Fourth Annual US Cost of Data Breach Study

Benchmark Study of Companies

Sponsored by PGP Corporation

Independently conducted by Ponemon Institute LLC

Publication Date: January 2009

Fourth Annual US Cost of Data Breach Study

By Dr. Larry Ponemon

Despite regulations, laws and growing awareness of the critical need to protect a company's information assets, data breaches continue to occur in businesses, educational and governmental institutions and medical facilities. Since 2005 when the Privacy Rights Clearinghouse began tracking the data breach incidents, more than 250 million customer records containing sensitive and confidential information have been lost or stolen.[1]

Ponemon Institute research indicates that data breaches have serious financial consequences on an organization. According to this year's Ponemon Institute *Annual Cost of a Data Breach* study, the average cost of a data breach has risen to $202 from last year's $197 per customer record.

Ponemon Institute research has shown that the frequency of data breaches and, as a consequence, the high percentage of individuals notified that their personal information was lost or stolen has increased overall concerns about privacy and identity theft. In Ponemon Institute's *2007 Survey on Consumer Privacy,* we queried 786 consumers who reside in the United States. Sixty-two percent of respondents had been notified that their confidential data was lost or stolen and 84% of these consumers expressed increased concern or anxiety due to the data loss.

What is the potential financial impact for companies unfortunate enough to experience a data breach? Answering that question and providing valuable insight for companies is the goal of Ponemon Institute's annual *US Cost of Data Breach study*.

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 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 acquisition rates.

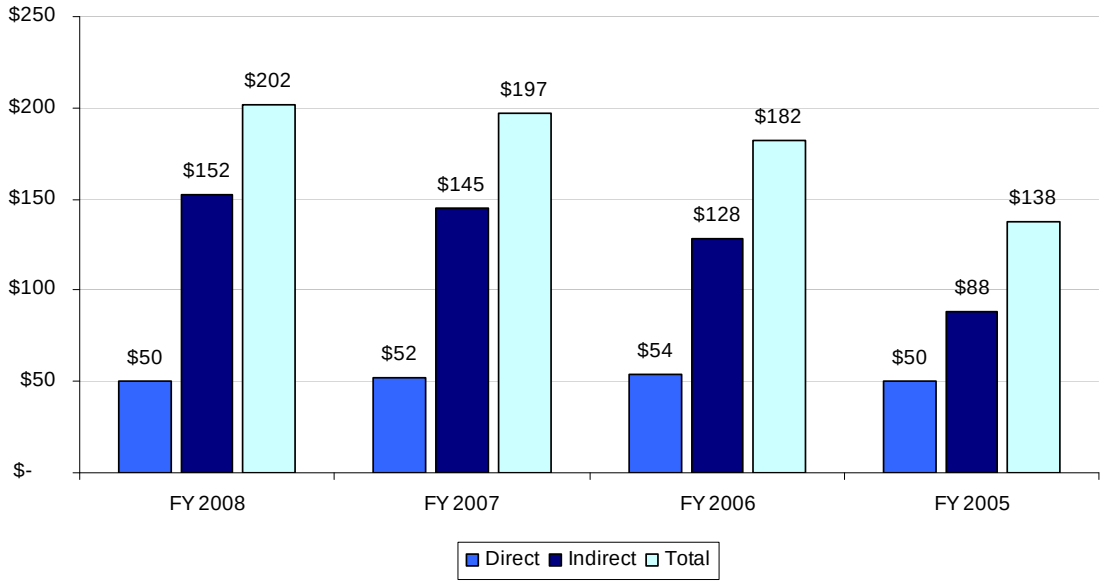
What did we learn from this year's study?

The total cost of a data breach continues to increase every year. According to Bar Chart 1, data breaches in the 2008 sample cost companies an average of $202 per compromised record – of which $152 pertains to indirect cost including abnormal turnover or churn of existing and future customers.[2] Last year's average per victim cost was $197 with an average indirect cost at $145 per breach victim. Despite an overall rise in total data breach cost over the past four years, direct costs appear to be declining slightly from a high of $54 in 2006 to a low of $50 in 2008.

[1] See the Privacy Rights Clearinghouse website www.privacyrightsclearinghouse.org for more details about this ongoing data breach tracking survey.

