



2011 Cost of Data Breach Study: United States

Benchmark Research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
March 2012

2011 Cost of Data Breach Study: United States

Ponemon Institute, March 2012

Part 1. Introduction

Symantec Corporation and Ponemon Institute are pleased to present *2011 Cost of Data Breach Study: United States*, our seventh annual benchmark study concerning the cost of data breach incidents for U.S.- based companies. 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 has declined from \$214 to \$194.

Since Ponemon Institute began studying this issue, more than 45 states have enacted laws requiring the owners of personal information databases to inform affected individuals in the event of a data security breach. As a result, we believe organizations are taking the protection of sensitive and confidential data more seriously in order to avoid costly fines and loss of reputation and brand.

This year's study examines the costs incurred by 49 U.S. companies in 14 different industry sectors after those companies experienced the loss or theft of protected personal data and then had to notify breach victims as required by law. Results are not based upon hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. More than 400 individuals were interviewed over a nine-month period. To date, 268 organizations have participated in this research.

The number of breached records per incident this year ranged from approximately 4,500 records to more than 98,000 records. This year the average size of breached records was 28,349. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and including them in the study would skew the results. The cost for the 49 data breach case studies in this year's report is presented in Appendix 1.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States seven years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia and, for the first time this year, India, Italy and Japan. 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, rates.

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

- **The cost of data breach declined.** For the first time in seven years, both the organizational cost of data breach and the cost per lost or stolen record have declined. The organizational cost has declined from \$7.2 million to \$5.5 million and the cost per record has declined from \$214 to \$194. We define a record as information that identifies an individual whose information has been compromised in a data breach.

This decline suggests that organizations represented in this study have improved 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.** For the first time, fewer customers are abandoning companies that have a data breach. However, certain industries are more susceptible to customer churn, which causes their data breach costs to be higher

than the average. Taking steps to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.

- **Negligent insiders and malicious attacks are the main causes of data breach.** Thirty-nine percent of organizations say that negligence was the root cause of the data breaches. For the first time, malicious or criminal attacks account for more than a third of the total breaches reported in this study. Since 2007, they also have been the most costly breaches. Accordingly, organizations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker.
- **Lost business costs declined sharply from \$4.54 million in 2010 to \$3.01 million in 2011.** 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 seven years we studied this aspect of a data breach, the highest cost for lost business was \$4.59 million in 2008 and the lowest was \$2.34 million in 2005.
- **Certain organizational factors reduce the overall cost.** If the organization has a CISO with overall responsibility for enterprise data protection the average cost of a data breach can be reduced as much as \$80 per compromised record. Outside consultants assisting with the breach response also can save as much as \$41 per record. 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, in this year's study organizations that had their first ever data breach spent on average \$37 more per record. Or, those that responded and notified customers too quickly without a thorough assessment of the data breach also paid an average of \$33 more per record. Data breaches caused by third parties or a lost or stolen device increased the cost by \$26 and \$22, respectively.
- **Detection and escalation costs declined but notification costs increased.** Detection and escalation costs declined from approximately in \$460,000 in 2010 to \$433,000 in 2011. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion. This suggests that organizations in 2011 study had the appropriate processes and technologies to execute these activities.

Notification refers to the steps taken to report the breach of protected information to appropriate personnel within a specified time period. The costs to notify victims of the breach increased in this year's study from approximately \$510,000 to \$560,000. A key factor is the increase in laws and regulations governing data breach notification.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews with more than 400 individuals conducted over a nine-month period. Recruiting organizations for the 2011 study began in January 2011 and interviews were completed in December. In each of the 49 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 paid 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 the individual. As discussed previously, we recruited 49 organizations to participate in this study.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as the ones experienced by Sony or Epsilon?

The average cost of a data breach in our research does not apply to catastrophic breaches. Primarily because these are not typical of the breaches most organizations experience. In order to be representative of the population of U.S. 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.

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 268 U.S. organizations.

Part 2. Key Findings

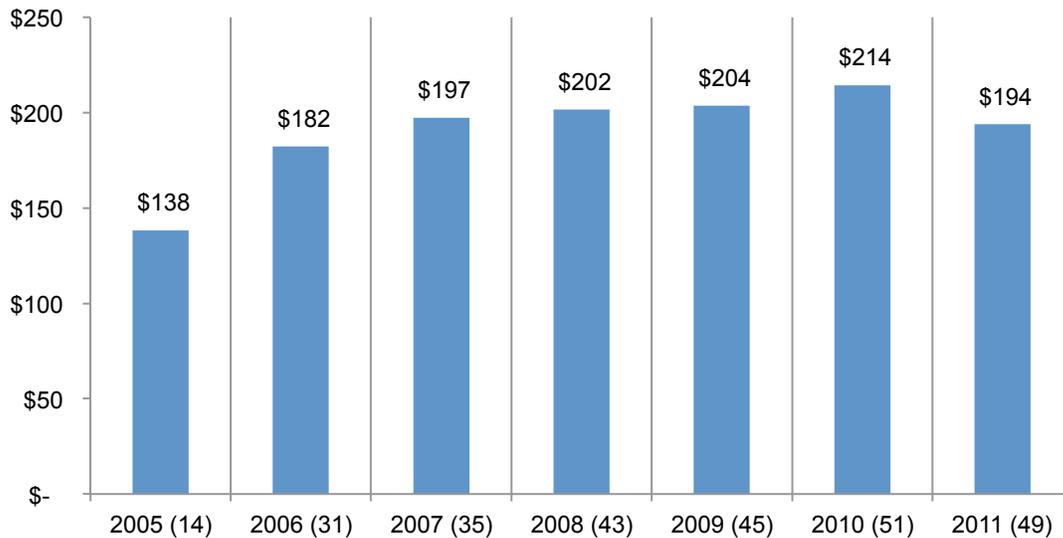
In this section we provide the detailed findings of this research. Topics are presented in the following order:

- Cost of data breach: per record, organizational and industry
- Root causes of a data breach
- Attributes 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 costs: detection and escalation, notification, lost business, direct and indirect and post-data breach
- Trends in the Security Effectiveness Score for benchmarked organizations

The cost of data breach declines. For the first time in seven years, the cost of data breach actually decreased. Figure 1 reports the average per capita cost of a data breach since the inception of this research series seven years ago.¹ According to this year’s benchmark findings, data breaches cost companies an average of \$194 per compromised record – of which \$135 pertains to indirect costs including abnormal turnover or churn of existing and future customers. Last year’s average per capita cost was \$214 with an average indirect cost of \$141.

Figure 1: The average per capita cost of data breach over seven years

Bracketed number defines the benchmark sample size



¹Per 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.

² Negligent insiders are individuals who cause a data breach because of their carelessness, as determined

Average organizational cost of data breach declined. Figure 2 shows that the total average cost of data breach over seven years actually decreased from \$7.2 million to \$5.5 million – or, a 24 percent decline between 2010 and 2011 results. This suggests that organizations are making significant improvements in how they prevent and respond to a data breach.

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



Containing the size of the breach and improving the response to the incident result in lower data breach costs. If cost is an indicator of performance, the findings of our 2011 study suggest organizations have improved their ability to contain the size of the breach and response to data breach incidents to stop churn.

Figure 3 reports the four key metrics that provide reasons for the improvement. As we have discussed, the average total cost of a data breach decreased by 24 percent and the average per capita cost decreased by 10 percent. Factors that contributed to these positive results are a decrease in abnormal turnover of existing customers and fewer lost or stolen records.

Figure 3: Reasons for the decline in cost

Net change defined as the difference between the 2011 and 2010 results

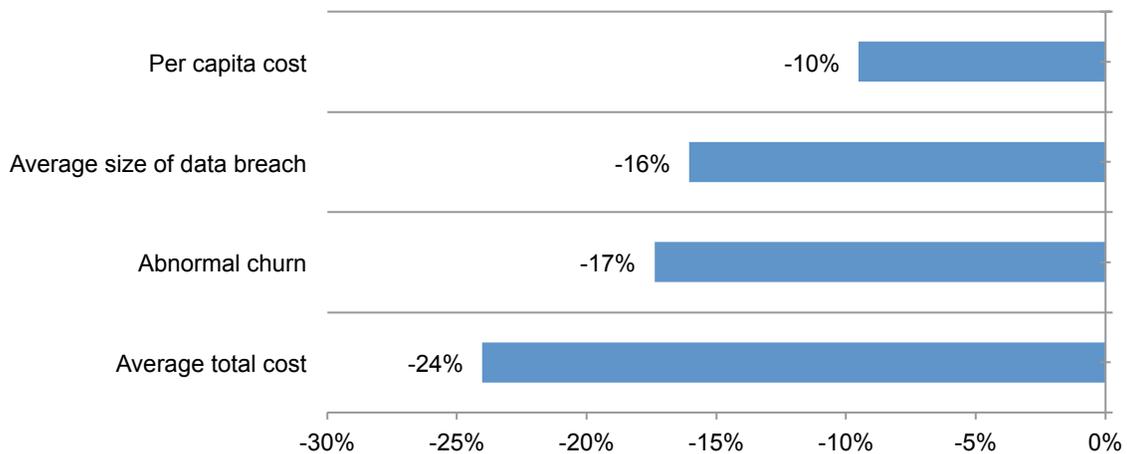
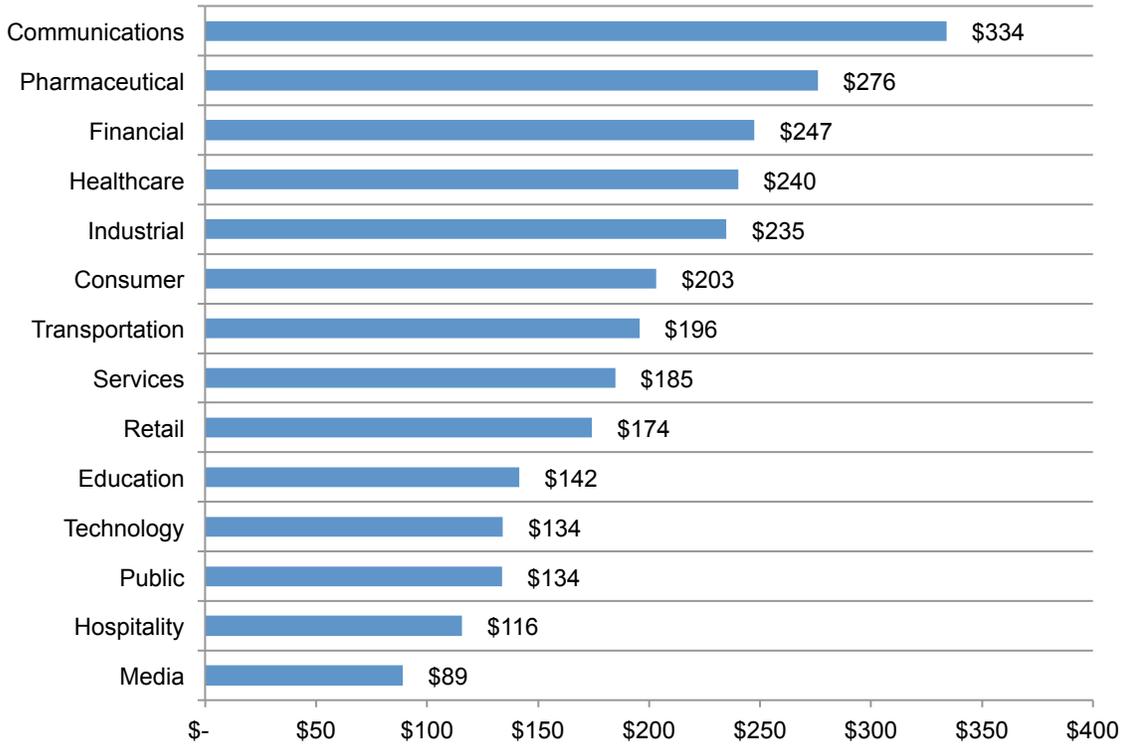


