2008 Annual Study: Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventitive Solutions

Executive Summary:

This 2008 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the costs incurred by 43 organizations 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 fourth annual survey of this issue.

Breaches included in the survey ranged from less than 4,200 records to more than 113,000 records from 17 different industry sectors.

Benchmark research conducted by

Ponemon Institute, LLC

February 2009

Table of Contents

Executive Summary

While high profile data breaches such as the TJX breach of January 2007 are finally seeing perpetrators indicted and convicted, new, potentially even larger breaches, such as the January 2009 credit card breach notification by Heartland Payment Systems, are coming to light. Fear of a breach has been driving the discussion on whether the President of the United States of America should be allowed to carry a BlackBerry®. From large corporations to individual users, protecting individual information remains paramount as the cost to an organization that loses personal information continues to rise.

First conducted over four years ago, our initial study established objective methods for quantifying specific activities that result in direct, indirect and opportunity costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law or policy.

Our current analysis of the actual data breach experiences of 43 U.S. companies from 17 different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after the fact (ex-post) response. We also analyze the economic impact of lost or diminished customer trust and confidence, measured by customer churn or turnover rates.

Utilizing activity-based costing, our methods capture information about direct expenses such as engaging forensic experts, outsourced hotline support, free credit monitoring subscriptions, and discounts for future products and services. We also capture indirect costs such as in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

Data Breach Notification Requirements

Regulations in 44 states, the District of Columbia, Puerto Rico and the Virgin Islands require that individuals (customers, employees, citizens, students, alumni, etc.) be notified if their confidential or personal data has been lost, stolen, or compromised.[1] When a regulatory breach occurs, organizations must notify all affected individuals, attempt to minimize downstream brand consequences, and put solutions in place to prevent a recurrence. Although the specific conditions for notification vary by state, organizations may not be required to notify individuals when the breached data is protected by encryption or the breach was stopped before information was wrongfully acquired.

While breach notification laws increased within the United States as expected so did the total number of records containing sensitive personal information involved in security breaches in the U.S. Since January 2005, the Privacy Rights Clearinghouse has identified more than 250 million records of U.S. residents that have been exposed due to security breaches.[2]

[1] More information on state laws is available from the National Conference of State Legislatures at http://www.ncsl.org/programs/lis/cip/priv/breach.htm

[2] See the Privacy Rights Clearinghouse website http://www.privacyrights.org/ for more details about this ongoing data breach tracking survey

2008 Annual Study: Cost of a Data Breach

This 2008 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the costs incurred by 43 organizations 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 fourth annual survey of this issue.

Breaches included in the survey ranged from less than 4,200 records to more than 113,000 records from 17 different industry sectors.

Among the study's key findings:

- **Total costs continue to increase:** The total average costs of a data breach grew to $202 per record compromised, an increase of 2.5 percent since 2007 ($197 per record) and 11 percent compared to 2006 ($182 per record). Breaches are costly events for an organization; the average total cost per reporting company was more than $6.6 million per breach (up from $6.3 million in 2007 and $4.7 million in 2006) and ranged from $613,000 to almost $32 million.
- **Cost of lost business continues to carry the highest impact:** The cost of lost business continued to be the most costly effect of a breach averaging $4.59 million or $139 per record compromised. Lost business now accounts for 69 percent of data breach costs, up from 65 percent in 2007, compared to 54 percent in the 2006 study.
- **Third-party data breaches increase, and cost more:** Breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 44 percent of respondents, up from 40 percent in 2007, up from 29 percent in 2006 and 21 percent in 2005. Per-victim cost for third-party flubs is $52 higher (e.g., $231 vs. $179) than if the breach is internally caused.
- **"First timers" cost more, repeat breaches continue:** Data breaches experienced by "first timers" are more expensive than those experienced by organizations that have had previous data breaches. Per-victim cost for a first time data breach is $243 vs. $192 for experienced companies. More than 84% of all cases in this year's study involved organizations that had more than one major data breach.
- **Training and awareness programs lead companies' efforts to prevent future breaches, according to 53% of respondents**. Forty-nine percent are creating additional manual procedures and controls. Of the technology options, 44% of companies have expanded their use of encryption technologies, followed by identity and access management solutions to prevent future data breaches.

Additional study findings:

- **Healthcare and Financial Services suffer highest customer loss:** Healthcare and financial services companies have the highest average rate of churn – 6.5% and 5.5%, respectively. High churn rates reflect the fact that these industries manage and collect consumers' most sensitive data. Additionally the average cost of a healthcare breach ($282) is more than twice that of an average retail breach ($131). Thus, another sign that consumers may have a higher expectation for the protection and privacy of their healthcare records.
- **Increased customer churn rates help drive lost business costs higher:** In 2008, the average resulting abnormal customer churn rate was 3.6 percent, an increase from 2.67 in 2007 and 2.01 percent in 2006. Between 2005 and 2008, this one cost component grew by more than $64 on a per-victim basis, or a 38% overall increase.

- **Insider negligence highest cause of breaches:** Over 88% of all cases this year involved incidents resulting from negligence. Per-victim cost for data breaches involving negligence cost $199 per record vs. malicious acts costing $225 per record.
- **Other data breach costs stabilize or slightly decrease year over year:** The most significant cost decrease concerns ex-post response, which implies that organizations are becoming more cost effective in their management of the data breach. In contrast, consulting, legal defense and, as mentioned previously, lost customer business have increased in this year's study.

Conclusions

Over 5 years since California Senate Bill 1386 first mandated data breach notification, the cost of a data breach continues to rise. Increasingly more organizations are losing business as a result of a breach, with 69 percent of a breach cost attributed to lost business. In these very tough economic times, businesses cannot afford to lose customers as a result of breach. Although new data breaches are reported each week, and seem to be getting larger, consumers have not become immune. While organizations have learned how to respond to a breach more cost-effectively, customers are increasingly prone to terminate their business relationship due to lost data, producing consistently higher abnormal churn rates.

This finding reinforces the message delivered by leading enterprise IT managers and industry analysts that organizations must focus on proactively protecting their data instead of relying exclusively on written policies, procedures, and training.

The survey reveals:

- Trust may be intangible and hard to quantify, but the result of breaking that trust is clear as the cost of lost business represents 69 percent of the total cost of a data breach.
- Given both the rise in incidents where third parties are responsible and the cost disparity between in-house and third-party breaches, organizations should closely evaluate the enterprise data protection policies and systems used with and by third-party outsourcers or consultants. Small and medium sized businesses will have to pay special attention to this as new "cloud computing" and SaaS infrastructure costs appear attractive yet, custody of data is unclear.
- Organizations that have built their brand on trust have more to lose from a data breach – demonstrated by the higher costs and higher churn for healthcare and financial services compared to an average breach.
- Encryption, identity and access management and data loss prevention solutions top the list of most-frequently named post-breach technology measures being deployed to help avert a future data breach.

As information risk management becomes important across the enterprise, the investment required to prevent a data breach is dwarfed by the resulting costs of a breach. With average breach costs totaling $6.6 million and the source of many breaches (such as laptops and USB flash drives) critical to productivity, the return on investment (ROI) and justification for preventative measures is clear.

Preventative Solutions

Automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Centralized management of encryption solutions allows information protection to be aligned with corporate security policies and regulatory or business-partner mandates. A holistic approach to data protection – at rest, in motion and in use – allows security best practices to be automatically enforced throughout the enterprise.