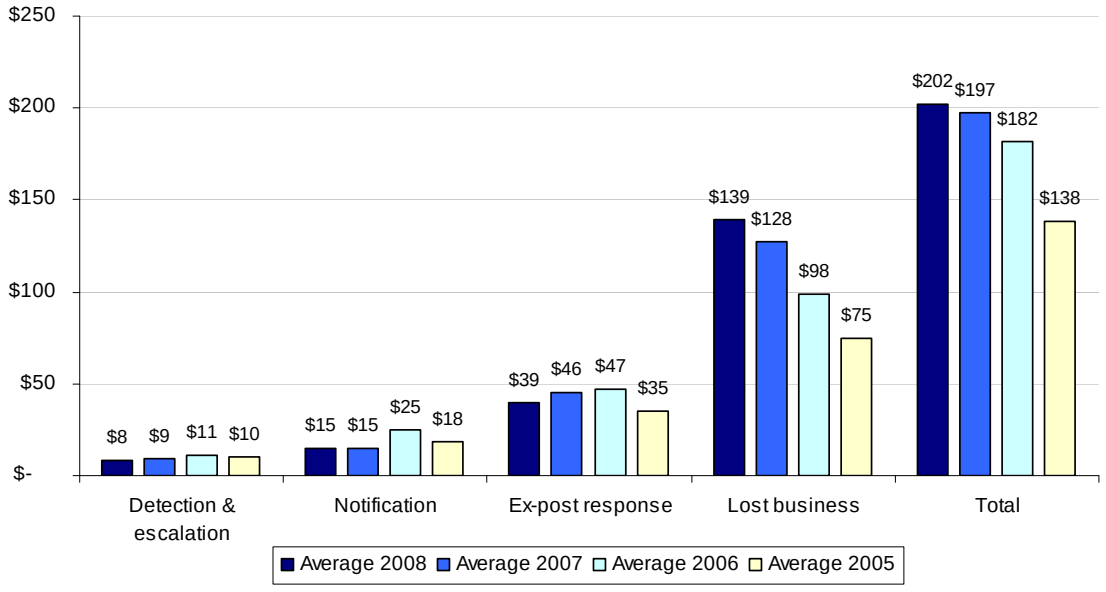
[2] For purposes of comparability across different breach incidents, we measure data breach cost on a per compromised record basis (a.k.a. per victim cost).

Bar Chart 1
Direct and indirect data breach cost over four years
Bar chart shows cost on a per victim basis



An increase in the cost of lost business suggests the American public continues to care deeply about the loss or theft of their personal information. As shown in Bar Chart 2, the largest cost increase in 2008 concerns lost business created by abnormal churn or turnover of customers. Over the past four years lost business cost component grew by more than $64 on a per victim basis, or a 38% overall percentage increase. Our research finds organizations in highly trusted industries such as banking, pharmaceuticals and healthcare are more likely to experience a data breach with high abnormal churn rates. In contrast, retailers and companies with less direct consumer contact seem to experience a lower overall data breach cost.

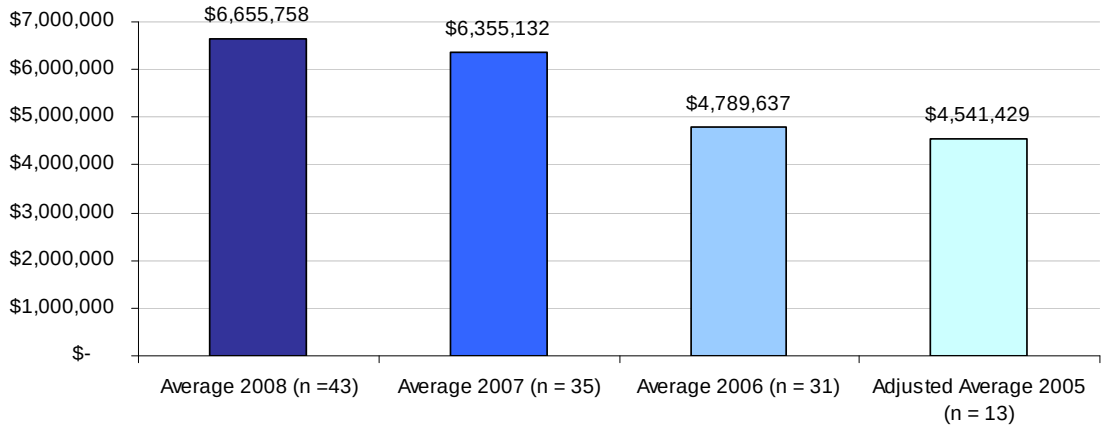
Bar Chart 2
Cost of data breach on a per victim basis over four years



As shown in the above bar chart, other cost components of a data breach appear to have stabilized or slightly decreased over the past year. The most significant cost decrease concerns ex-post response, which implies organizations are becoming more cost efficient in their management of the data breach. Despite efficiency gains, consulting, legal defense and, as mentioned previously, lost customer business have increased in this year's study.

