



## 2006 Annual Study: Cost of a Data Breach

Understanding Financial Impact, Customer Turnover,  
and Preventative Solutions

---

PGP® Research Study – Executive Summary:

A study summarizing the actual costs incurred by 31 organizations that lost confidential customer information and had a regulatory requirement to publicly notify affected individuals.

Benchmark research conducted by  
**Ponemon Institute, LLC**



October 2006



## Executive Summary

Following is a summary of The Ponemon Institute's "2006 Annual Study: Cost of a Data Breach". To download the full report, please visit [www.expertsagreepgp.com](http://www.expertsagreepgp.com).

### Customer Notification Requirements

Regulations in more than half of all U.S. states require that customers be notified if their confidential or personal data has been lost, stolen, or compromised. The only "safe harbor" exception, exempting organizations from the notification requirement, is for data held in an encrypted form when lost. When a regulatory breach occurs, organizations must notify all affected customers, attempt to minimize downstream brand consequences, and put solutions in place to prevent a recurrence.

The frequency of lost customer information is on the increase. Since February 2005, the Privacy Rights Clearinghouse has identified more than 93 million records of U.S. residents that have been exposed due to security breaches. New disclosures occur every week, and websites track these for the media and interested parties ([www.privacyrights.org/ar/chrondatabreaches.htm](http://www.privacyrights.org/ar/chrondatabreaches.htm)).

### 2006 Annual Survey: Cost of a Data Breach

This 2006 Ponemon Institute benchmark study, sponsored by Vontu, Inc., and PGP Corporation, examines the costs incurred by 31 companies after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the second annual survey of this issue; the first survey was published in November 2005 and is available on the PGP website (registration required): [http://www.pgp.com/downloads/research\\_reports/index.html](http://www.pgp.com/downloads/research_reports/index.html).

Breaches included in the survey ranged from 2,500 records to 263,000 records from 15 different industry sectors and cover the costs resulting from 815,000 compromised customer records.

Among the study's key findings:

- **Total costs:** averaged \$182 per lost customer record, an increase of 30 percent over 2005 results. The average total cost per reporting company was \$4.8 million per breach and ranged from \$226,000 to \$22 million.
- **Direct incremental costs:** averaged \$54 per lost record, an 8 percent increase over 2005 results for unbudgeted, out-of-pocket spending. Includes free or discounted services offered; notification letters, phone calls, and emails; legal, audit and accounting fees; call center expenses; public and investor relations; and other costs.
- **Lost productivity costs:** averaged \$30 per lost record, an increase of 100 percent over 2005 results, for lost employee or contractor time and productivity diverted from other tasks.
- **Customer opportunity costs:** averaged \$98 per lost record, an increase of 31 percent over 2005 results, covering turnover of existing customers and increased difficulty in acquiring new customers. Customer turnover averaged 2 percent and ranged as high as 7 percent.

Other findings:

- **Breach location:** Almost 30 percent of all reported breaches originated with external partners, consultants, outsourcers, or contractors.
- **Breach source:** More than 90 percent of all breaches were in digital form—primarily laptops, electronic backups, and hacked and attacked systems.
- **Groups affected:** Costs were borne primarily by Marketing (55 percent for customer turnover), Customer Support (34 percent for emails, call center, letters), and Legal, Risk Management, and Audit (11 percent for investigations). IT had no direct costs other than to put subsequent preventative measures in place.
- **IT preventative measures:** The cost of new preventative measures averaged 4 percent of the total breach cost, or \$180,000 on average. Not all respondents put electronic protections in place.
- **Cost increases:** 75 percent of the increased recovery costs reported between 2005 and 2006 were due to increased expenditures on notification phone calls, offers of free or discounted services, and increased estimates of customer turnover.
- **Response responsibility:** IT executives or IT security were responsible for breach response in 53 percent of incidents. Others responsible included the Business Unit (7 percent), Privacy Officer (7 percent), and Compliance Officer (3 percent). No Single Group (30 percent) was a frequent reply to the question of who was responsible for the breach response.
- **Total cost reported:** The total cost reported by the 31 respondents was \$148 million. At \$182 per record lost, the total cost of 93 million compromised records reported by the Privacy Clearinghouse is in the billions.

## National Consumer Survey on Data Security Breach Notification

In a related survey of 51,000 adult consumers conducted by The Ponemon Institute in 2005, consumers were asked if they had received breach notifications from companies.

- 12 percent of 9,000 respondents had received a notification that their information had been lost
- Extrapolated to the U.S. population, 23 million adults may have received such notifications

Consumers reacted extremely negatively to these notifications and to the companies that mishandled their private and confidential information: almost 60 percent terminated or considered terminating their relationship with the offending company.

Affected individuals created significant damage to corporate reputation, corporate brand, and customer retention:

- Almost 20 percent of respondents terminated their relationship with the company
- A further 40 percent were considering terminating their relationship
- Only 14 percent were “not concerned”

## Download the Full Report

To download the full report, please visit [www.expertsagreepgp.com](http://www.expertsagreepgp.com).

## About The Ponemon Institute

The Ponemon Institute© is dedicated to advancing ethical information and privacy management practices in business and government. The Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

Dr. Larry Ponemon is the chairman and founder of the Ponemon Institute. He is also a founding member of the Unisys Security Leadership Institute and an Adjunct Professor of Ethics & Privacy at Carnegie Mellon University's CIO Institute. Dr. Ponemon is a critically acclaimed author, lecturer, spokesman, and pioneer in the development of privacy auditing, privacy risk management, and the ethical information management process.

Previously, Dr. Ponemon was the CEO of the Privacy Council and the Global Managing Partner for Compliance Risk Management at PricewaterhouseCoopers (where he founded the privacy practice). Prior to joining PricewaterhouseCoopers, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG and as the Executive Director of the KPMG Business Ethics Institute. Dr. Ponemon holds a Ph.D. from Union College, attended the Doctoral Program in System Sciences at Carnegie-Mellon University, and has a Masters degree from Harvard University as well as a Bachelors degree from the University of Arizona. Contact The Ponemon Institute at [www.ponemon.org](http://www.ponemon.org) or +1 800 887 3118.

## About PGP Corporation

PGP Corporation, a global security software company, is the leader in email and data encryption. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. The platform enables organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, network storage, FTP and bulk data transfers, and backups.

PGP solutions are used by more than 80,000 enterprises, businesses, and governments worldwide, including 95 percent of the Fortune® 100, 75 percent of the Fortune® Global 100, 76 percent of the German DAX Index, and 51 percent of the U.K. FTSE 100 Index. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at <http://www.pgp.com/> or +1 650 319 9000.

## About Vontu, Inc.

Vontu is the leading provider of Data Loss Prevention solutions for both data at rest and data in motion. Vontu allows organizations to discover and protect exposed confidential information, monitor all network traffic, block select email, FTP and web communications, and automatically enforce data loss prevention policies. By reducing the frequency and severity of both inadvertent and malicious data loss incidents, Vontu helps organizations ensure

public confidence, reduce compliance risk and protect competitive advantage. Vontu customers include Fortune 500 companies in financial services, insurance, high technology, retail, telecommunications, manufacturing, media, and healthcare, as well as state and federal government agencies. Vontu has received numerous awards, including *SC Magazine's* 2006 U.S. Excellence Award for "Best Enterprise Security Solution" and Global Award for "Best New Security Solution," as well as IDG's *InfoWorld* 2006 Technology of the Year Award for "Best Insider Threat Defense." For more information, please visit [www.vontu.com](http://www.vontu.com).

© 2007 PGP Corporation

Approved for redistribution by The Ponemon Institute.

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of PGP Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.