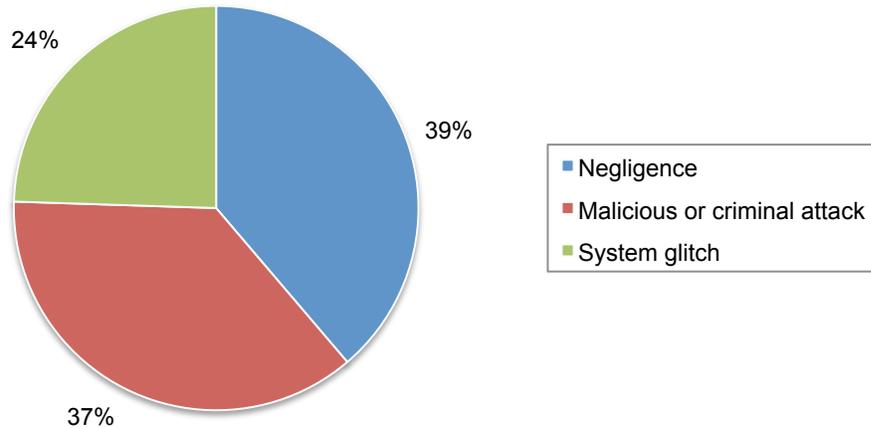
Figure 4 reports the per capita costs for the 2011 study by industry classification. While small sample size prevents us from generalizing industry cost differences, the pattern of 2011 industry results is consistent with prior years. Accordingly, financial service companies tend to have a per capita cost above the mean (\$247) and retail companies have a per capita cost below the mean (\$174).

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



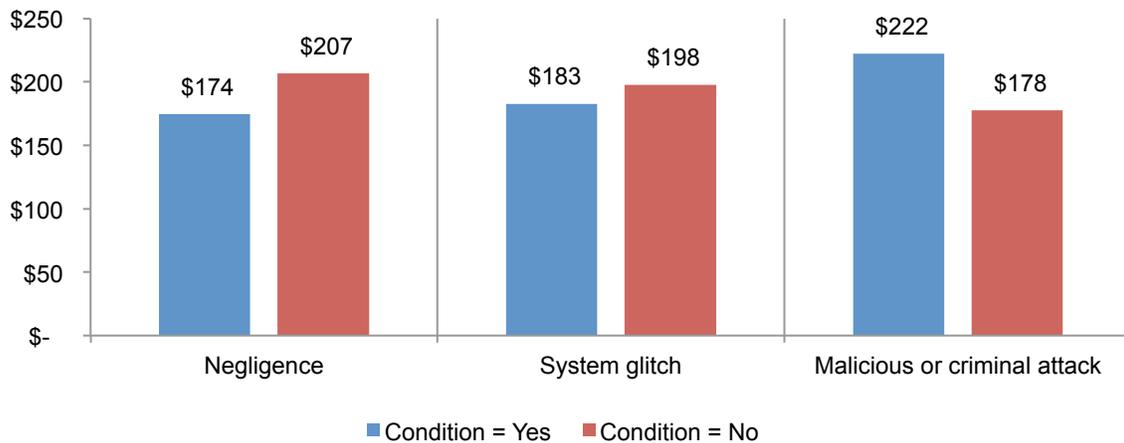
Negligent employees and malicious attacks are most often the cause of the data breach.² Figure 5 provides a summary of the main root causes of data breach for all 49 organizations. Thirty-nine percent of incidents involved a negligent employee or contractor, 37 percent concerned a malicious or criminal attack, and 24 percent involved system glitches including a combination of both IT and business process failures.³