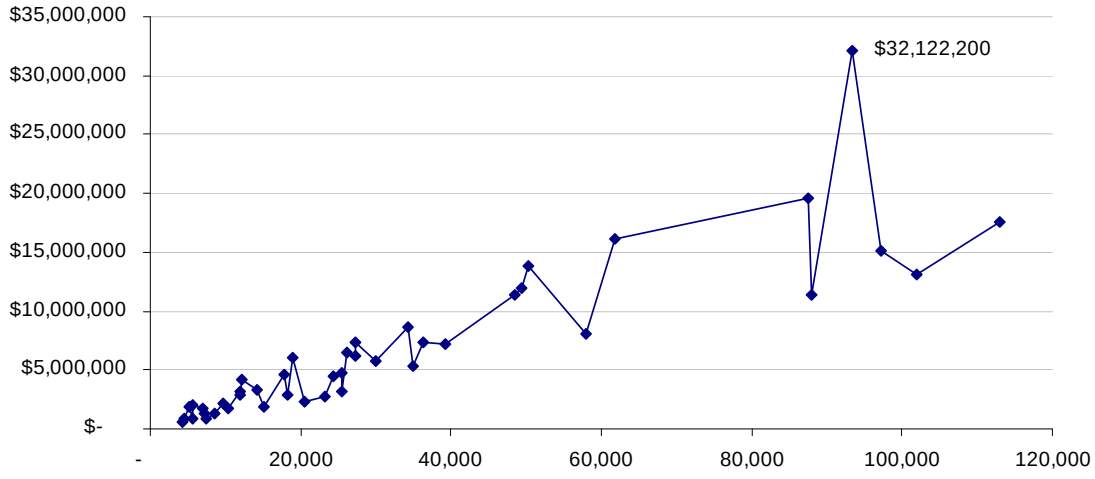
Data breach continues to be a very costly event for organizations. Bar Chart 3 reports the average organizational cost of data breach. As shown, data breach cost increases from prior years to $6.65 million in our 2008 study.[3]

Bar Chart 3
Average organizational cost of data breach cost over four years



Line Graph 1 reports total organizational cost in ascending order by the size of the breach event.

Line Graph 1
Total data breach cost in ascending order by the number of compromised records



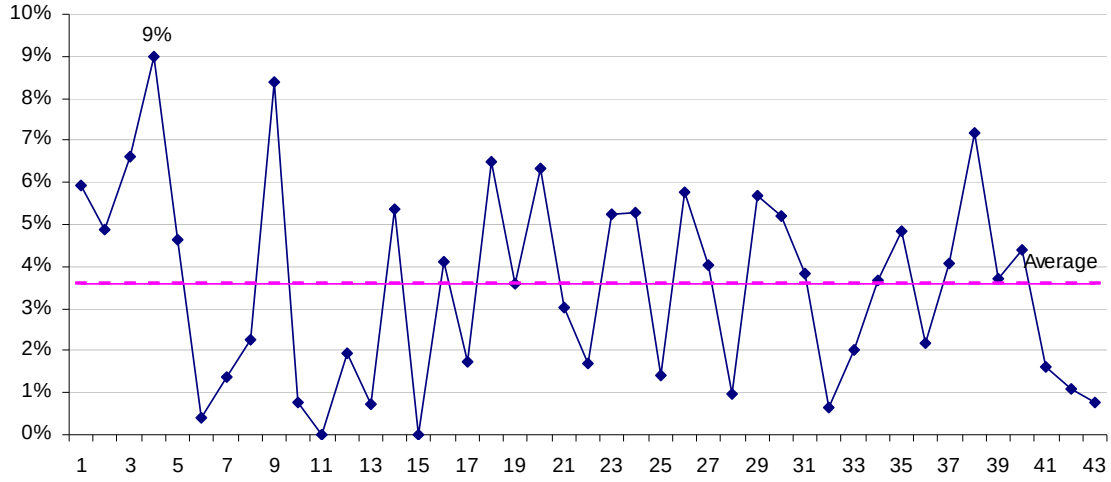
The range of total cost among the 43 data breach incidents contained in this year's study is a minimum of $613k to more than $32 million. The magnitude of the breach event ranged from 4,200 to 113,000 lost or stolen records. As in prior years, data breach cost appears to be linearly related to the size or magnitude of the breach event.

[3] The 2005 study involved one very large (catastrophic) data breach that represented an outlier cost event. Hence, it was removed from the total for comparison purposes.

Abnormal churn or turnover of customers resulting directly from the data breach incident appears to the main driver for data breach cost.

