



2013 Cost of Data Breach Study: United States

Benchmark research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
May 2013

2013¹ Cost of Data Breach Study: United States

Ponemon Institute, May 2013

Part 1. Executive Summary

Symantec Corporation and Ponemon Institute are pleased to present the *2013 Cost of Data Breach: United States*, our eighth annual benchmark study concerning the cost of data breach incidents for companies located in the United States. While Ponemon Institute research indicates that data breaches continue to have serious financial consequences for organizations, there is evidence that organizations are becoming better at managing the costs incurred to respond and resolve a data breach incident. In this year's study, the average per capita cost of data breach declined from \$194 to \$188.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States eight years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia, India, Italy, Japan and, for the first time this year, Brazil. To date, 322 U.S. organizations have participated in the benchmarking process since the inception of this research series.

This year's study examines the costs incurred by 54 U.S. companies in 14 industry sectors after those companies experienced the loss or theft of protected personal data and then had to notify breach victims as required by various laws. It is important to note the costs presented in this research are not hypothetical but are from actual data loss incidents. They are based upon cost estimates provided by the more than 450 individuals we interviewed over a ten-month period in the companies that are represented in this research.

The number of breached records per incident this year ranged from approximately 5,000 records to more than 99,000 records. This year the average number of breached records was 28,765. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and to include them in the study would skew the results. The cost for the 54 data breach case studies in this year's report is presented in Appendix 1.

The report examines 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 as measured by customer turnover or churn.

The following are the most interesting findings and implications for organizations:

- **The cost of data breach continues to decline.** Similar to last year's trend, both the organizational cost of data breach and the cost per lost or stolen record have declined. The organizational cost has declined from \$5.5 million to \$5.4 million and the cost per record² has declined from \$194 to \$188. We define a record as information that identifies the natural person (individual) whose information has been compromised in a data breach.

This decline suggests that organizations represented in this study continue to improve their performance in both preparing for and responding to a data breach. As the findings reveal, more organizations are using data loss prevention technologies, fewer records are being lost in these breaches and there is less customer churn.

- **More customers remain loyal following the data breach.** Following last year's trend, fewer customers are abandoning companies after being notified of a data breach involving the loss

¹ The Cost of Data Breach report is dated as a 2013 publication. Please note that all data breach incidents studied in this year's report happened in the 2012 calendar year. Thus, all figures reflect the 2012 data breach incidents.

² The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

or theft of their personal information. This fact is evidenced by a 13 percent decrease in the average abnormal churn rate between 2011 and 2012. Despite this overall decline, certain industries, especially healthcare and financial services, are still more susceptible to high customer churn in the event of a data breach.

- **Malicious or criminal attacks rather than negligence or system glitches are the main causes of data breach.** For the first time, this year's study shows malicious or criminal attacks as the most frequently encountered root cause of data breaches by organizations in this study. Accordingly, 41 percent say the main cause of data breach was malicious or criminal attacks against the organization. Thirty-three percent of organizations say employee negligence (a.k.a. human factor) and 26 percent say system glitches were the main causes of the data loss.
- **Malicious or criminal attacks result in the highest per capita data breach cost.** Consistent with prior reports, data loss or exfiltration resulting from a malicious or criminal attack yielded the highest cost at \$277 per compromised record, on average. In contrast, both system glitches and employee mistakes resulted in a much lower per capita cost at \$177 and \$159, respectively.
- **Lost business costs remained steady from \$3.01 million in 2011 to \$3.03 million in 2012.** These costs refer to abnormal turnover of customers (a higher than average loss of customers for the industry or organization), increased customer acquisition activities, reputation losses and diminished goodwill. During the eight years we studied this aspect of a data breach, the highest cost for lost business was \$4.59 million in 2008. This year's cost of lost business represents the lowest cost since the inception of this study in 2005.
- **Certain organizational factors reduce the overall cost.** If the organization has a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as \$42 per compromised record. In addition, a strong security posture and the appointment of a CISO saved as much as \$34 and \$23, respectively. Finally engaging an outside consultants to assist with the breach response also saved as much as \$13 per record. Hence, when considering the average number of records lost or stolen, all of these factors can provide significant and positive financial benefits.
- **Specific attributes or factors of the data breach also can increase the overall cost.** For example, organizations that notified customers too quickly without a thorough assessment or forensic examination, incurred an average of \$37 more per record. Data breaches caused by third parties increased per capita cost by \$43. Finally, data breach incidents involving the loss or theft of data bearing devices increased per capita cost by as much as \$10 per record.
- **Ex-post response and detection costs decreased slightly.** The costs associated with ex-post response decreased from approximately \$1.51 million in 2011 to \$1.41 million in 2012. Ex-post response costs refer to all activities that attempt to address victim, regulator and plaintiff counsels' concerns about the breach incident. This cost category also includes legal and consulting fees that attempt to reduce business risk and liability. Redress, identity protection services and free or discounted products are also included in this cost category.

Similarly, the costs associated with detection and escalation activities decreased from \$428,000 in 2011 to \$395,000 in 2012. This category refers to activities that enable a company to detect the breach and determine its root cause. It also includes upstream and lateral communications that are required to focus activities and keep management informed.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews with more than 450 individuals conducted over a ten-month period. Recruiting organizations for the 2012 study began in January 2012 and interviews were completed in December. In each of the 54 participating organizations, we spoke with IT, compliance and information security practitioners who are knowledgeable about their organization's data breach and the costs associated with resolving the breach. For privacy purposes we do not collect any organization-specific information.

How do you calculate the cost of data breach?

To calculate the average cost of data breach, we collect both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates. For a detailed explanation about Ponemon Institute's benchmark methodology, please see Part 4 of this report.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of Data Breach* study is the organization. In survey research, the unit of analysis is typically the individual. As discussed previously, we recruited 54 organizations to participate in this study. All of these organizations experienced a data breach ranging from a low of about 5,000 to nearly 100,000 compromised records.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as those involving millions of lost or stolen records?

The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience. In order to be representative of the population of US organizations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than 100,000 compromised records in our analysis.

Are you tracking the same organizations each year?

Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 322 U.S. organizations.

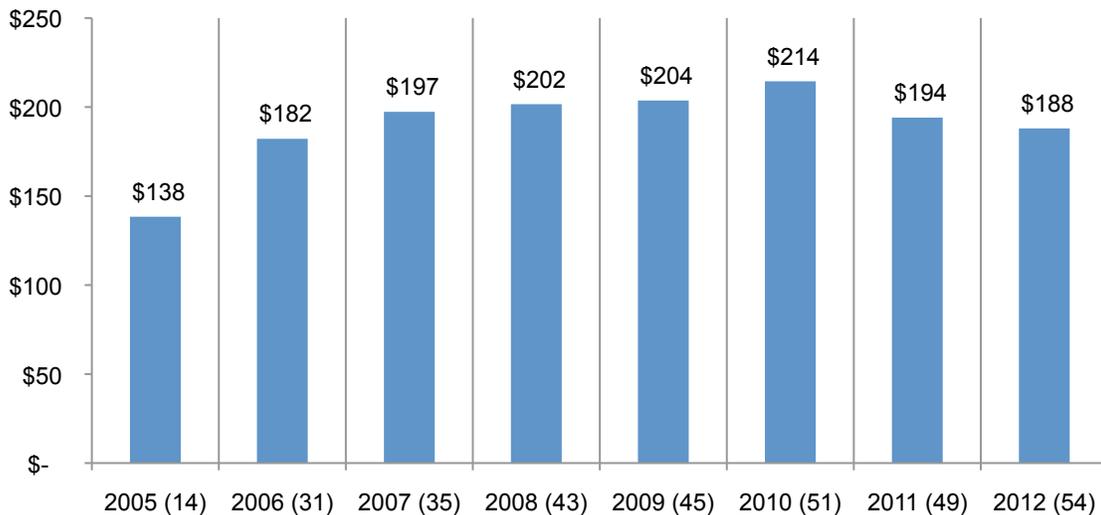
Part 2. Key Findings

In this section we provide the detailed findings of this research. Topics are presented in the following order:

- Cost of data breach per record and organization
- Cost of data breach by industry
- Root causes of a data breach
- Factors that influence the cost of a data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following cost components: detection and escalation, notification, lost business, direct and indirect and post-data breach
- Preventive measures taken after the breach
- Percentage changes in cost categories

The cost of data breach declines. Similar to last year, the cost of data breach appears to be trending downward. Figure 1 reports the average per capita cost of a data breach since the inception of this research series eight years ago.³ According to this year’s benchmark findings, data breaches cost companies an average of \$188 per compromised record – of which \$128 pertains to indirect costs including abnormal turnover or churn of customers. Last year’s average per capita cost was \$194 with an average indirect cost of \$135.

Figure 1. The average per capita cost of data breach over eight years
Bracketed number defines the benchmark sample size



³Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records.

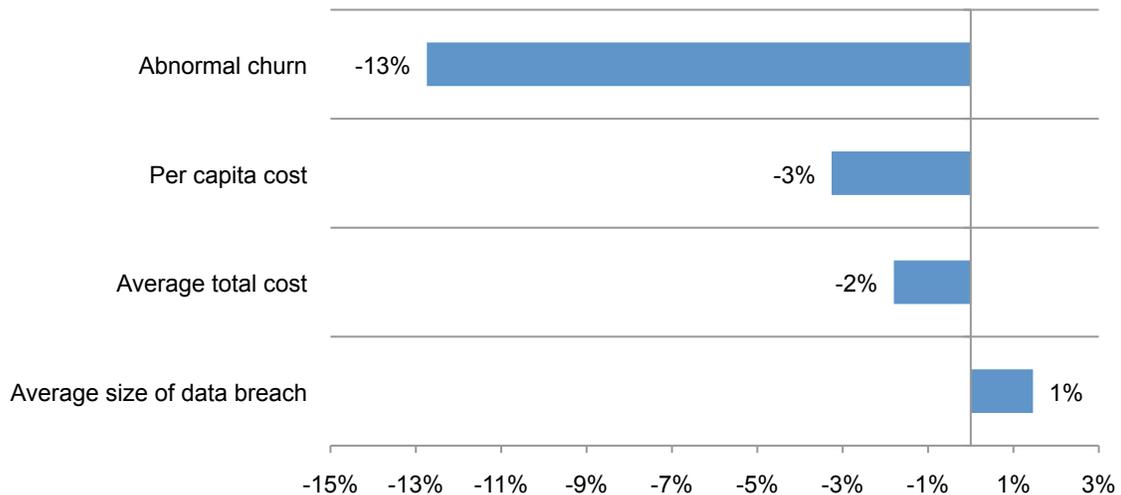
Average organizational cost of data breach declined slightly. Figure 2 shows that the total average cost of data breach over eight years steadily increased from a low of \$4.54 million in 2005 to a high of \$7.24 million in 2010. In 2012 we see a decrease in total data breach cost to \$5.40 million. This finding may suggest organizations have made improvements in how they plan for and respond to material data breach incidents.

Figure 2. The average total organizational cost of data breach over eight years
\$000,000 omitted



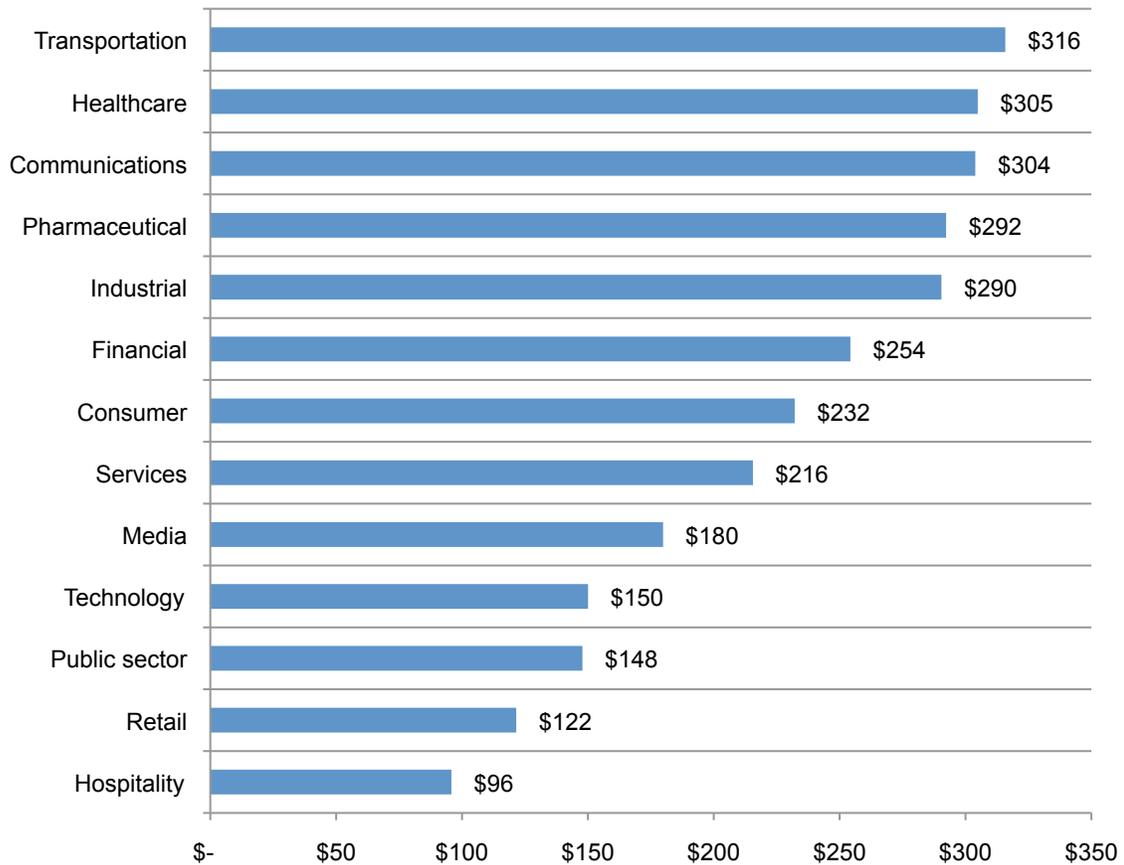
Key cost of data breach measures. Figure 3 reports the four net changes from last year's report. As discussed, the average total cost of a data breach decreased by 2 percent and the average per capita cost decreased by 3 percent. A decrease in abnormal churn of existing customers by 13 percent was a major reason for decline in cost. In the context of this paper, abnormal churn is defined as a greater than expected loss of customers in the normal course of business.