Next Steps

This fourth annual report enables organizations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology cost of preventing data breaches.

Introduction

Organizations that experience a data breach can suffer the loss of existing customer confidence, damage to their brand and loss of future revenue from new customers that take their business elsewhere. This is especially true of healthcare and financial services companies that are entrusted with some of the most sensitive personal information and therefore pay a higher cost (more than 2 times that of a retail organization) when they experience a breach. Equally damaging are the actual costs associated with legal requirements to notify customers that their private, sensitive, and confidential information has been mishandled.

As of 2008, at least 44 states in the U.S. have passed laws requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts.

Regulations such as California Senate Bill 1386 apply to “any person or business that conducts business in California” even if they are located outside the U.S. In addition, both the U.S. Senate and House of Representatives continue to evaluate federal laws regarding data privacy and breach notification.

Although the specific conditions for notification vary by state, organizations may not be required to notify individuals when:

- The breached data is protected by at least 128-bit encryption
- The breached data elements are not considered “protected”
- The breach was stopped before information was wrongfully acquired
- Other special circumstances (such as national security or law enforcement investigations) exist

When a breach occurs and customers must be notified, what is the corporate cost to recover? The Ponemon Institute and PGP Corporation are pleased to offer the fourth annual survey that quantifies the actual costs incurred by 43 organizations compelled to notify individuals of data privacy breaches. Summarized in this document, the study provides detailed information from responses to questions companies face when responding to a data breach:

- What are the potential legal costs?
- What are industry-average costs resulting from a breach, including the detection, investigation, notification, and possible services offered to affected individuals?
- What are the costs of lost customers and brand damage?
- What are the key trends?
- What measures are taken following a breach that could have been implemented to avert a breach?

Study Overview & Methodology

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

- To complete the study, benchmark surveys were sent to companies known to have experienced a breach involving the loss or theft of personal customer, consumer, or student data during the past year.
- Of that group, 43 companies agreed to participate by completing the survey. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from an actual data loss incident.
- The reported number of individual records breached ranged from less than 4,200 records to more than 113,000 records from companies in 17 different industry sectors.
- The 2008 survey shows that 44 percent of breaches occurred due to external causes, an increase from 40 percent in 2007 and 29 percent in 2006. A third-party breach is defined as a case where a third party (such as professional services, outsourcers, vendors, business partners) was in the possession of the data and responsible for its protection. In comparison, an in-house breach is defined as a case where the protection of data was the responsibility of the organization itself (by an employee or for data on the corporate network, for example).

Table 1 summarizes the 43 study participants by industry and source of data breach:

Industry	Total	Internal Breaches	Third-Party Breaches
Communications	1	1	0
Consumer	2	2	0
Defense	1	0	1
Education	3	2	1
Energy	1	1	0
Entertainment	1	1	0
Financial	8	5	3
Healthcare	4	1	3
Hotel & Leisure	1	1	0
Manufacturing	2	2	0
Marketing	1	1	0
Pharmaceutical	1	0	1
Research	1	0	1
Retail	7	4	3
Services	4	1	3
Technology	3	1	2
Transportation	2	1	1
Totals	**43**	**24**	**19**

Table 1: Study participant sectors and data breach source

Study Methodology

The study looked at core process-related activities associated with a company's detection of and response to a data breach, identifying four "cost centers":

- **Detection or discovery:** Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.
- **Escalation:** Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- **Notification:** Activities that enable the company to notify data subjects with a letter, outbound telephone call, email, or general notice that personal information was lost or stolen.
- **Ex-post response:** Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations to minimize potential harm. Redress activities also include ex-post responses such as credit report monitoring or the reissuing of a new account or credit card.

In addition to the above process-related activities, most companies experience opportunity costs associated with the breach incident, which result from diminished trust or confidence by present and future customers. Accordingly, the research shows that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover or churn rates as well as a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, the study uses a shadow costing method that relies on the "lifetime value" of an average customer as defined for each participating organization. These costs are dependent on two significant components:

- **Turnover or "churn" of existing customers:** The estimated number of customers that will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.
- **Diminished new customer acquisition:** The estimated number of target customers that will not have a relationship with the organization as a consequence of the breach. This number is provided as an annual percentage.

Key Report Findings

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

Data breach costs continue to increase: For 2008, per-record compromised costs continued to increase, growing more than 2.5 percent since 2007 ($197 per record) and 11 percent compared to 2006 ($182 per record).

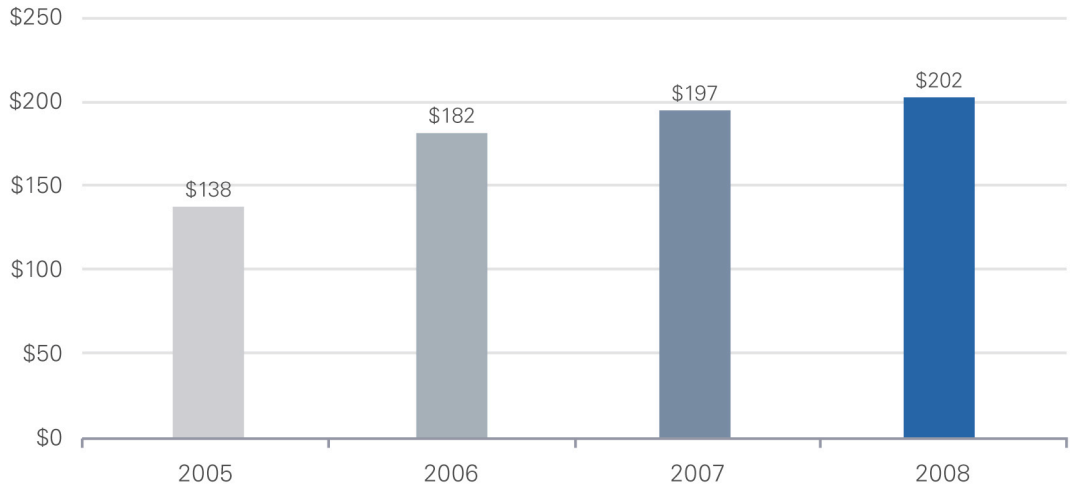


Figure 1: Average per-record cost of a data breach, 2005–2008

Total cost average continues to increase: Breaches are costly events for an organization; the average total cost per reporting company was more than $6.6 million per breach (up from $6.3 million in 2007 and $4.7 million in 2006) and ranged from $613,000 to almost $32 million in 2008.