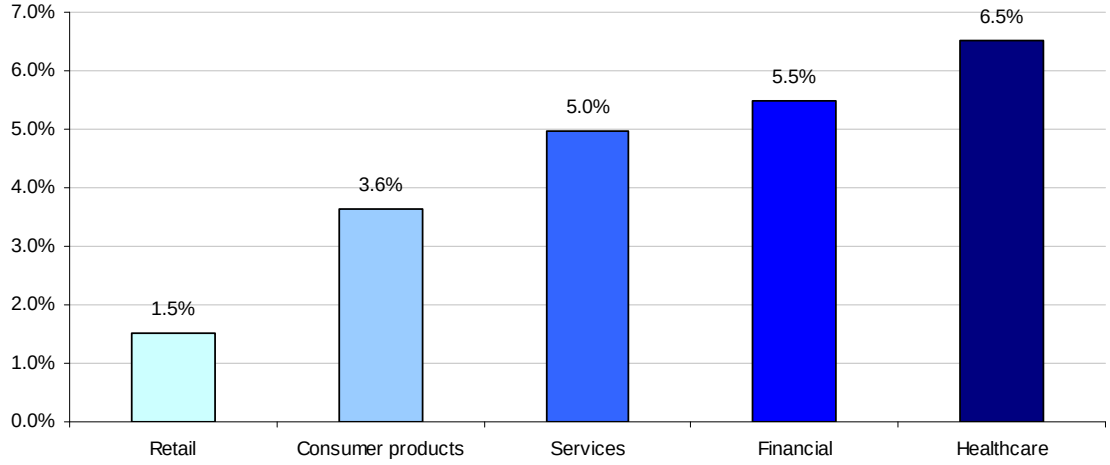
In this year's study, average abnormal churn rates across all 43 incidents is 3.6%, which was measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). The abnormal churn or turnover rate in 2007 for customers receiving notification was 2.7%. Line Graph 2 shows abnormal churn ranging from null to a high of more than 9%.

Line Graph 2
Abnormal churn rates for 43 companies



Bar Chart 4a reports the abnormal churn rates for five industries. As can been seen, percentage churn differs markedly across industries.[4]

Bar Chart 4a
Abnormal churn rates by industry classification

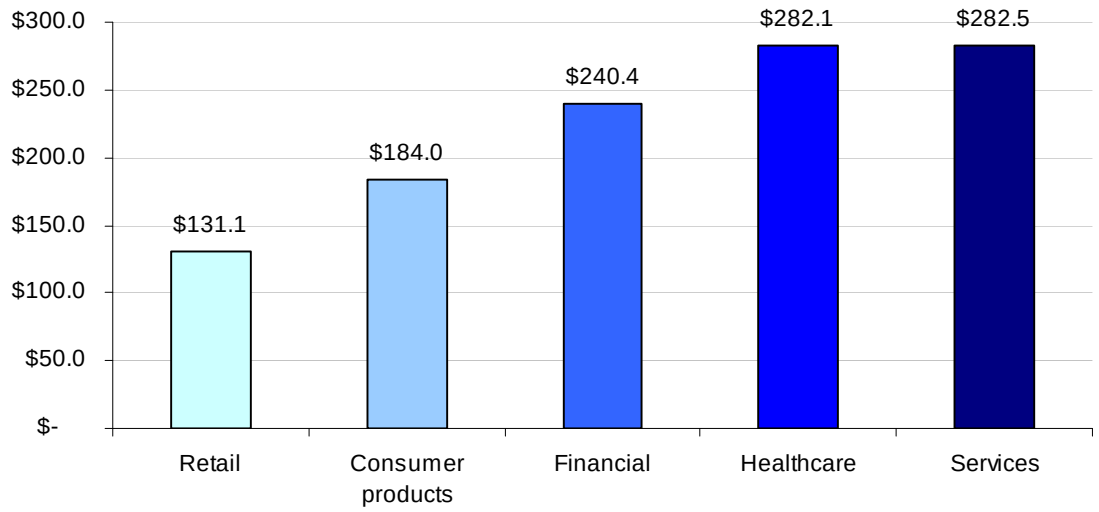


[4] The 2008 benchmark survey includes companies in 17 different industry groups. The five industries shown in Bar Chart 4 are those having three or more companies within the group.

Healthcare and financial service companies have the highest average rate of churn at 6.5% and 5.5%, respectively. High churn rates reflect the fact that these industries manage and collect consumers' most sensitive data. Thus, consumers may have a higher expectation for the protection and privacy of their financial and healthcare records.