Figure 3. Cost of data breach measures
Net change defined as the difference between the 2012 and 2011 results



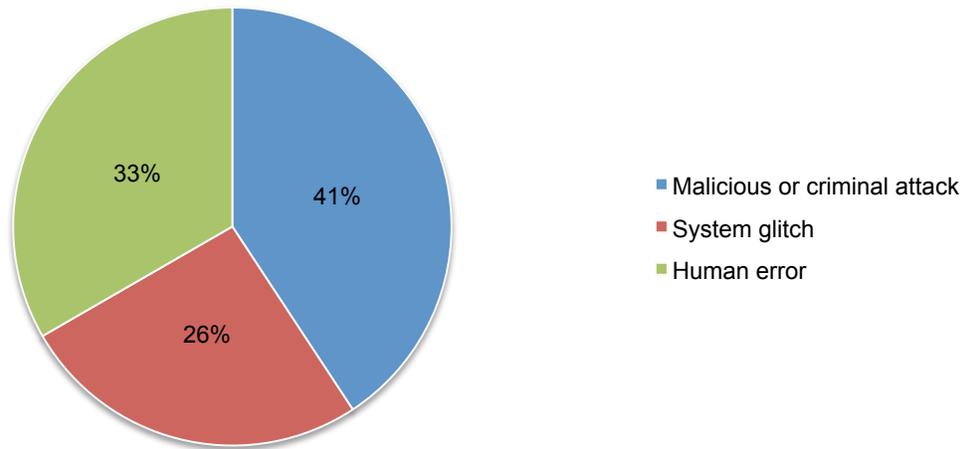
Certain industries have higher data breach costs. Figure 4 reports the per capita costs for the 2012 study by industry classification. While a small sample size prevents us from generalizing industry cost differences, the pattern of 2012 industry results is consistent with prior years. Specifically, heavily regulated industries such as healthcare, communications, pharmaceuticals and financial services tend to have a per capita data breach cost substantially above the overall mean of \$188. Retailers, hospitality companies and public sector organizations have a per capita cost below the overall mean value.

Figure 4. Per capita cost by industry classification of benchmarked companies



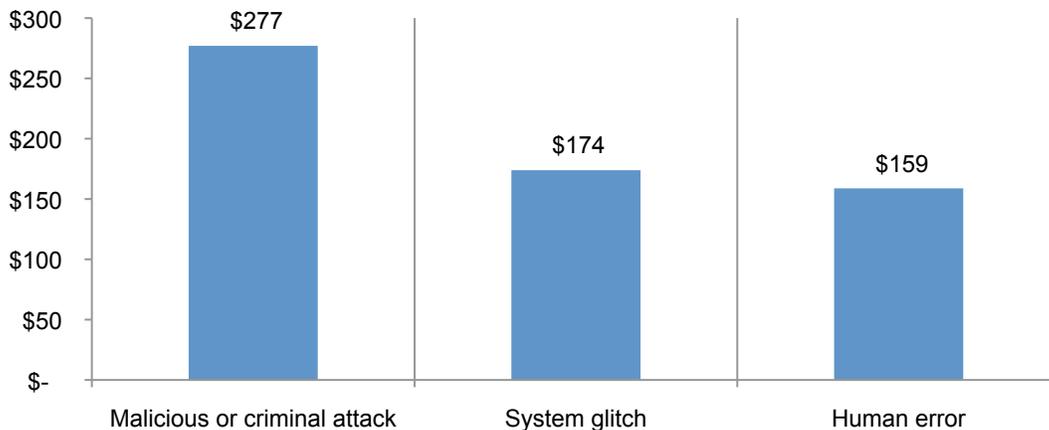
In this year's study, malicious or criminal attacks are most often the cause of data breach.⁴ Figure 5 provides a summary of the main root causes of data breach for all 54 organizations. Forty-one percent of incidents involved a malicious or criminal attack, 33 percent concerned a negligent employee, and 26 percent involved system glitches that includes both IT and business process failures.⁵

Figure 5. Distribution of the benchmark sample by root cause of the data breach



Malicious attacks are most costly. Figure 6 reports the per capita cost of data breach for three root causes of the breach incident. The 2012 results are consistent with prior years, wherein the most costly breaches typically involve malicious acts against the company. According to our research, companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost (\$277) that was significantly above the mean. In contrast, companies experiencing system glitches (\$174) or employee negligence (\$159) as the root cause had per capita costs significantly below the mean value.

Figure 6. Per capita cost for three root causes of the data breach



⁴Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Malicious attacks can be caused by hackers or criminal insiders (employees, contractors or other third parties).

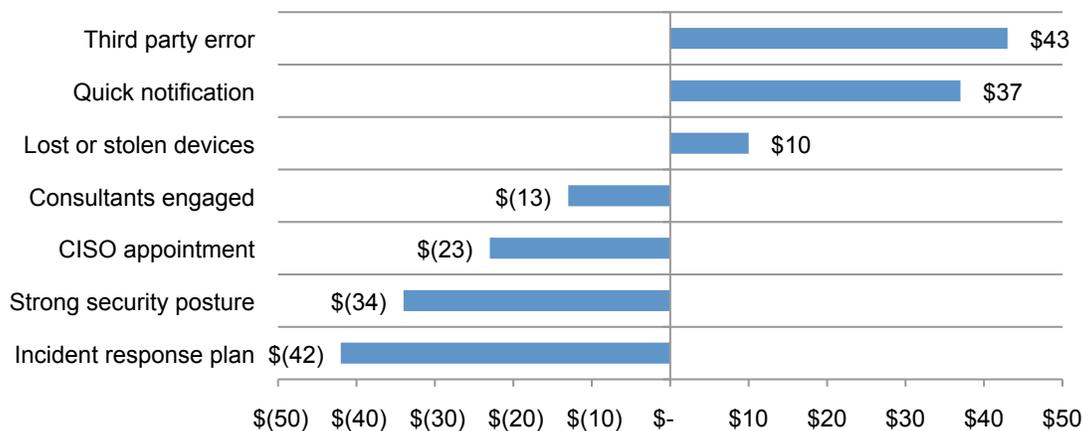
⁵Malicious and criminal attacks increased from 37 percent in last year's study. The most common types of attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Seven factors that influence the cost of data breach. We identified seven factors that influence the cost consequences of a data breach incident. These attributes are as follows:

- **The company had an incident management plan.** Fifty-two percent of organizations in our benchmark sample had a data breach incident management plan in place at the time of the data breach event.
- **The company had a relatively strong security posture at the time of the incident.** Forty-seven percent of organizations had a security effectiveness score (SES) at or above the normative average. We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process.⁶
- **CISO (or equivalent title) has overall responsibility for enterprise data protection.** Forty-three percent of organizations have centralized the management of data protection with the appointment of a C-level information security professional.
- **Data was lost due to third party error.** Forty percent of organizations had a data breach caused by a third party, such as vendors, outsourcers and business partners.
- **The company notified data breach victims quickly.** Thirty-eight percent of organizations notified data breach victims within 30 days after the discovery of data loss or theft.
- **The data breach involved lost or stolen devices.** Thirty-five percent of organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
- **Consultants were engaged to help remediate the data breach.** Forty-two percent of organizations hired consultants to assist in their data breach response and remediation.