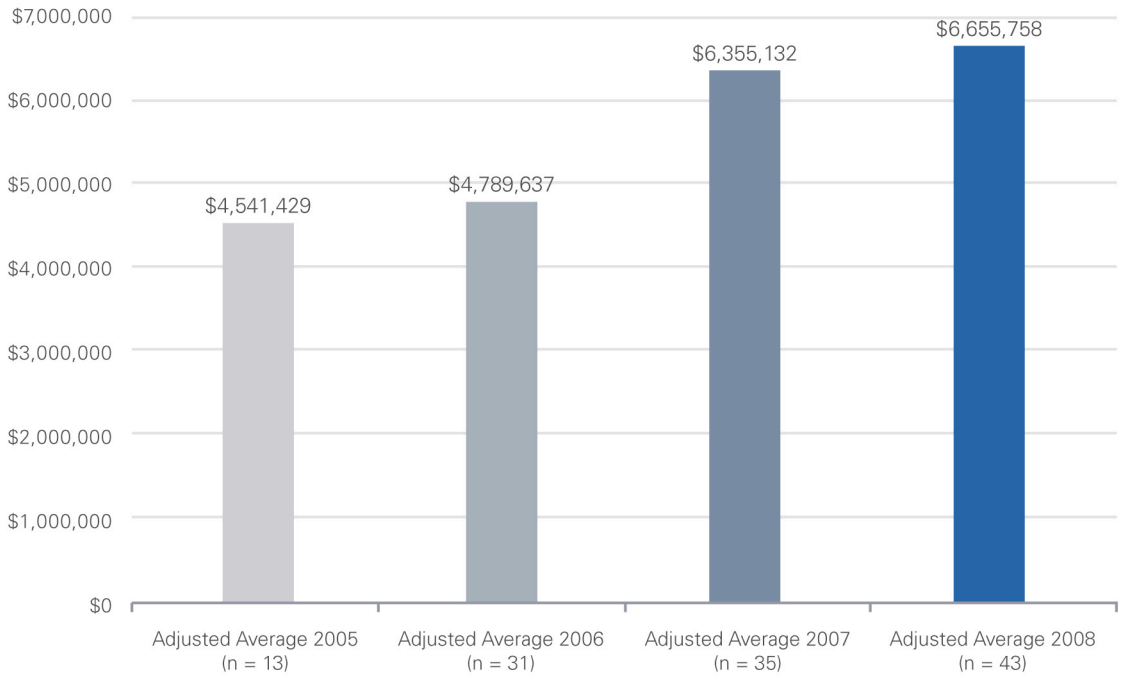


Figure 2: Average organizational costs of a data breach, 2005–2008

Lost business costs continue to grow: Lost business continues to dominate the cost of a data breach, accounting for 69 percent of breach costs, up from 65 percent in 2007, compared to 54 percent in the 2006 study while other costs continue to decline. This finding indicates organizations are better informed and measured in their response to a data breach. At the same time, the growth in lost business costs demonstrates consumers do not take a breach of their trust and privacy lightly and have not become desensitized to the issue.

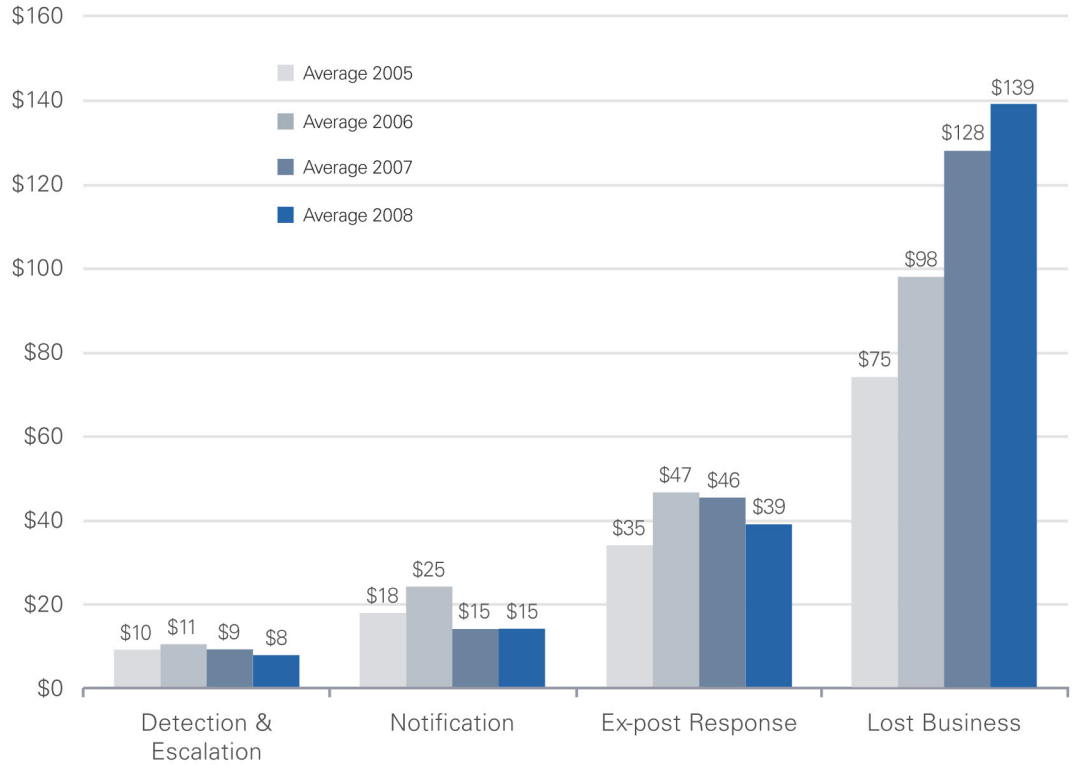


Figure 3: Average cost of data breach on a per-victim basis, 2005–2008

Increasing incidents where third party is responsible; growing costs: Since 2005, the percentage of incidents where a third party such as an outsourcer or consultant was responsible for a data breach has increased from 21 percent in 2005 to 29 percent in 2006 to 40 percent in 2007 to 44 percent in 2008. After experiencing a large gap the difference in cost for a data breach based on responsibility has become increasingly stable. In 2005, the difference in per-record compromised costs between third-party and internal responsibility for a breach was $12. In 2007, that difference grew to $67, and in 2008 that amount is now $52. Third-party outsourcers or consultants often analyze or process large volumes of customer-related information.