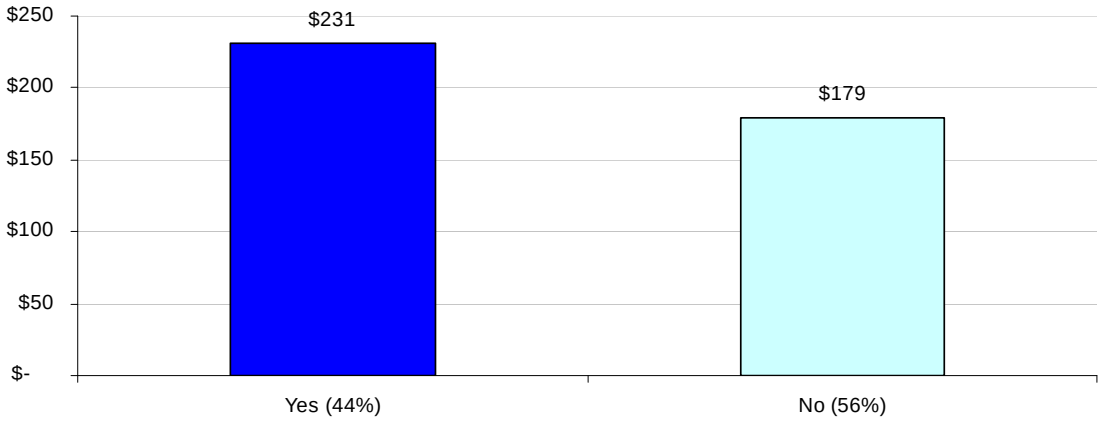
Bar Chart 4b reports the per capita cost of data breach for the same five industries indicated above. Once again, results differ across industries. In this year's study, retail has the lowest and services the highest per capita costs, respectively.

Bar Chart 4b
Per capita cost of data breach by industry classification



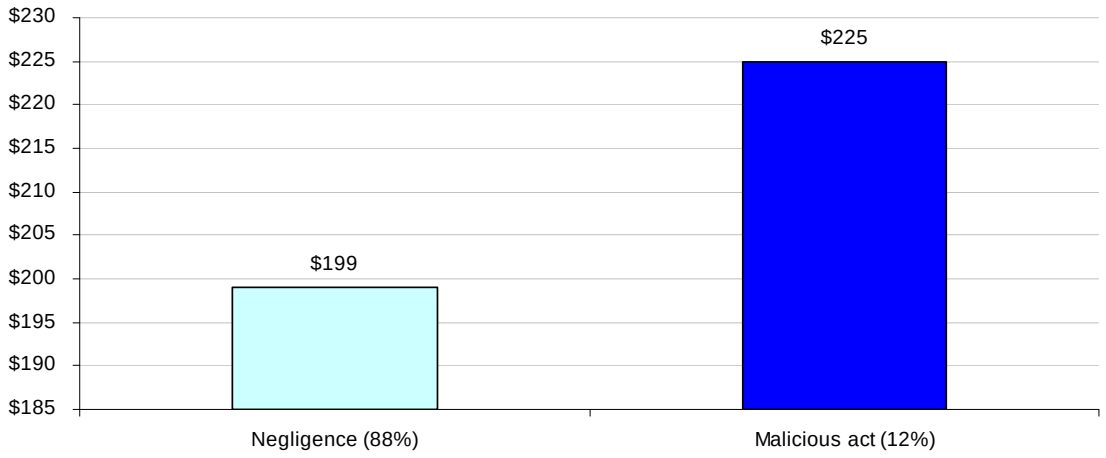
Over 44% of all cases in this year's study involved third-party mistakes or flubs. Data breaches involving outsourced data to third parties are the most costly. This could be due to additional investigation and consulting fees. As shown in Bar Chart 5, per victim cost for data breaches involving third parties is $231 versus $179, more than a $52 difference.

Bar Chart 5
Did the data breach involve a third party flub?
Bar chart shows average per victim cost



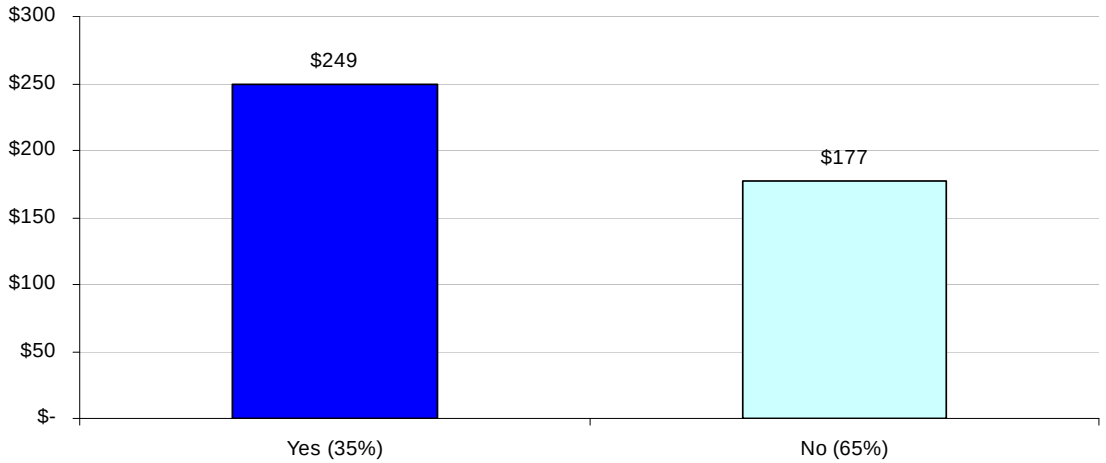
More than 88% of all cases in this year's study involved insider negligence. Data breaches involving malicious acts are more expensive than incidents resulting from negligence. Bar Chart 6 reports per victim cost of a data breach involving a malicious or criminal act is $225 vs. $199 due to insider negligence.