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



Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically cause the data breach as determined by the post data breach investigation. Figure 6 reports per capita cost of data breach for three conditions or root causes of the breach incident. Again, the pattern of results in 2011 is consistent with prior years, when the most costly breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experience malicious or criminal attacks have a per capita cost above the mean (\$222) and companies experiencing negligence have a per capita cost below the mean (\$174).

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



² Negligent 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).

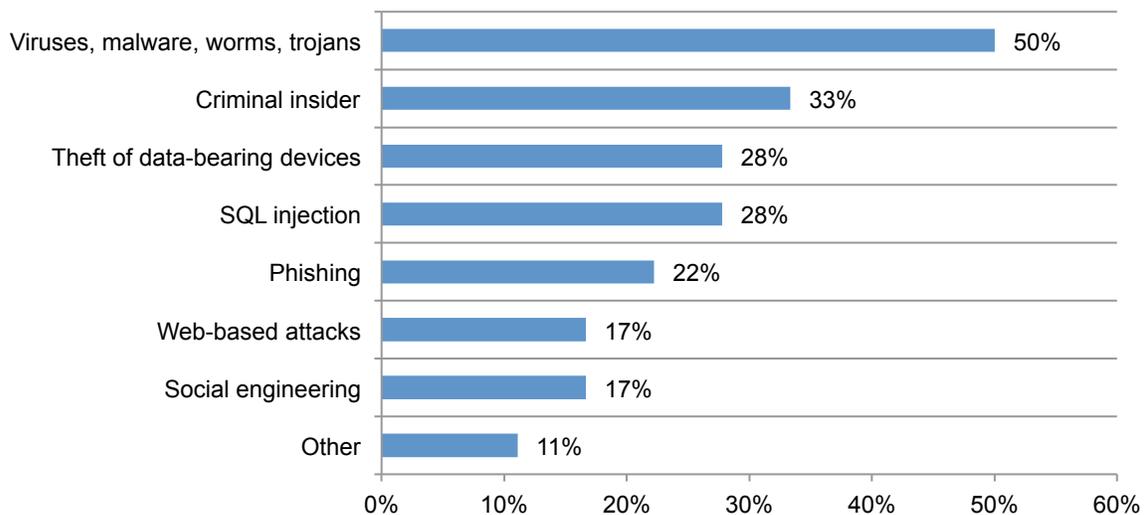
³ Malicious and criminal attacks increased from 31 percent in our 2010 study.

Criminal attacks are mainly electronic agents. In this year’s report, we analyzed the findings from the 18 organizations that report their data breach was caused by a malicious insider or hacker as previously described. Figure 7 summarizes the types of criminal attacks experienced. Please note that a given company might have experienced two or more of these attacks.

As shown, 50 percent of the subsample experienced electronic agents such as viruses, malware, worms and trojans. Thirty-three percent experienced criminal insiders such as rogue employees or contractors. Other major conditions include the theft of data-bearing devices (28 percent), SQL injection (28 percent) and phishing (including spear phishing) (22 percent) attacks.

Figure 7. Analysis of malicious or criminal attacks experienced by 18 companies

More than one attack type may exist for each company



Six positive and negative attributes can influence the cost of data breach. Over the years of conducting this research, we have identified six attributes that can influence the cost of data breach. The percent of organizations in this study that have these attributes are shown in Figure 8. These attributes are defined as follows:

- **CISO (or equivalent title) has overall responsibility for enterprise data protection.** Forty-three percent have centralized the management of data protection with the appointment of a C-level security professional.
- **Data was lost or stolen due to a third party flub.** Forty-one percent of organizations had a data breach caused by a third party. This can include when protected data is in the hands of outsourcers, cloud providers and business partners.
- **The organization notified data breach victims quickly.** Forty-one percent notified victims within 30 days or less.
- **The data breach involved lost or stolen devices.** Thirty-nine percent of organizations had a data breach as a result of a lost or stolen mobile device, which included laptops, smartphones, tablets and USB drives that contained confidential and sensitive information.
- **Consultants are engaged to help remediate the data breach.** Thirty-seven percent of organizations represented in this study hired consultants to assist in their data breach response and remediation.

- **It is the first time the organization had a data breach.** Most of the organizations in this year's study have already experienced a data breach. Only 22 percent say it is the first time.