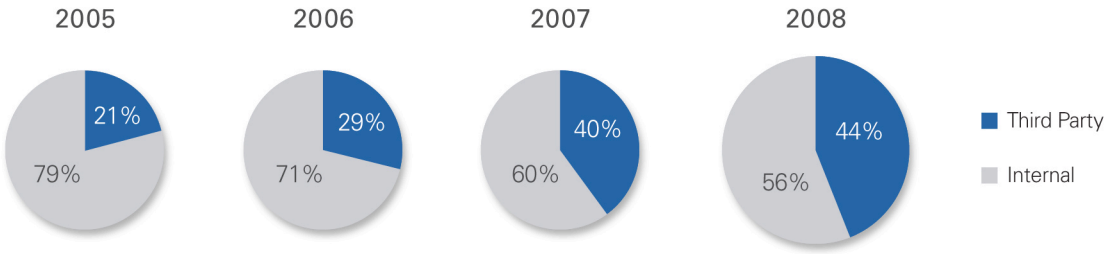


Figure 4: Third-party share of data breaches, 2005–2008

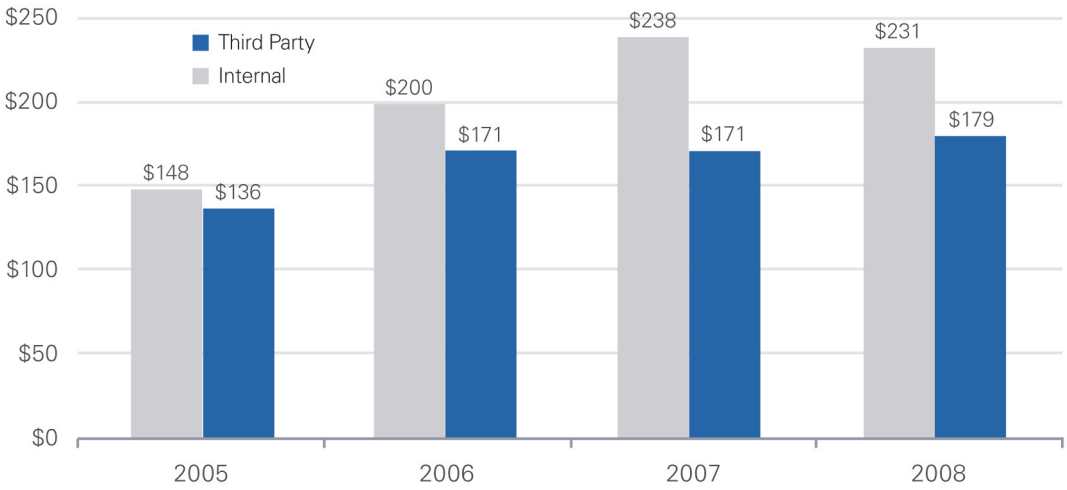


Figure 5: Cost of a breach per record, 2005–2008

"First timers" cost more, repeat breaches continue: Data breaches experienced by "first timers" are more expensive than those experienced by organizations that have had previous data breaches. Per-victim cost for a first time data breach is $243 vs. $192 for experienced companies. More than 84% of all cases in this year's study involved organizations that had more than one major data breach.

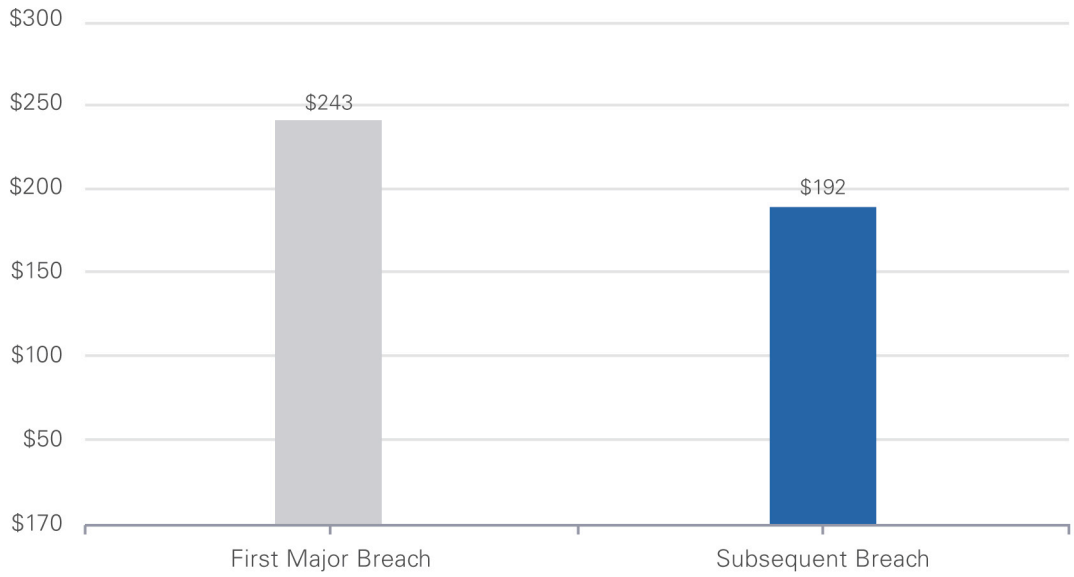


Figure 6: Cost of first time and subsequent data breaches, 2008

Measures implemented following a breach: As the result of a data breach, organizations look at a number of remedies. Encryption is most often relied upon to protect confidential and sensitive data as part of an enterprise data protection strategy.

What preventive measures have been implemented?	Frequency	Total %
Training and awareness programs	23	53%
Additional manual procedures and controls	21	49%
Expanded use of encryption	19	44%
Identity and access management solutions	17	40%
Data loss prevention (DLP) solutions	16	37%
Other system control practices	13	30%
Other manual control practices	12	28%
Endpoint security solutions (including laptop anti-theft)	11	26%
Security certification or audit	9	21%
Security event management systems	8	19%
Strengthening of perimeter controls	7	16%

Table 2: Measures implemented as a result of a data breach

Increased churn rates following a breach: Following a data breach, organizations suffered an average increased customer churn rate of 3.6 percent up from 2.67 percent in 2007 as well up from 2.01 percent in 2006. Five out of the 43 organizations suffered abnormal churn rates of more than 5 percent. The two industries that suffered the highest customer loss or churn were healthcare and financial services where more sensitive personal information is often lost. Greater customer turnover leads to lower revenues and a higher cost of new customer acquisition resulting from the increased marketing expenditures required to recover lost customer business. These increased churn rates demonstrate that customers are concerned about the impact of a data breach – concerned enough to discontinue their business relationship – and have not become desensitized by the frequent reporting of data breach incidents.