Bar Chart 6
Did the data breach result from negligence or a malicious act?
Bar chart shows average per victim cost



About 35% of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. As shown in Bar Chart 7, data breaches concerning lost laptops are more expensive than all other incidents. Per victim cost for a data breach involving a lost or stolen laptop is $249 vs. $177 for all other loss events.

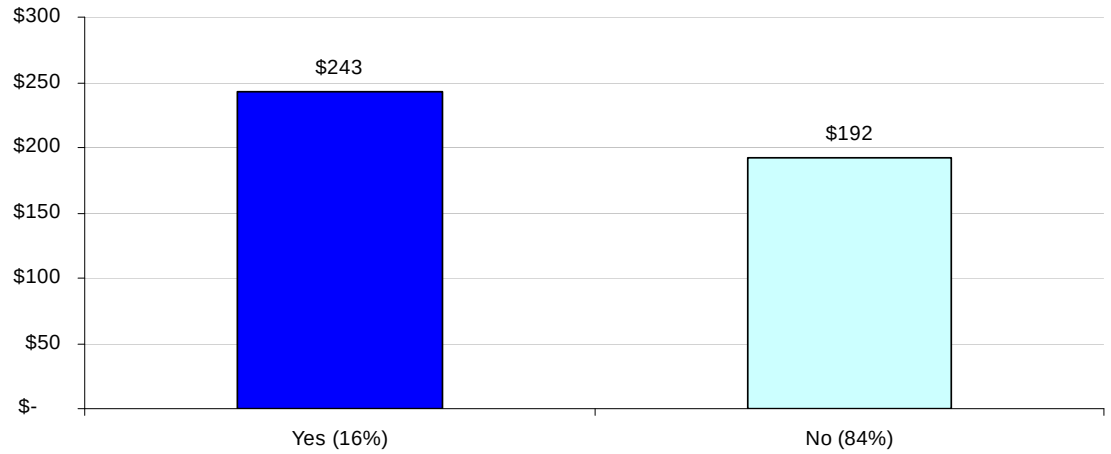
Bar Chart 7
Did the data breach involve a lost or stolen laptop computer?
Bar chart shows average per victim cost



More than 84% of all cases in this year's study involved organizations that had more than one data breach involving the loss or theft of more than 1,000 records. Bar Chart 8 shows data breaches experienced by "first timers" are more expensive than those experienced by

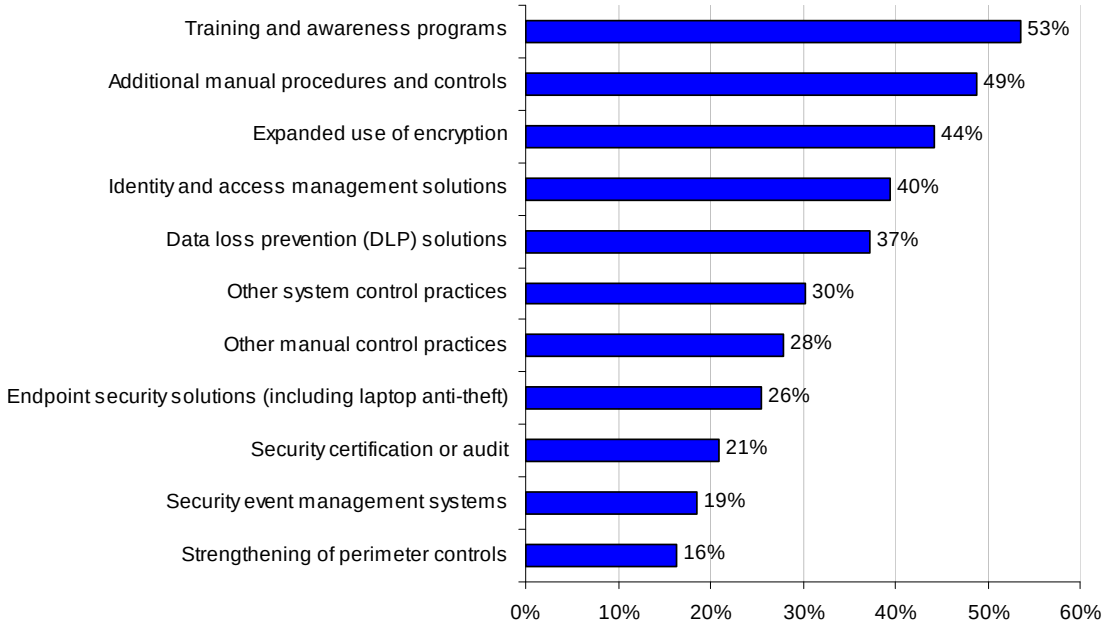
organizations that have had previous data breaches. Per victim cost for a first time data breach is $243 vs. $192 for experienced companies.