As shown in Figure 7, incident response plans, security posture, CISO appointments and consulting support decreased the per capita cost of data breach. However, third party errors, quick notification and lost or stolen devices increased the per capita cost of data breach. Hence, an incident response plan in place reduced the average cost of data breach from \$188 to \$146 (decreased cost = \$42). In contrast, a third party error increased the average cost to as much as \$231 (increased cost = \$43).

Figure 7. Impact of seven factors on the per capita cost of data breach

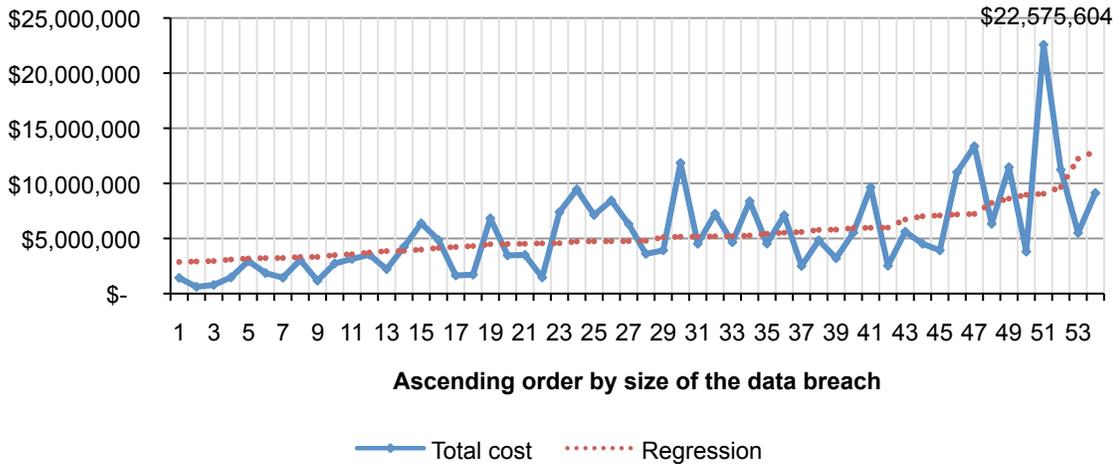


⁶The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.

The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for 54 benchmarked companies in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year's study, the cost ranged from \$611,000 to \$22.5 million.

Figure 8. Total cost of data breach by size of the data breach

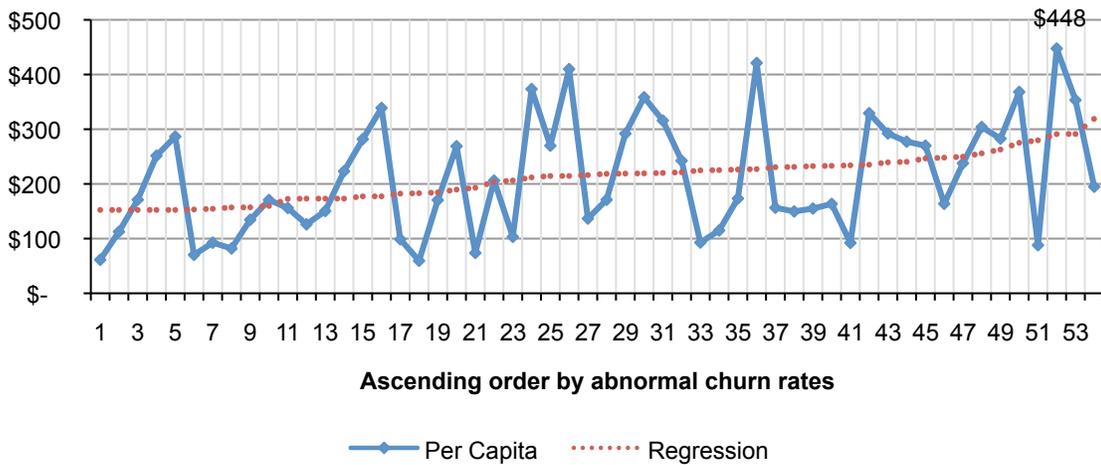
Regression = Intercept + {Size of Breach Event} x β , where β denotes the slope.



The more churn, the higher the per capita cost of data breach. Figure 9 reports the distribution of per capita data breach costs in ascending rate of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn and per capita costs are linearly related. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 9. Distribution of abnormal churn rates in ascending order by per capita costs

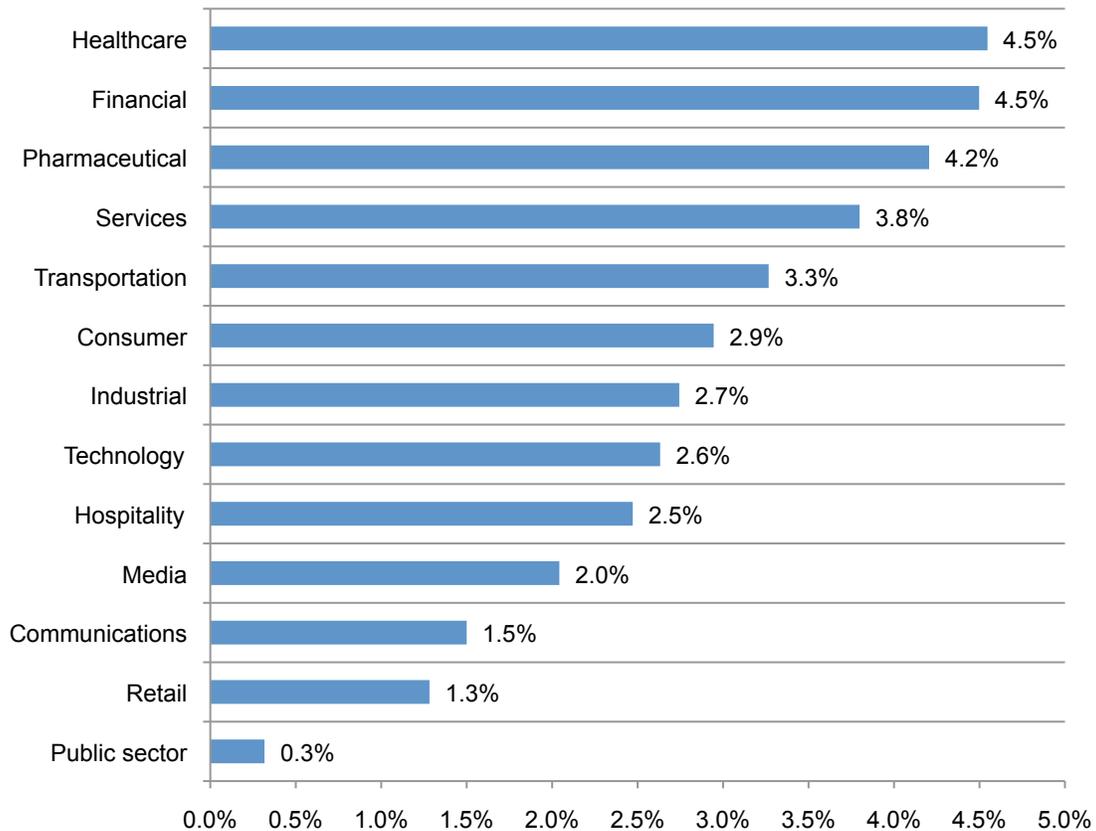
Regression = Intercept + {abnormal churn rate} x β , where β denotes the slope.



Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate of benchmarked organizations for the present study. While a small sample size prevents us from generalizing the affect of industry on data breach cost, our 2012 industry results are consistent with prior years – wherein healthcare and financial service organizations tend to experience relatively high abnormal churn and public sector and retail companies tend to experience a relatively low abnormal churn.⁷

The implications of this analysis is that industries with the highest churn rates could significantly reduce the costs of a data breach by putting an emphasis on customer retention and activities to preserve reputation and brand value.

Figure 10. Abnormal churn rates by industry classification of benchmarked companies

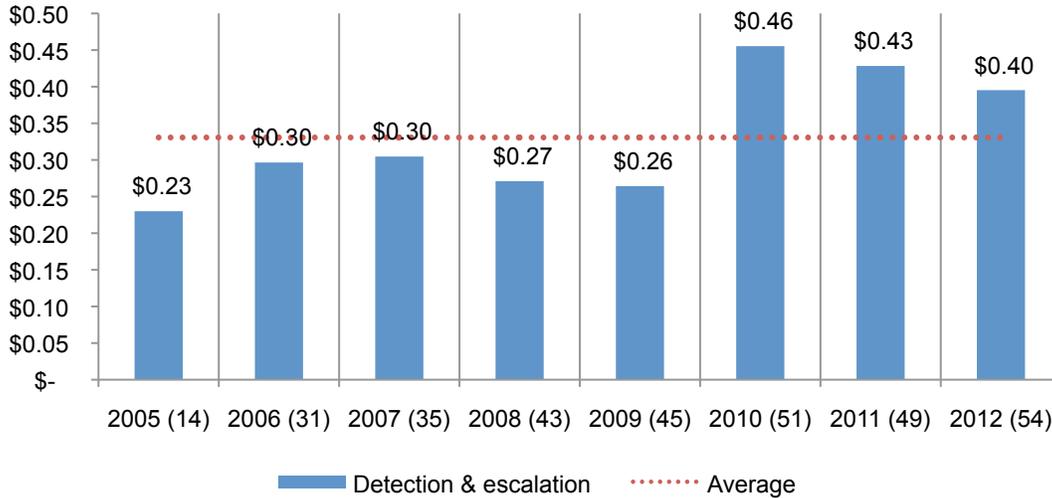


⁷Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Detection and escalation costs decrease. Figure 11 shows the eight-year trend for costs associated with detection and escalation of data breach incidents. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. As noted, average detection and escalation costs declined slightly from a high of \$.46 million in 2010 to \$.40 million in the present study.

Figure 11. Average detection and escalation costs over eight years

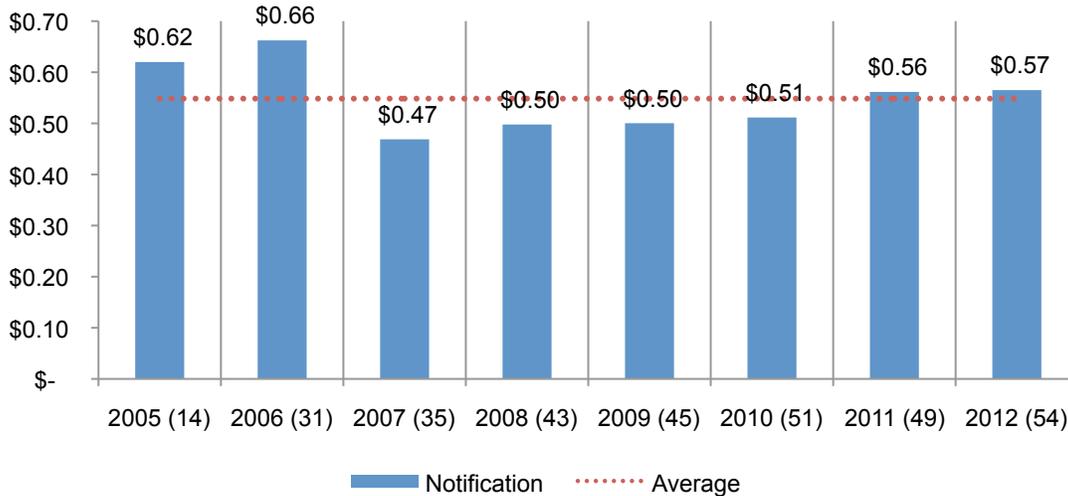
\$000,000 omitted



Notification costs increase. Figure 12 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year’s average notification increased slightly from \$.56 million in 2011 to \$.57 million in the present year. The highest notification cost over eight years was \$.66 million that occurred in 2006.

Figure 12. Average notification costs over eight years

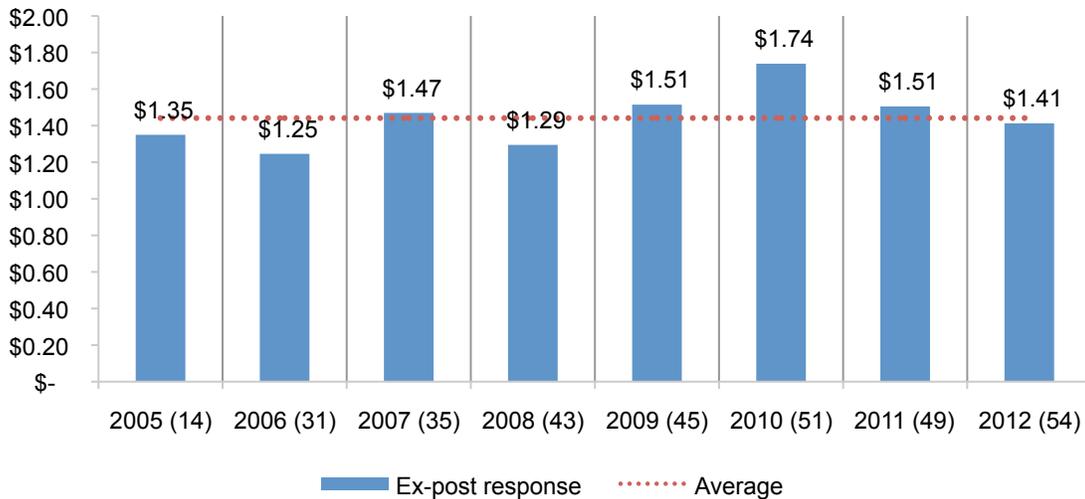
\$000,000 omitted



Post data breach costs decrease. Figure 13 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost decreased from an eight-year high of \$1.74 million 2010 to \$1.41 million in this year's study. This finding suggests greater efficiencies but also could mean organizations in this year's study are spending less on such remediation activities.

