This story appeared on CIO Magazine at
http://www.cio.com/article/479101/Costs_of_a_Data_Breach_Can_You_Afford_6.65_Million_
2/4/09

Costs of a Data Breach: Can You Afford $6.65 Million?
By: Dr. Larry Ponemon, Ponemon Institute, CIO

Affixing a dollar cost to a problem has immense benefit, and The Ponemon Institute goes to great lengths to arrive at the figures for its Annual Cost of a Data Breach Study.

We painstakingly analyzed the financial impact a data breach has on a company by examining 43 different companies from a cross section of industries, all of which experienced a significant data breach affecting a range of data records representative of the norm. And knowing that a data breach may cost your company $6.65 million dollars may be all the information that is needed for a company to assign an appropriate budget to those tasked with information security.

In 2008 the average total cost of a data breach was $6.65 million, up from $6.35 million last year and $4.54 in 2005. In 2008, the per-victim cost of a data breach was $202, up from $197 in 2007, and from $138 when the study was launched in 2005. Breaches involving a third party to which data had been outsourced bore a per-victim cost of $231, whereas self contained breaches bore a per-victim cost of $179. Breaches that were the result of a malicious act bore a per-victim cost of $225, whereas breaches that were the result of negligence bore a per-victim cost of $199. Breaches that were the result of a lost of stolen laptop computer bore a per-victim cost of $249, whereas breaches that did not involve a lost or stolen laptop computer bore a per-victim cost of $177. If the data breach was a first-time event for the company the per victim cost was $243, but if the company had experienced a breach previously the per victim cost was $192.

The simple conclusion to these numbers is clear: the financial impact for a company that experiences a data breach is significant and rising. That finding alone may be alarming, but it seems to merely quantify what most people already knew to be true. The "wow" factor comes when you realize that we haven't simply identified the cost of an inevitable outcome, as if to tell the world, "buckle up and brace for impact," but we've shown that companies well have the means to significantly diminish their loss if and when a breach occurs.

Consider the last data point on our list. First-time data breaches cost companies $51 more per victim than for companies who had already learned the hard lessons of data breach. That means the previous experience resulted in a smarter, more efficient response the second time around. Last year the Ponemon Institute began working with risk management firm WillisHRH on a data breach response tracking system called the Privacy Breach Index. We use the PBI to analyze the methods and strategies used by companies when responding to a breach, and the outcome of the response, to create best practices so other organizations don't have to learn from their own experience.

Looking at other data points, given that the per victim cost of a data breach involving outsourced data was $52 more than when no vendor was involved, it stands to reason that a better vendor management program might help reduce risk and cost. Stricter policies for and better enforcement of mobile data security might help to reduce the risk and impact of a data breach resulting from a lost or stolen laptop computer or other mobile device. More efficient data governance could go a long way toward reducing the cost of a breach by preventing unauthorized or improper access to data. These are just some of the conclusions we reach based on a superficial look at the study's results, but as we dive deeper into the data and look at other factors, our focus becomes sharper and our reaction more informed, allowing us to apply more specific measures to information management, security, and compliance.

Examples here involve the impact of lost business resulting from a data breach. This year, lost business costs rose to a level 38 percent higher than in 2005. What's more, healthcare and financial services organizations experienced much higher abnormal customer loss—6.5 percent and 5.5 percent respectively—when compared with retail and consumer products organizations, whose churn rates were found to be 1.5 percent and 3.6 percent respectively. The significant difference in these rates of customer loss can be explained in one word: trust. Violate a consumer's trust and they are more likely to walk, and that likelihood increases when the breach involves an organization in which the consumer has placed a great deal of trust.

What do I mean? When a consumer chooses to do business with a financial services or healthcare organization, they tend to conduct more due diligence than when they walk through the doors of a department store to buy a shirt or a pair of shoes. A retail purchase is a simple transaction, but banking and healthcare requires entrusting an individual or organization with a great deal of highly sensitive information. Violate that trust and the customer may be more inclined to look for a new relationship. This is especially evident when the consumer receives multiple breach notifications from such an organization.

The risk of a data breach incident is real and ever present. The Ponemon Institute agrees with the belief that a data breach is not a matter of if, but when, but we also strongly believe that there is a body of knowledge that can be used to understand the issues and consequences of a data breach, and that forewarned is forearmed. By acting in advance, companies can do much to diminish the likelihood of a data breach, and to lessen the effects should one occur.

Dr. Larry Ponemon is founder and chairman of the Ponemon Institute, a think tank dedicated to understanding and advancing responsible information and privacy management practices in business and government through independent research. Ponemon Institute research, expertise, and thought leadership is used to educate private and public sector organization on privacy and data protection practices in a variety of industries. The Annual Cost of a Data Breach Study is an independent research report conducted by the Ponemon Institute and underwritten by PGP Corporation, a global provider of email and enterprise data encryption products.