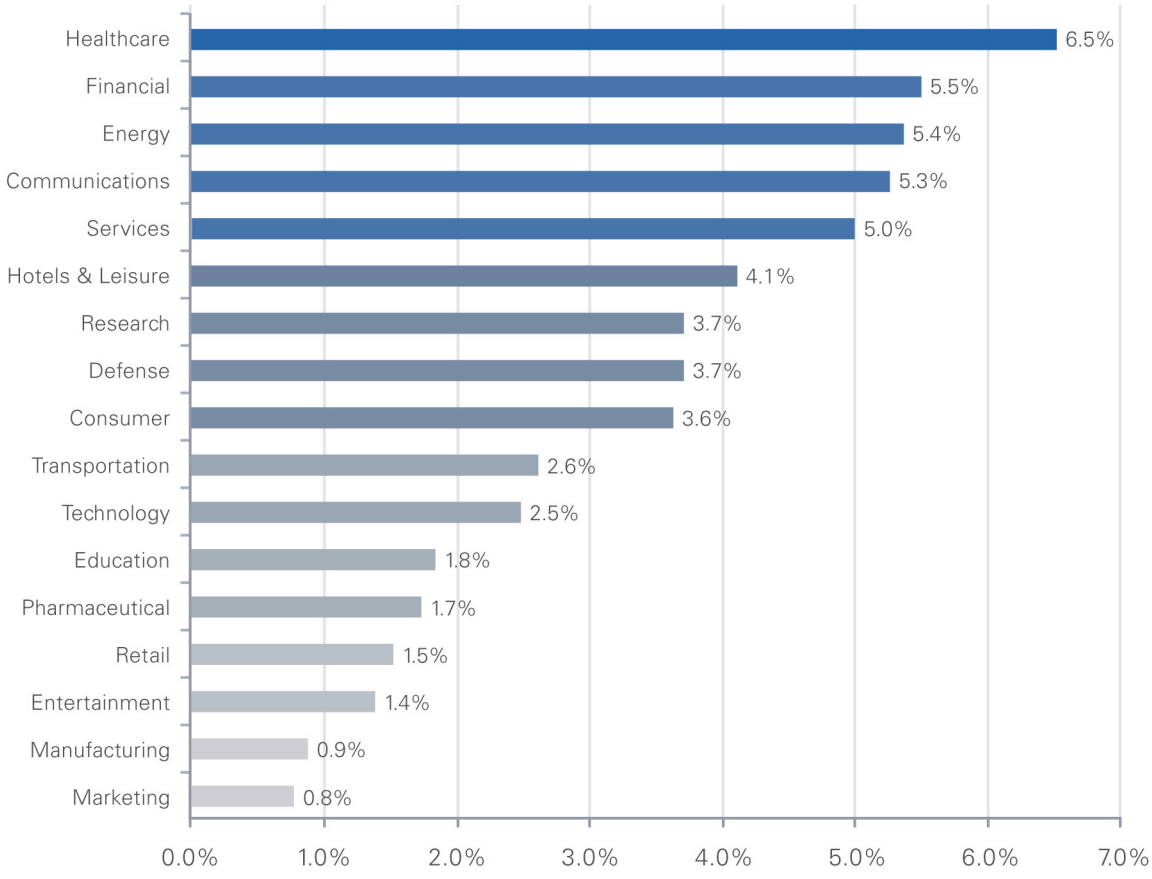


Figure 7: Abnormal churn rates following a data breach incident by industry classification, 2008

Expectations of trust and privacy drive data breach costs higher: The expectation customers have for healthcare firms to treat their confidential data with greater care is illustrated by a 39 percent higher cost of a data breach compared to the survey average of $202. Additionally the cost of a breach to a healthcare company is more than 2 times (115 percent) that of a retail breach, where it appears customers have lower awareness, expectations, or concerns about data privacy.

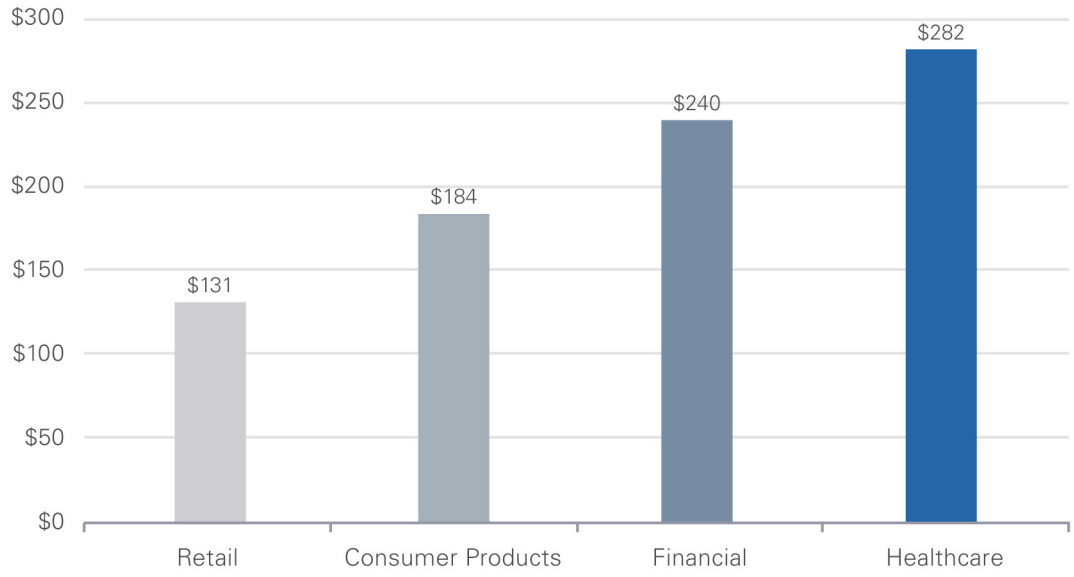


Figure 8: Per capita costs of a breach compared by industry classification, 2008

Insider negligence highest cause of breaches: Over 88% of all cases this year involved incidents resulting from negligence. Per-victim cost for data breaches involving negligence cost $199 per record vs. malicious acts costing $225 per record.

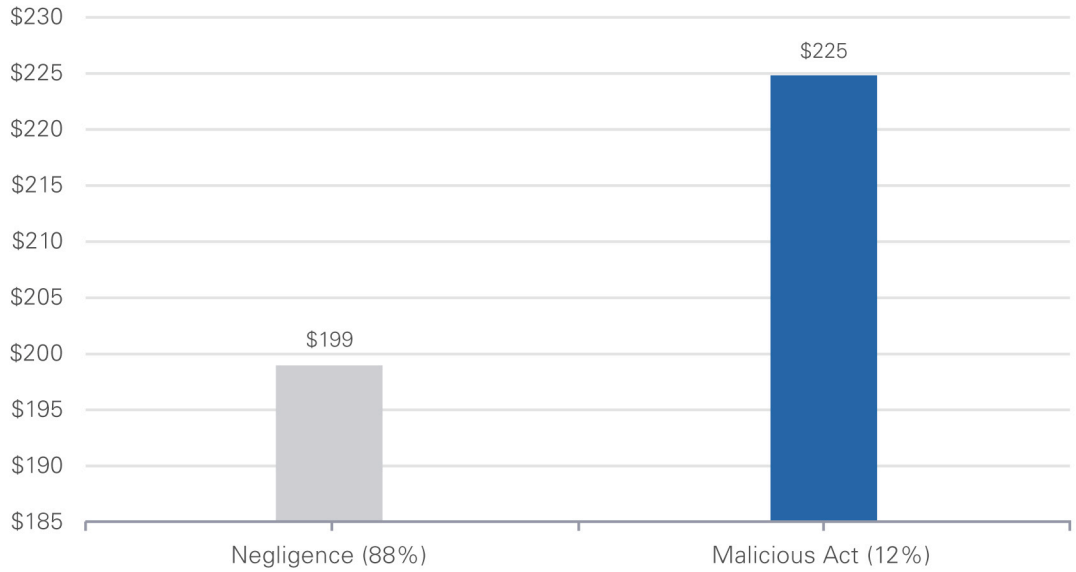


Figure 9: Insider breach cost – negligence vs. malicious, 2008

Costs by category shift: When the survey first started in 2005, the cost of lost business due to churn and customer acquisition accounted for 55 percent of total breach costs. In 2008, these costs climbed to account for 69 percent of total costs. Costs associated with legal defense also grew in 2008, while costs of customer support, notification, and free services such as credit monitoring decreased, signaling that organizations are better informed and measured in their response to a data breach.

Cost changes over four years	2005	2006	2007	2008	Net change
Investigation & forensics	8%	8%	8%	9%	stable
Audit & consulting services	8%	10%	10%	11%	increase
Outbound contact costs	13%	9%	7%	6%	stable
Inbound contact costs	15%	10%	8%	6%	decrease
Public relations/communications	0%	1%	3%	1%	stable
Legal services - defense	5%	6%	8%	9%	increase
Legal services - compliance	3%	3%	3%	1%	stable
Free or discounted services	4%	2%	1%	2%	stable
Credit monitoring services	3%	3%	2%	2%	stable
Lost business (due to churn)	35%	39%	41%	43%	increase
Customer acquisition cost	6%	8%	9%	9%	stable

Table 3: Percent of breach costs by activity cost category, 2005–2008

Note: The cost of lost business includes both lost business due to churn and increased customer acquisition costs.