Figure 13. Average ex-post response costs over eight years

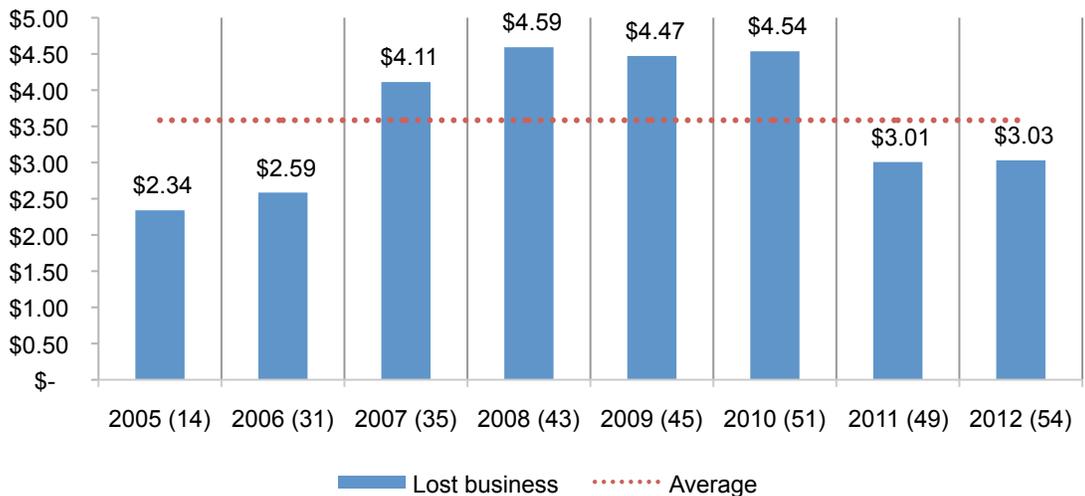
\$000,000 omitted



Lost business costs are stable. Figure 14 reports lost business costs associated with data breach incidents over eight years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen, lost business costs over the past few years appear to be trending downward. The 2012 lost business cost of \$3.03 million is very close to the 2011 cost of \$3.01 million. The highest lost business cost occurred in 2008 and the lowest in 2005.

Figure 14. Average lost business costs over eight years

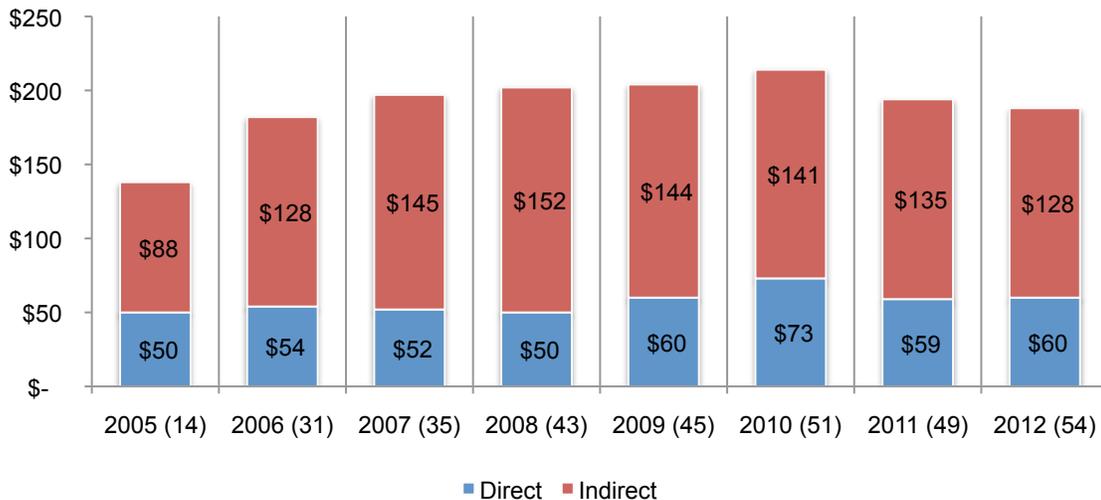
\$000,000 omitted



The proportion of direct and indirect costs of data breach is stable. Direct costs refer to the direct expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services. Indirect costs include the time, effort and other organizational resources spent during the data breach resolution. It includes the use of existing employees to help in the data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn.

Figure 15 reports the direct and indirect cost components of a data breach on a per capita basis. As already noted, the cost of data breach per compromised record decreased by \$6 – from \$194 in 2011 to \$188 in 2012. Direct costs actually increased by \$1 per record, while indirect costs decreased by \$7 from last year.

Figure 15. Direct and indirect per capita data breach cost over eight years



Preventive measures taken after the breach

In addition to measuring specific cost activities relating to the data breach incident, we report in Table 1 the preventive measures implemented by companies after this event. The most popular measures and controls implemented after the data breach have been fairly consistent. They are: the expanded use of encryption, tokenization and other cryptographic solutions (57 percent), additional training and awareness activities (51 percent), data loss prevention tools (49 percent), additional manual procedures and controls (46 percent), identity and access management solutions (43 percent) and endpoint security solutions (40 percent).

This year, the use of encryption and data loss prevention tools increased the most since last year's study. Identity and access management solutions and other system control practices declined among this year's participants.

| Table 1. Preventive measures and controls implemented after the data breach incident | FY 2009 | FY 2010 | FY 2011 | FY 2012 |
|--|---------|---------|---------|---------|
| Expanded use of encryption, tokenization and other cryptographic solutions | 58% | 61% | 52% | 57% |
| Training and awareness programs | 67% | 63% | 53% | 51% |
| Data loss prevention tools | 42% | 43% | 45% | 49% |
| Additional manual procedures and controls | 58% | 54% | 49% | 46% |
| Identity and access management solutions | 49% | 52% | 47% | 43% |
| Endpoint security solutions | 36% | 41% | 42% | 40% |
| Other system control practices | 40% | 43% | 38% | 34% |
| Strengthening of perimeter controls | 20% | 22% | 25% | 23% |
| Security intelligence solutions | 22% | 21% | 26% | 28% |
| Security certification or audit | 33% | 29% | 19% | 19% |

*Please note that a company may be implementing more than one preventive measure.

Cost changes of data breach categories over time

Since first conducting the research there have been interesting shifts in spending on data breaches. For example, legal costs incurred to defend against lawsuits and fines have more than doubled on a percentage basis. Organizations are steadily increasing their investments in investigation and forensics to determine data breach root causes.