Figure 8. Percentage of organizations with defining attributes

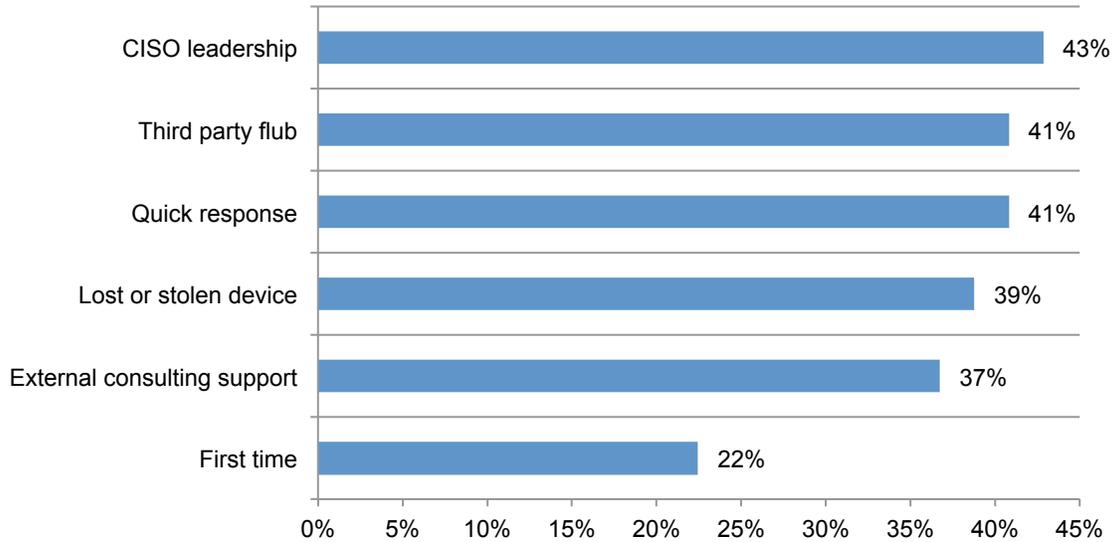


Figure 9 summarizes the per capita costs for six normatively important conditions or attributes about the benchmark sample. As previously mentioned, these attributes were selected based on learned experiences from previous cost benchmark studies.

Per capita costs are above the mean for first timers, quick responders, those experiencing a third party flub and those experiencing a lost or stolen device. Per capita costs are below the mean for organizations engaging external consultants and having an information security leader (CISO) with enterprise-wide responsibility for data protection.

Figure 9. Per capita cost for six attributes or conditions

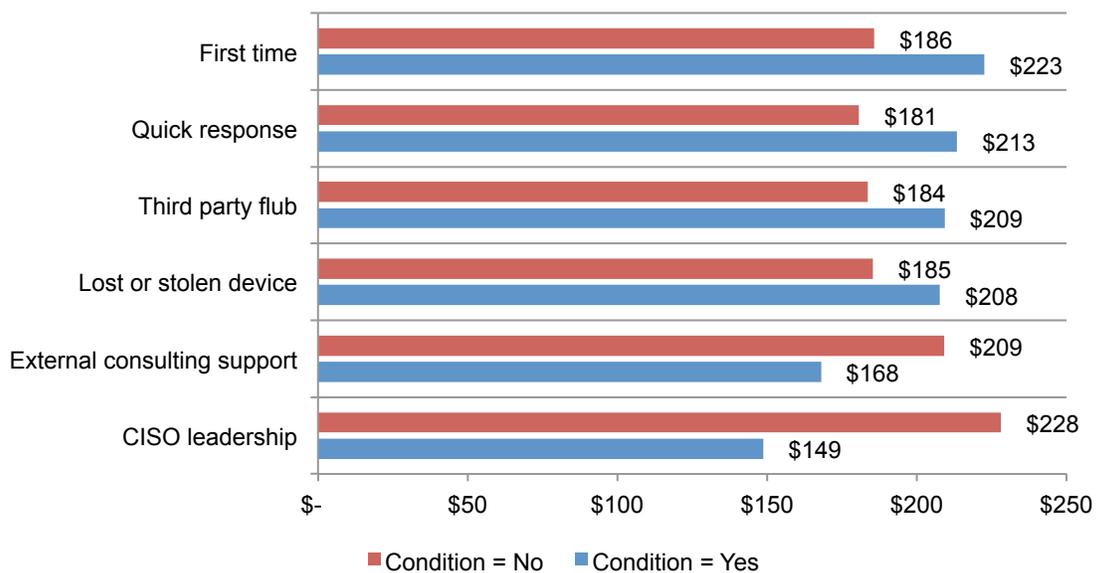
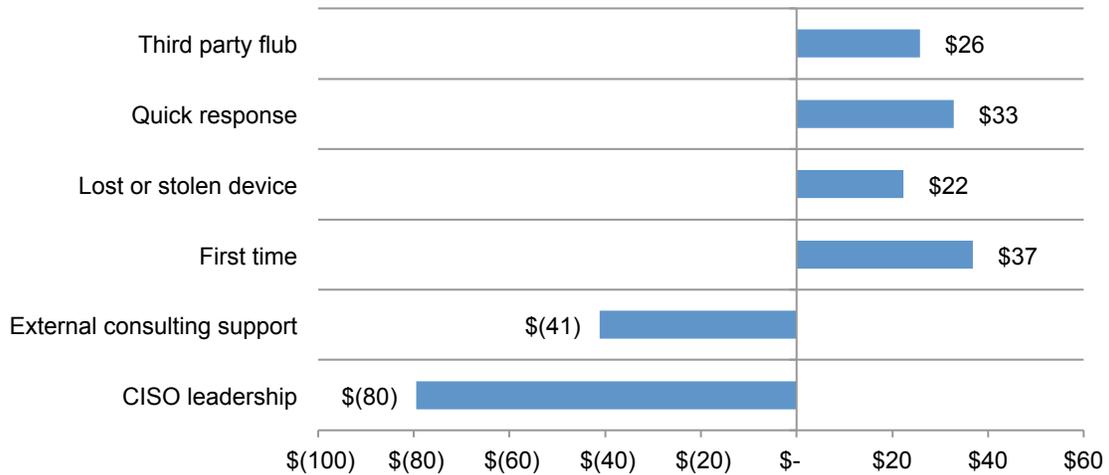