Bar Chart 8
Was this the company's first major data breach incident?
Bar chart shows average per victim cost



Training and awareness programs lead companies' efforts to prevent future breaches according to 53% of respondents. As shown in Bar Chart 9, 49% percent of companies are creating additional manual procedures and controls. In addition, 44% of companies have expanded their use of encryption technologies to prevent future data breaches.

Bar Chart 9
What preventive measures have been implemented after the data breach?



Background

Our fourth annual benchmark study seeks to examine the cost that organizations incur when responding to data breach incidents resulting in the loss or theft of sensitive personal information. Our benchmark results are intended to provide a meaningful baseline for companies experiencing a data breach event that requires notification to individuals as required by law.

At the time of this study, most U.S. states require both business and governmental organizations to provide notification to data subjects (customers, consumers, employees and others) when a breach of sensitive personal information is caused by negligence (insider threats), technology problems or malicious acts. While conditions for notification vary across states, the organization may not be required to notify individuals when:

- ✓ The breached data is encrypted (minimum 128 bit standard).
- ✓ 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.

Most state regulations focus on personal information that is private, sensitive or confidential. In the wrong hands, possession of this information can bring about harm or risk to the victim. Regulations that require organizations to notify victims in the event of a data security breach often define the data elements that are considered protected. Also, certain breach laws require notification only when the data is acquired by an unauthorized party – defined as an individual or organization that does not have the right to collect, use or share sensitive or confidential information about the data subject.

The Cost of a Breach

Our study addresses core process-related activities that drive a range of expenditures associated with a company's data breach detection and response. The four cost centers are:

- 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, e-mail 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 in order to minimize potential harms. Redress activities also include ex-post response 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 results from diminished trust or confidence by present and future customers. Accordingly, our Institute's research shows that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover or churn rates well as a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we will be using a shadow costing method that relies on the "lifetime value" of an average customer as defined for each participating organization.

- Turnover intentions of existing customers: The estimated number of customers who 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 who will not have a relationship with the organization as a consequence of the breach. This number is provided as an annual percentage.

It is important to note, however, that the loss of non-customer data, such as employee records, may not impact an organization's churn or turnover rates directly.

Caveats

Our 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 sample: The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of U.S. organizations experiencing a breach involving the loss or theft of customer or consumer data over the past 12 month period.

  For consistency purposes, our study does not include data breaches resulting from missing or stolen employee records. In addition, we deliberately excluded data breaches considered to be catastrophic (as defined by an event involving the loss or theft of more than 150,000 records). Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the judgmental nature of our company recruitment process.

- Non-response: The current findings are based on a small representative sample of completed benchmark surveys. An initial invitation was sent to a targeted group of 110 organizations, all known to have experienced a breach involving the lost or theft of customer or consumer data sometime over the past year. Forty-three US 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 in terms of the methods used to manage the data breach process, as well as the underlying costs associated with information loss.

- Sampling-frame bias: Because our 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. It is our belief 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, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. 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. While reliability checks were incorporated into the benchmark survey process, there is always the possibility that respondents did not provide

truthful responses. In addition, the use of a cost estimation technique rather than the company's detailed actual cost data could create significant bias in presented results.

Benchmark methods

The benchmark survey instrument was designed to collect descriptive information about the costs incurred either directly or indirectly concerning the breach event. Typically, the point-person for each survey was privacy, data protection or compliance professionals responsible for managing the data breach incident. The survey required these practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a structured survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal churn rates that resulted from the breach event.

The survey design relied upon a shadow costing method used in applied economic research. This method doesn't 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 cost and opportunity cost, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct cost within a given category.