Cause of a data breach: Lost laptops and system failure are the main causes of data breaches, 35 and 33 percent respectively). Within the classification of systems glitch, respondents cited a number of different issues including software applications development that did not anonymize live customer data, merger/acquisition activities in which customer data was sent to an unrelated law firm by mistake, credit card processing systems infiltrated by malware, social engineering attacks and insecure wireless connectivity among other IT related glitches which caused a breach.

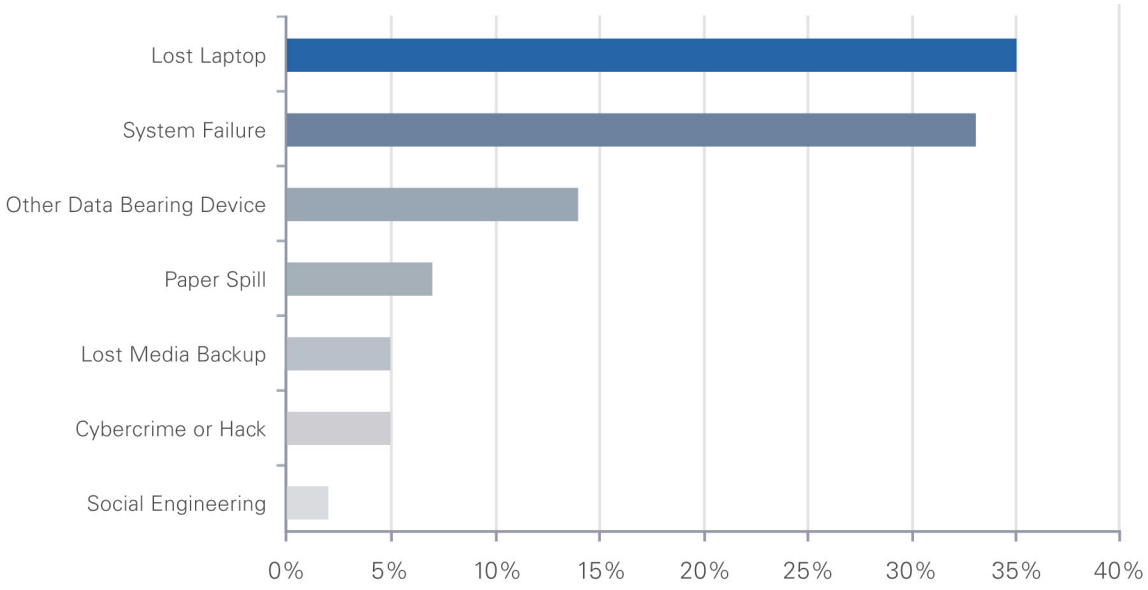


Figure 10: Primary cause of a data breach, 2008

Risk management practices make a difference: The following bar chart shows differences in the per capita cost of data breach for companies that exercise information risk management practices (44%) vs. those that do not (56%). As can be seen, data breach cost appears to be associated with the organization's risk management practices.

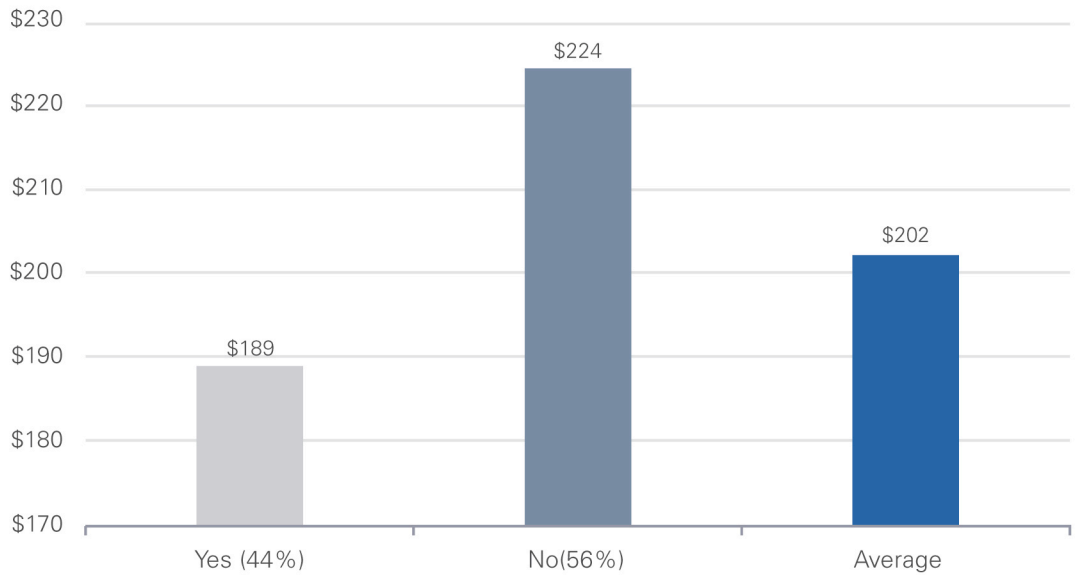


Figure 11: Cost of a data breach when proactive risk management is in use, 2008

Incident response roles and responsibilities: The group most frequently involved in the response to a data breach was the legal department (79 percent of organizations). IT shared responsibility for breach response in 49 percent of organizations. Please note that the bar chart does not sum to 100% because more than one response is permitted, this due to the response to a data breach was a shared responsibility among two or more departments.

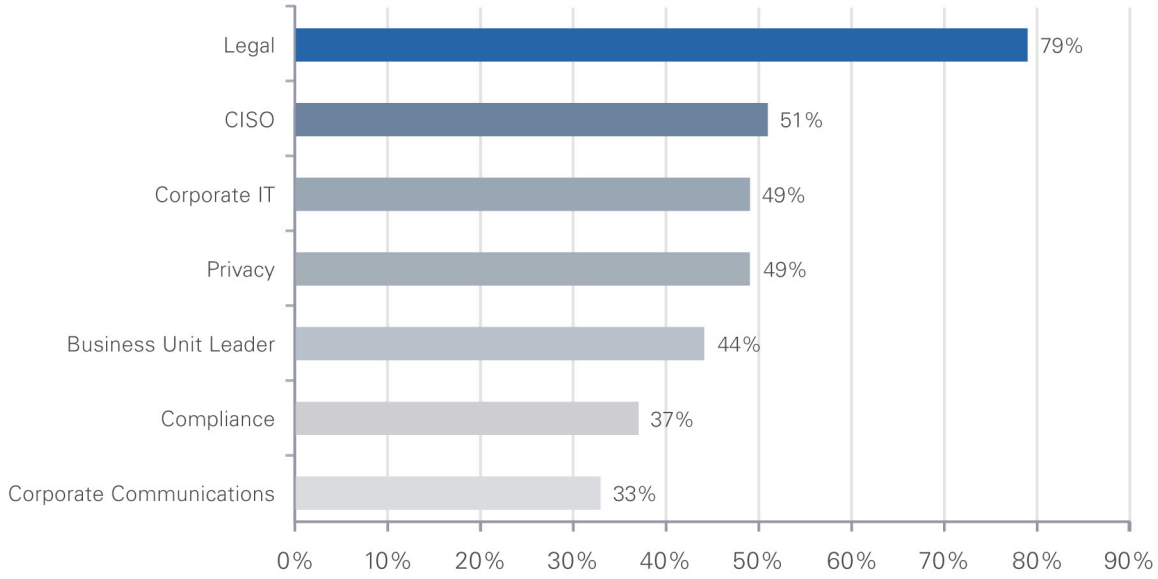


Figure 12: Data breach response shared responsibility, 2008

Report Conclusions

Over 5 years since California Senate Bill 1386 first mandated data breach notification, the cost of a data breach continues to rise. Increasingly more organizations are losing business as a result of a breach, with 69 percent of a breach cost attributed to lost business. In these very tough economic times, businesses cannot afford to lose customers as a result of breach. Although new data breaches are reported each week, and seem to be getting larger, consumers have not become immune. At the same time as organizations have learned how to respond to a breach more cost-effectively, customers are increasingly prone to terminate their business relationship due to lost data, producing consistently higher abnormal churn rates.