Figure 10 summarizes the per capita cost differences for six normatively important conditions or attributes about the benchmark sample. In this analysis, a negative difference means that the attribute or condition moderates (lessens) the data breach costs. A positive difference means the opposite.

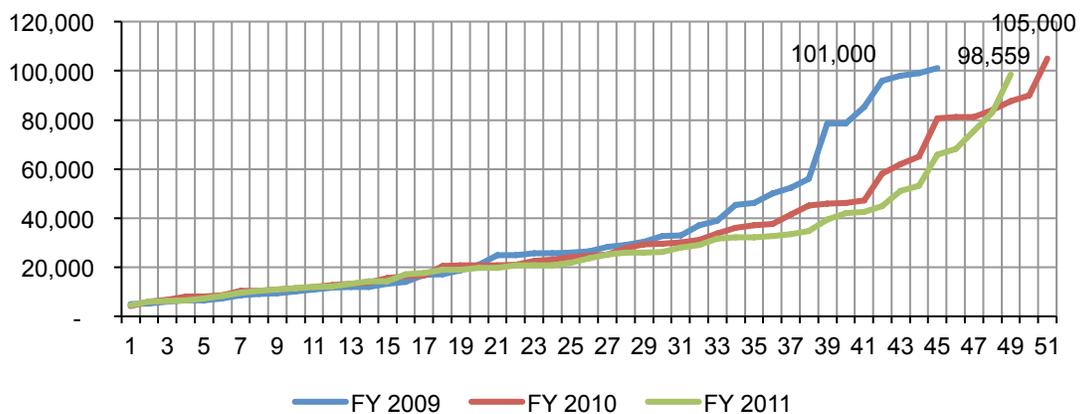
As can be seen, organizations that employ a CISO with enterprise-wide responsibility for data protection experience an \$80 cost saving per compromised record. Organizations engaging an external consultant enjoy a \$41 cost saving.

Figure 10. Per capita cost differences for six attributes or conditions



On average, fewer records were lost or stolen. Figure 11 shows, in ascending order, the number of lost or stolen records involved in data breach incidents included in studies conducted over the past three years. According to the figure, the number of compromised records has remained consistent since 2009. The benchmark samples do not contain data breach incidents involving millions of compromised records. In our experience, these so-called “mega breaches” are rare events and including them would skew results. The largest data breach incident in this year’s study involved 98,559 records.

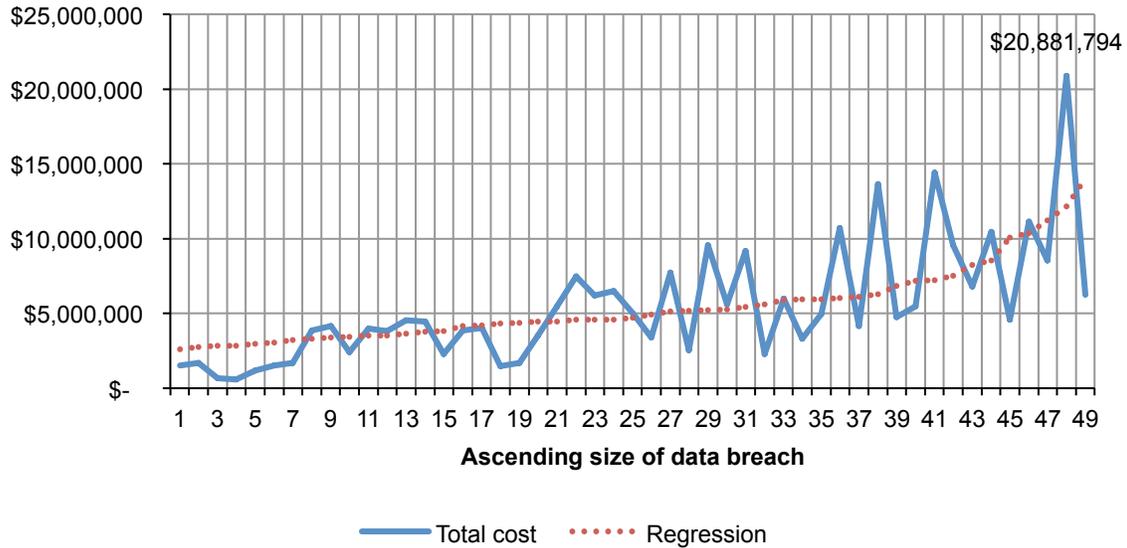
Figure 11. Ascending frequency of compromised records over three years



The more records lost, the higher the cost of the data breach. Figure 12 shows the relationship between the total cost of data breach and the size of the incident for 49 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 \$566,208 to \$20,881,794.