Table 2 reports 11 cost categories on a percentage basis over seven years. While certain cost categories have increased, inbound contact costs have decreased from 10 percent in 2006 to 5 percent in both 2011 and 2012.

| Table 2. Percentage data breach cost categories | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|------|------|------|------|------|------|------|
| Investigations & forensics | 8% | 8% | 9% | 8% | 11% | 11% | 12% |
| Audit and consulting services | 10% | 10% | 11% | 12% | 10% | 9% | 8% |
| Outbound contact costs | 9% | 7% | 6% | 6% | 5% | 6% | 5% |
| Inbound contact costs | 10% | 8% | 6% | 5% | 6% | 5% | 5% |
| Public relations/communications | 1% | 3% | 1% | 1% | 1% | 1% | 1% |
| Legal services – defense | 6% | 8% | 9% | 14% | 14% | 15% | 15% |
| Legal services – compliance | 3% | 3% | 1% | 2% | 2% | 3% | 4% |
| Free or discounted services | 2% | 1% | 2% | 1% | 1% | 1% | 1% |
| Identity protection services | 3% | 2% | 2% | 2% | 2% | 3% | 4% |
| Lost customer business | 39% | 41% | 43% | 40% | 39% | 37% | 36% |
| Customer acquisition cost | 8% | 9% | 9% | 9% | 9% | 9% | 9% |
| Total | 100% | 100% | 100% | 100% | 100% | 100% | 100% |

Part 3. Observations and description about participating companies

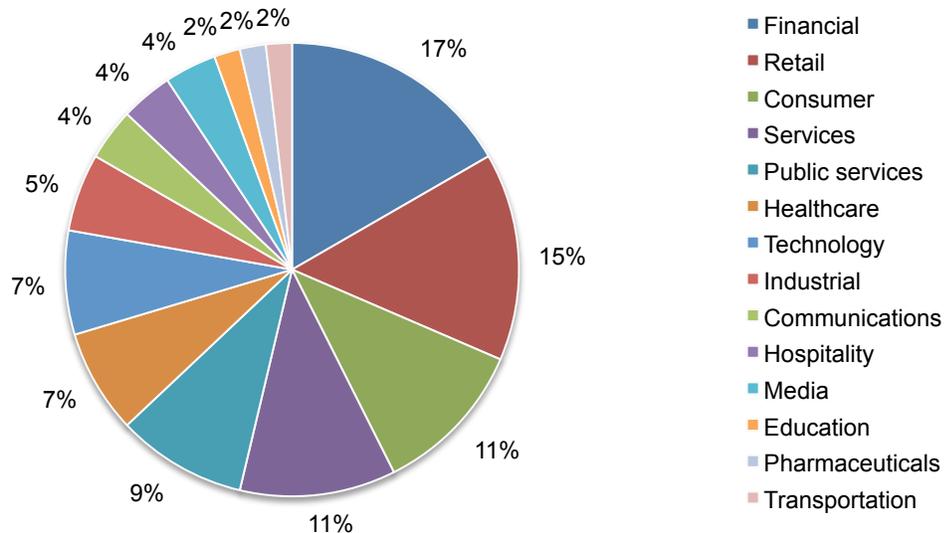
Companies participating in our annual study report that data breaches resulted in a lower rate of churn than in prior years. We conclude that companies' efforts in improving their data protection practices are paying off. As evidenced by the lower cost of data breach, the most profitable investments companies can make seem to be an incident response plan, a strong security posture, the appointment of a CISO with enterprise-wide responsibility and the engagement of outside consultants.

We hope this study helps to understand what the potential costs of a data breach could be based upon certain characteristics and how best to allocate resources to the prevention, detection and resolution of a data breach. Specifically, the study reveals the severe financial consequences from malicious or criminal acts. These data breaches can prove to be the most costly.

In this report, we compare the results of the present study to those from prior years. It is important to note that each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint, and size of data breach.

Figure 16 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 14 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Figure 16. Distribution of the benchmark sample by industry segment



Part 4. How we calculate the cost of data breach

Our study addresses core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. 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 as well as a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we use a cost estimation method that relies on the "lifetime value" of an average customer as defined for each participating organization.

- Turnover 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.⁸
- Diminished 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.

We acknowledge that the loss of non-customer data, such as employee records, may not impact an organization's churn or turnover.⁹ In these cases, we would expect the business cost category to be lower when data breaches do not involve customer or consumer data (including payment transactional information).

⁸In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector entities – where termination is costly or economically infeasible.

⁹In this study, we consider citizen, patient and student information as customer data.

Benchmark methods

All participating organizations experienced one or more data breach incidents sometime over the past year, requiring notification according to U.S. state laws. Our benchmark instrument captured descriptive information from IT, compliance and information security practitioners about the full cost impact of a breach involving the loss or theft of customer or consumer information. It also required these practitioners to estimate opportunity costs associated with program activities.

Estimated data breach cost components were captured on a rating form. In most cases, the researcher conducted follow-up interviews to obtain additional facts, including estimated abnormal churn rates that resulted from the company’s most recent breach event involving 1,000 or more compromised records.¹⁰

Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number line format.

How to use the number line: The number line provided under each data breach cost category is one way to obtain your best estimate for the sum of cash outlays, labor and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

Post your estimate of direct costs here for [presented cost category]

| | | |
|----|--|----|
| LL | <hr style="border: 0; border-top: 1px solid black; margin: 0;"/> | UL |
|----|--|----|

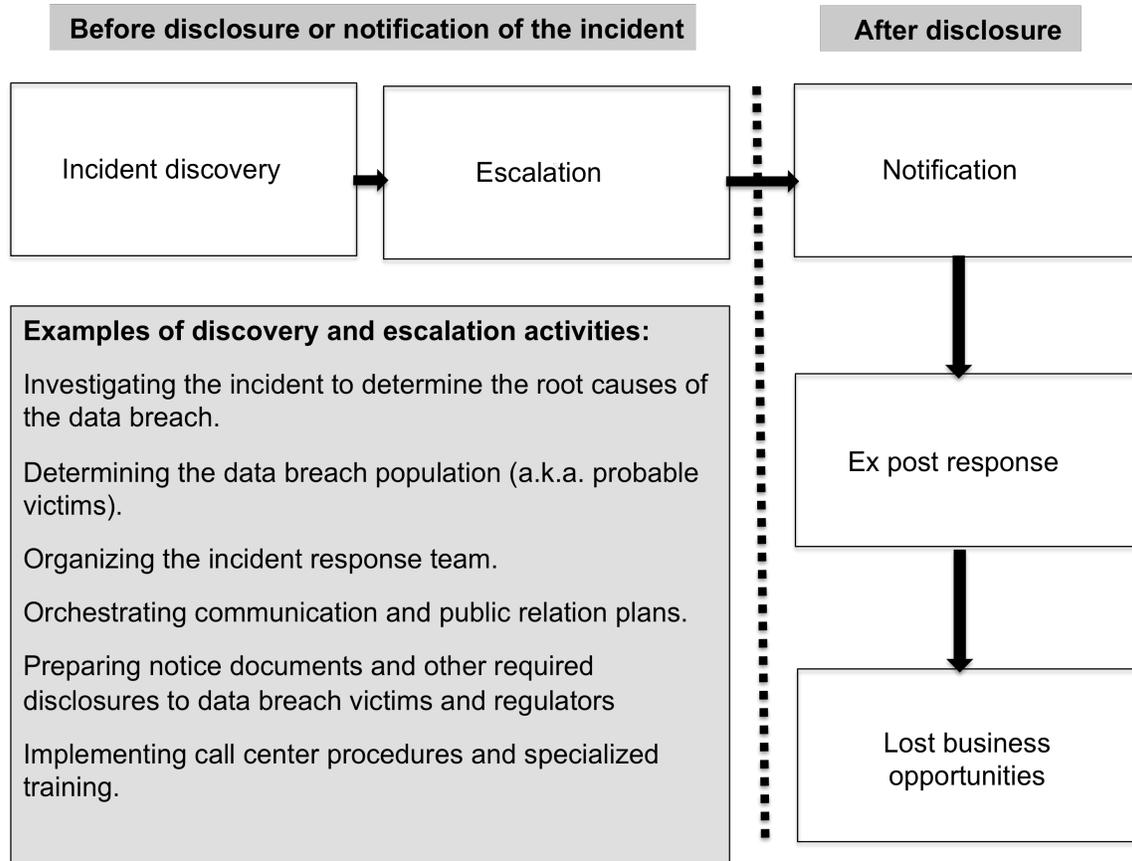
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information. We believed that a study focused on business process – and not data protection or privacy compliance activities – would yield a better quality of results.