This finding reinforces the message delivered by leading enterprise IT managers and industry analysts that organizations must focus on proactively protecting their data instead of relying exclusively on written policies, procedures, and training.

The survey reveals:

- Trust may be intangible and hard to quantify, but the result of breaking that trust is clear as the cost of lost business represent 69 percent of a data breach.
- Given both the rise in incidents where third parties are responsible and the widening cost disparity between in-house and third-party breaches, organizations should closely evaluate the enterprise data protection policies and systems used with and by third-party outsourcers or consultants. Small and medium sized businesses will have to pay special attention to this as new cloud and SaaS infrastructure costs appear attractive, yet custody of data is unclear.
- Organizations that have built their brand on trust have more to lose from a data breach – demonstrated by the higher costs and higher churn for healthcare and financial services compared to an average breach.
- Encryption, identity and access management and data loss prevention solutions top the list of most-frequently named post-breach technology measures being deployed to help avert a future data breach.

As information risk management becomes important across the enterprise, the investment required to prevent a data breach is dwarfed by the resulting costs of a breach. With average breach costs totaling $6.6 million and the source of many breaches (such as laptops and USB flash drives) critical to productivity, the return on investment (ROI) and justification for preventative measures is clear.

Preventative Solutions

Automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Centralized management of encryption solutions allows information protection to be aligned with corporate security policies and regulatory or business-partner mandates. A holistic approach to data protection – at rest, in motion and in use – allows security best practices to be automatically enforced throughout the enterprise.

Next Steps

This fourth annual report enables organizations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology cost of preventing data breaches.

PGP® Solutions

PGP Corporation has developed the PGP® Encryption Platform to protect confidential information from data breaches, regulatory notification requirements, and resulting remediation costs. As part of an enterprise data protection strategy to defend data wherever it goes, this unified platform allows IT organizations a simple, cost-effective way to provide data security to all internal departments and external partners that handle confidential information.

The PGP Encryption Platform allows for central management with automatic operation, email infrastructure transparency, and removal of laptop/desktop, gateway/server, and mobile/wireless encryption silos. It meets business unit requirements for customer privacy, competitive protection, supply chain integrity, and “brand insurance” against public breaches – without disrupting users.

Once deployed, the PGP Encryption Platform is capable of provisioning encryption applications in a combination of gateway and endpoint locations. This “deploy-once, enable-over-time” approach allows enterprises to address their greatest risks today and grow into a comprehensive security solution.

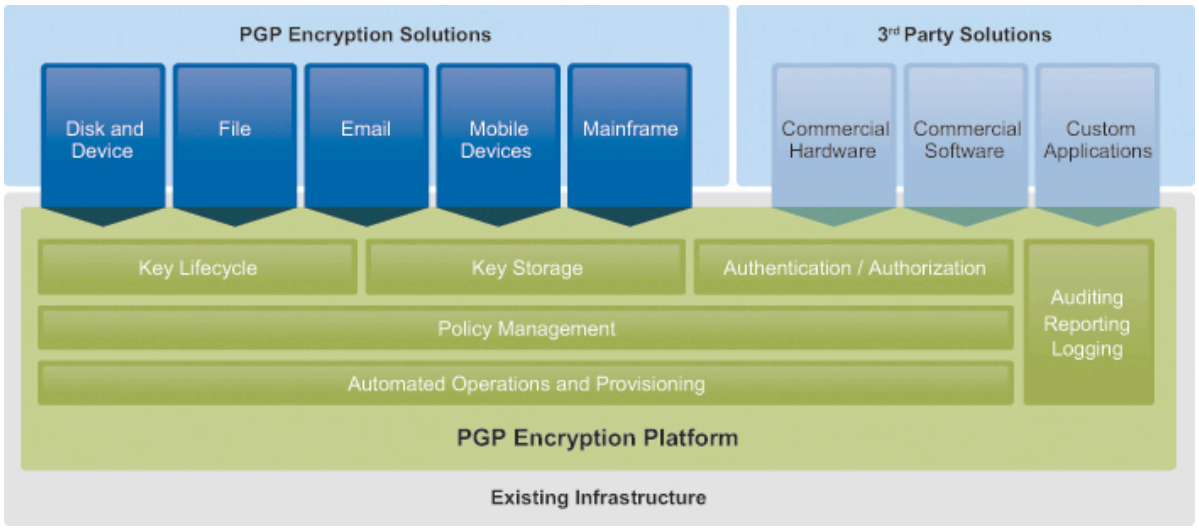


Figure 13: PGP Encryption Platform and solutions

Current PGP encryption applications:

- **PGP® Whole Disk Encryption:** encrypted full disk, files, folders, USB drives, and external backups
- **PGP® NetShare:** encrypted files and folders stored on network file servers
- **PGP Universal™ Gateway Email:** gateway encryption and digital signatures
- **PGP® Desktop Email:** desktop encryption, digital signatures, file shred, and IM encryption
- **PGP® Endpoint**: granular, policy-based control of devices and applications
- **PGP® Mobile:** comprehensive data encryption for mobile devices
- **PGP® Support Package for BlackBerry®:** PGP encryption on BlackBerry handheld devices
- **PGP® Command Line:** encryption for automated processes and file transfers
- **PGP® Software Development Kit:** encryption for customized, internal applications

The PGP Encryption platform is an automated, server-based architecture that centrally handles all key management, corporate encryption policy, and network infrastructure interaction. It manages both gateway and client encryption applications, providing an authoritative set of encryption policies that are automatically and consistently enforced for all users. Automatic encryption and decryption means no user training, minimal IT resource impact, and low operational costs. Its proxy-based design installs without disruption to existing network architectures and easily expands to meet future risks to data security.

PGP Corporation sets the standard for verifying that no backdoors or secret access exists in its product software. The company is the only commercial security vendor to publish source code for peer review. PGP source code has been downloaded more than 100,000 times. The PGP Encryption Platform was one of only 12 innovations identified by a panel of experts to receive The Wall Street Journal 2007 Innovation Award. PGP Whole Disk Encryption and PGP Desktop Email are both *SC Magazine* "Best Buy" products, winning against competing point solutions in hands-on group tests.

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 or +1 800 887 3118.

