rise, drive security spending

Shamus McGillicuddy, News Writer

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."

Resources from IBM

[Data privacy best practices: time to take action!]

[Anatomy of a Database Archiving Project]

[Application Retirement: Enterprise Data Management Strategies for Decommissioning Projects]

About IBM:
Companies now have an opportunity to manage data smarter. To have continuous control of their application data so they can succeed and respond to the ever-evolving needs and demands of the business. Having one truly integrated platform to manage accelerating data growth—as well as manage data privacy — will enable companies to maximize business value. IBM Integrated Data Management solutions deliver this.