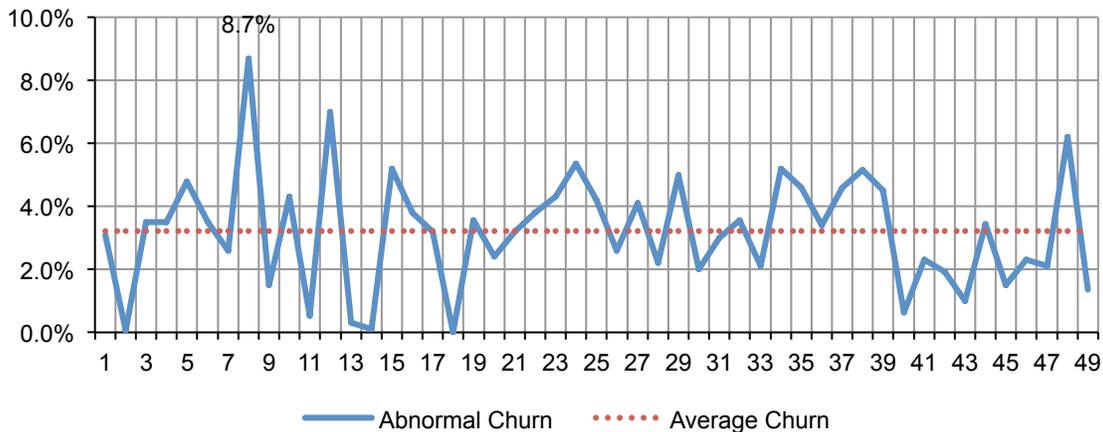
Figure 12. Total cost of data breach by size of lost or stolen records

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



More customers remain loyal to organizations following a data breach. Figure 13 shows the abnormal churn rates for each one of the 49 organizations included in this research. As shown, the churn rate distribution is varied, with a range of 0 (no abnormal churn) to 8.7 percent. It is important to note that the average abnormal churn decreased from 3.9 percent in the 2010 study to 3.2 percent this year.

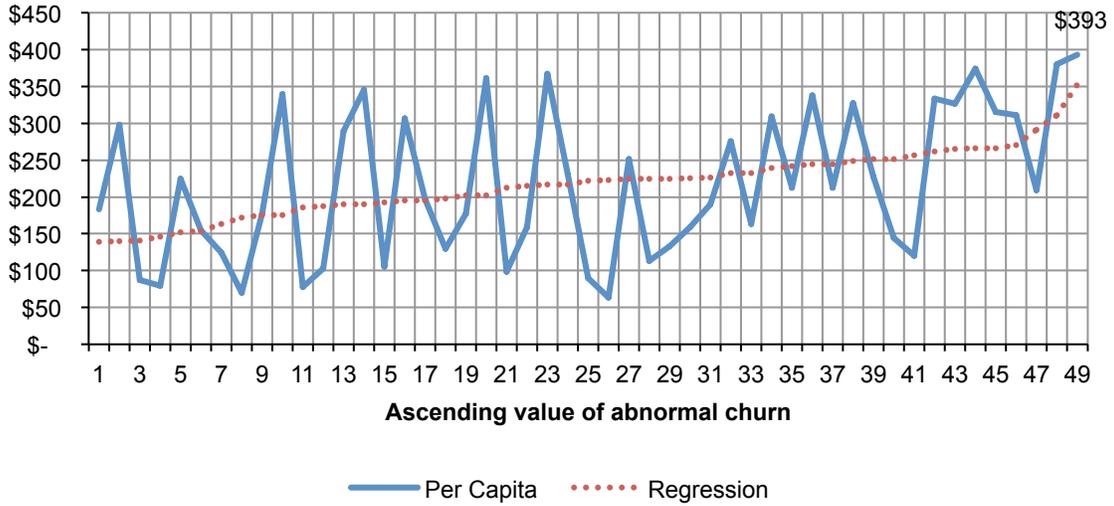
Figure 13. Distribution of abnormal churn rates for 49 benchmark companies



The more churn, the higher the cost of data breach. Figure 14 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. This pattern of results is consistent with benchmark studies completed in prior years.