About PGP Corporation

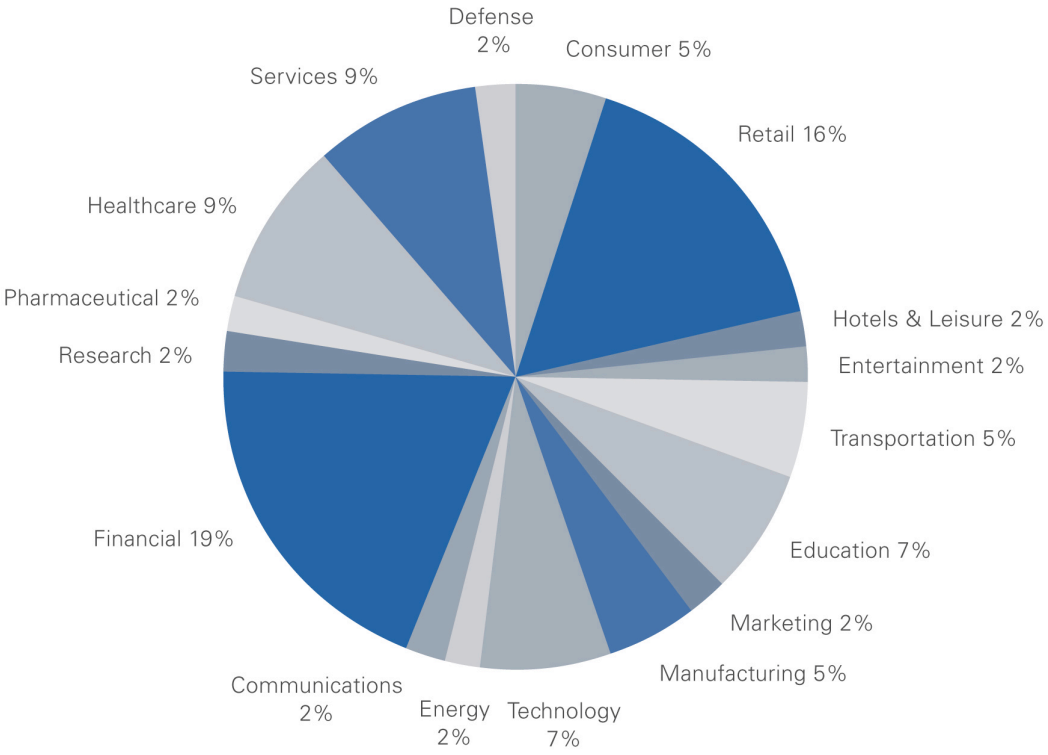
PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications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

PGP® solutions are used by more than 100,000 enterprises, businesses, and governments worldwide, including 95 percent of the Fortune® 100, 75 percent of the Fortune® Global 100, 87 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 www.pgp.com or +1 650 319 9000.

Appendix A – Survey Methodology

The Ponemon Institute's study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations, all U.S.-based entities experiencing a breach involving the loss or theft of customer, consumer, or employee data over the past 12 months. Statistical inferences, margins of error, and confidence intervals cannot be applied to this data, given the nature of the sampling plan.
- **Non-response:** The current findings are based on a representative sample of completed surveys. Thirty-five companies completed all parts of the benchmark survey. Non-response bias was not tested, so it is always possible companies that did not participate are substantially different from those that completed the survey in terms of the methods used to manage the data breach process as well as the underlying costs involved.
- **Sampling-frame bias:** Because the sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. The Institute believes that the current sampling frame is biased toward companies with more mature privacy or information security programs.
- **Company-specific information:** The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- **Unmeasured factors:** To keep the survey concise and focused, the Ponemon Institute decided to omit other important variables such as leading trends and organizational characteristics from its analyses. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- **Estimated cost results.** The quality of survey research is based on the integrity of confidential responses received from companies. Although certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed "shadow costing method," explained later) rather than actual cost data could create significant bias in presented results.
- **Survey sample.** Out of the 43 surveys completed, financial services and retail organization made up the largest segments of the sample. Along with professional services, these segments account for 40 percent of the survey sample. The following chart and table details the entire sample composition.



Industry	Frequency
Financial	8
Retail	7
Healthcare	4
Services	4
Education	3
Technology	3
Manufacturing	2
Transportation	2
Consumer	2
Hotels & Leisure	1
Entertainment	1
Marketing	1
Pharmaceutical	1
Communications	1
Research	1
Energy	1
Defense	1

Figure 14 and Table 4: Sample composition by industry vertical

Benchmark Methods

The benchmark survey instrument was designed to collect descriptive information from data protection or information security practitioners about the costs incurred either directly or indirectly concerning the breach event. It also required practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal customer turnover rates that resulted from the breach event.

The survey design relied on a “shadow costing method” used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.

Within each category, cost estimation was a two-stage process. First, the survey required individuals to provide direct cost estimates for each privacy cost category by checking a range variable. A range variable was used rather than a point estimate to preserve confidentiality (to ensure a higher response rate). Second, the survey required participants to provide a second estimate for both indirect costs and opportunity costs, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct costs within a given category.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. The Institute believed that a survey focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. It also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

The diagram below illustrates the activity-based costing schema used in the current benchmark study. The study examined the above-mentioned cost centers. The arrows suggest that these cost centers are sequentially aligned, starting with incident discovery and proceeding to escalation, notification, ex-post response, and culminating in lost business. The cost driver of ex-post response and lost business opportunities is the public disclosure or notice of the event.

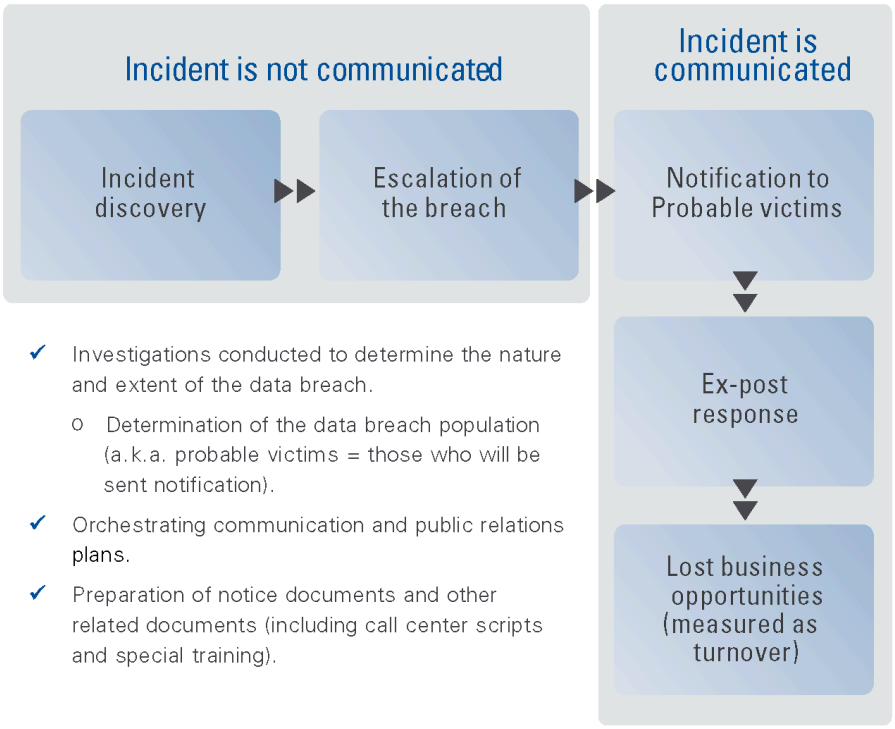


Figure 15: Visual representation of benchmark cost categories