¹⁰Our sampling criteria only included companies experiencing a data breach between 1,000 and 100,000 lost or stolen records sometime during the past 12 months. We excluded catastrophic data breach incidents to avoid skewing overall sample findings.

Figure 17 illustrates the activity-based costing schema used in our benchmark study. The cost centers we examine sequentially are: incident discovery, escalation, notification, ex-post response and lost business.

Figure 17. Schema of the data breach process



Within each cost center, the research instrument required subjects to estimate a cost range to capture estimates of 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 benchmark instrument did not capture any company-specific information. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

To keep the benchmarking process to a manageable size, we carefully limited items to only those cost activity centers that we considered crucial to data breach cost measurement. Based upon discussions with learned experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was re-examined carefully for consistency and completeness.

Part 5. Limitations

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

- **Non-statistical results:** Our study draws upon a representative, non-statistical sample of U.S.-based entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.
- **Non-response:** The current findings are based on a small representative sample of benchmarks. Fifty-four companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.
- **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.
- **Unmeasured factors:** To keep the interview script 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 determined.
- **Extrapolated cost results.** The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Appendix 1: Cost for 54 Data Breach Case Studies US\$

| Cases | Size of breach | Detection & escalation | Notification | Ex-post response | Lost business |
|-------|----------------|------------------------|--------------|------------------|---------------|
| 1 | 9,335 | 364,066 | 189,278 | 358,707 | 264,686 |
| 2 | 20,141 | 1,579,326 | 576,346 | 2,329,237 | 2,341,166 |
| 3 | 62,989 | 2,208,575 | 3,334,773 | 5,326,645 | 11,705,611 |
| 4 | 99,039 | 883,036 | 1,104,786 | 4,748,241 | 2,390,900 |
| 5 | 32,311 | 38,135 | 70,054 | 981,639 | 3,747,000 |
| 6 | 55,141 | 1,639,054 | 515,088 | 1,724,872 | 2,454,204 |
| 7 | 26,086 | 58,554 | 2,653,370 | 649,608 | 562,626 |
| 8 | 26,473 | 1,098,352 | 397,448 | 8,087,155 | 2,263,999 |
| 9 | 8,352 | 340,036 | 267,314 | 956,029 | 300,290 |
| 10 | 45,805 | 79,766 | 1,016,691 | 3,985,987 | 8,290,253 |
| 11 | 20,318 | 602,974 | 1,219,214 | 1,635,140 | 8,663 |
| 12 | 9,275 | 112,439 | 518,028 | 579,114 | 1,845,104 |
| 13 | 30,516 | 195,360 | 504,065 | 603,388 | 1,198,914 |
| 14 | 5,428 | 49,229 | 34,267 | 360,632 | 166,829 |
| 15 | 13,108 | 669,739 | 4,226 | 1,113,043 | 1,737,484 |
| 16 | 15,560 | 324,685 | 845,587 | 1,214,765 | 3,993,079 |
| 17 | 22,445 | 120,802 | 545,216 | 613,481 | 8,172,302 |
| 18 | 8,437 | 83,389 | 277,320 | 425,115 | 657,579 |
| 19 | 22,744 | 377,221 | 413,910 | 4,364,387 | 1,151,140 |
| 20 | 41,116 | 432,257 | 203,742 | 956,692 | 4,023,405 |
| 21 | 26,881 | 194,067 | 300,741 | 665,890 | 3,498,802 |
| 22 | 68,694 | 568,199 | 403,942 | 1,641,970 | 8,625,268 |
| 23 | 33,813 | 619,645 | 78,826 | 1,209,552 | 3,618,362 |
| 24 | 20,944 | 198,902 | 166,735 | 1,628,893 | 5,403,873 |
| 25 | 45,397 | 363,617 | 215,691 | 4,036,146 | 6,387,205 |
| 26 | 22,580 | 1,638,219 | 819,082 | 2,367,094 | 2,306,484 |
| 27 | 14,467 | 377,940 | 421,739 | 1,585,999 | 1,843,083 |
| 28 | 5,847 | 69,344 | 401,520 | 248,903 | 66,655 |
| 29 | 11,643 | 344,522 | 815,794 | 1,037,606 | 944,757 |
| 30 | 32,510 | 536,300 | 265,127 | 329,896 | 2,078,346 |
| 31 | 34,215 | 44,419 | 1,450,211 | 336,064 | 694,992 |
| 32 | 14,296 | 59,900 | 131,506 | 787,462 | 1,235,826 |
| 33 | 7,157 | 112,134 | 348,677 | 389,701 | 624,038 |
| 34 | 8,024 | 232,193 | 395,454 | 1,026,003 | 1,300,706 |
| 35 | 20,509 | 33,174 | 758,021 | 52,891 | 2,664,181 |
| 36 | 18,548 | 198,307 | 112,254 | 292,486 | 1,118,788 |
| 37 | 23,011 | 471,902 | 441,449 | 573,480 | 2,112,333 |
| 38 | 34,088 | 653,731 | 662,558 | 1,750,066 | 6,573,526 |
| 39 | 29,901 | 138,163 | 410,558 | 1,616,675 | 4,943,183 |
| 40 | 43,818 | 130,755 | 277,503 | 783,157 | 3,332,654 |
| 41 | 27,537 | 41,460 | 131,791 | 1,030,176 | 7,170,135 |
| 42 | 20,867 | 80,767 | 931,384 | 110,173 | 343,877 |
| 43 | 29,051 | 346,403 | 398,393 | 1,576,017 | 2,212,560 |
| 44 | 26,843 | 127,272 | 346,307 | 1,695,547 | 5,075,473 |
| 45 | 26,514 | 191,785 | 262,564 | 830,021 | 3,234,841 |
| 46 | 22,634 | 31,973 | 115,849 | 1,236,711 | 7,067,481 |
| 47 | 17,783 | 85,486 | 945,020 | 129,850 | 485,155 |
| 48 | 44,576 | 194,422 | 590,850 | 1,735,054 | 1,398,915 |
| 49 | 92,693 | 28,073 | 4,756 | 594,396 | 4,880,773 |
| 50 | 5,071 | 204,753 | 618,319 | 284,793 | 321,144 |
| 51 | 58,844 | 160,155 | 800,542 | 2,882,162 | 7,624,786 |
| 52 | 16,976 | 1,196,711 | 413,248 | 322,688 | 2,932,873 |
| 53 | 10,878 | 66,583 | 111,694 | 169,647 | 2,387,792 |
| 54 | 62,106 | 345,866 | 1,272,251 | 306,534 | 1,879,856 |

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
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.