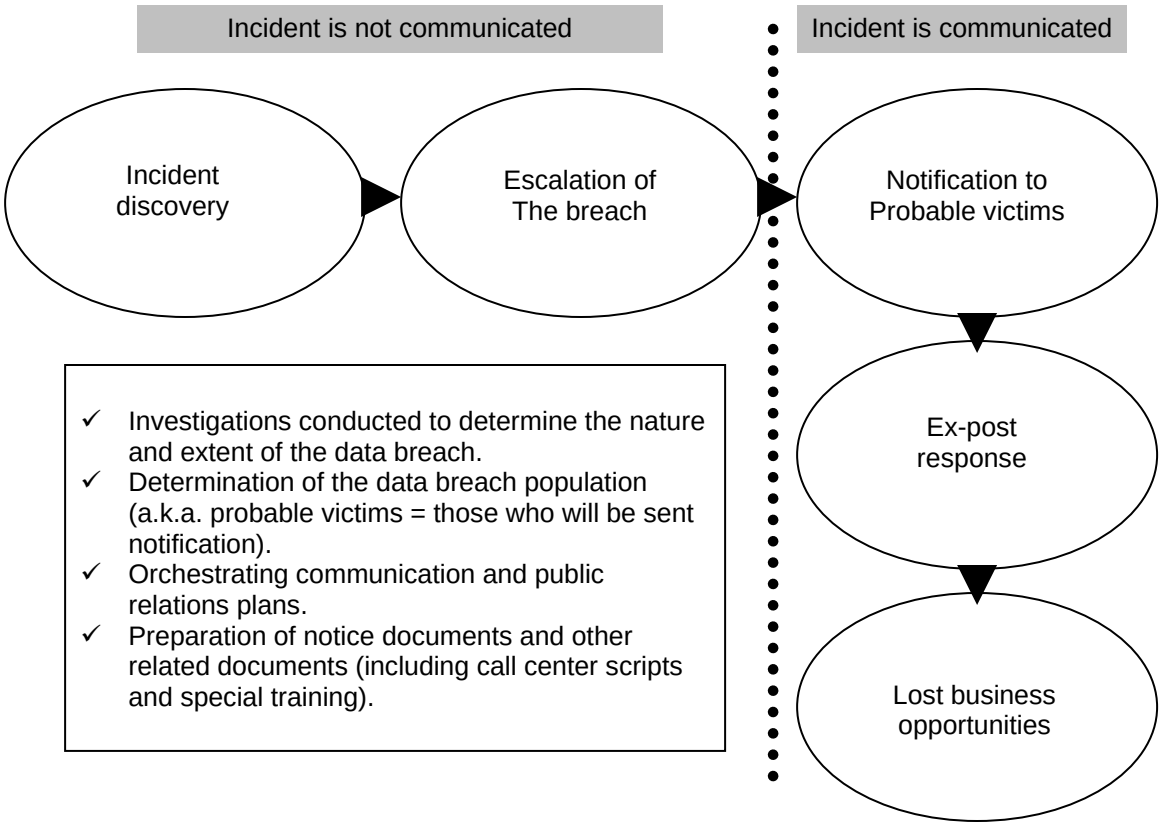
The size and scope of survey items was limited to known cost categories that cut across different industry sectors. We believed that a survey focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. We also used a paper instrument, rather than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

The diagram below illustrates the activity-based costing schema used in the current benchmark study. As can be seen, we examined the above mentioned cost centers. The arrows suggest that these cost centers are sequentially aligned – starting with incident discovery to escalation to notification to 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.

In total, the benchmark survey instrument contained descriptive cost activities for each one of the five cost centers mentioned above.

Within each cost center, the survey required subjects to estimate cost range to signify direct cost, indirect cost and opportunity cost, defined as follows:

- Direct cost – the direct expense outlay to accomplish a given activity.
- Indirect cost – the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- Opportunity cost – the cost resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been reported to victims (and publicly revealed to the media).



To maintain complete confidentiality, the survey instrument did not capture company-specific information of any kind. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

To keep the survey to a manageable size, we carefully limited items to only those cost activities that we consider crucial to the measurement of a data security breach. Based on discussions with learned experts, the final set of items focused on a finite set of direct or indirect cost activities. Upon collection of the survey information, each instrument was examined carefully for consistency and completeness. Three instruments were rejected based on incomplete, inconsistent or blank responses.

Conclusion

The findings of this benchmark study suggest US companies that have a loss or theft of personal information requiring notification do incur significant direct and indirect expenses. The most negative cost impact results from the diminishment of confidence and trust in the company, which translates into abnormal or unexpected customer turnover.

In summary, our research suggests that American consumers care about the lose or theft of their personal information and hold organizations accountable for safeguarding the plethora of personal information entrusted to them. Despite limitations, the research is encouraging to those who believe the proposition that good privacy and security practices have a positive return on investment.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.231.938.9900
research@ponemon.org