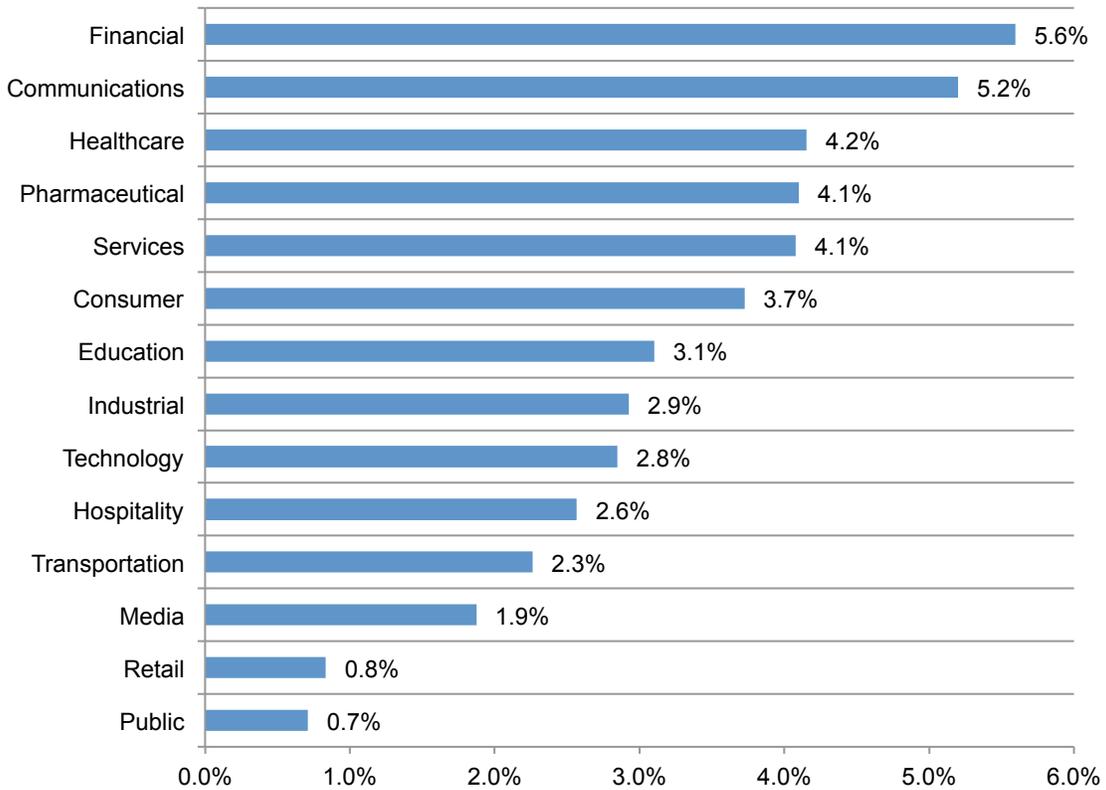
Figure 14. Distribution of per capita costs in ascending value of abnormal churn rates

Regression = Intercept + {Abnormal Churn} x β , where β denotes the slope.



Certain industries are more vulnerable to churn. Figure 15 reports the abnormal churn rate of benchmarked organizations for the 2011 study. While small sample size prevents us from generalizing the affect of industry on data breach cost, our 2011 industry results are consistent with prior years – wherein financial service organizations tend to experience relatively high abnormal churn and retail companies tend to experience a relatively low abnormal churn.⁴ 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 maintain reputation and brand.

Figure 15. Abnormal churn rates by industry classification of benchmarked companies

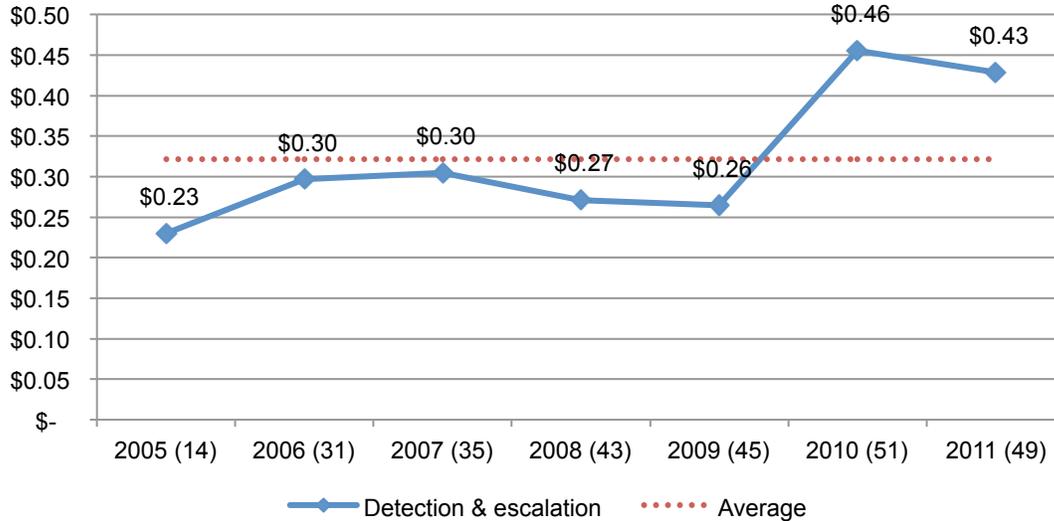


⁴Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Detection and escalation costs are lower. Figure 16 shows the distribution of costs associated with detection and escalation of the data breach event. 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 cost declined from its high of \$455,304 in 2010 to \$428,330 in the present study. This finding suggests that greater efficiencies in investigating the data breach and more certainty over the root cause of the breach.

Figure 16. Average detection and escalation costs over seven years

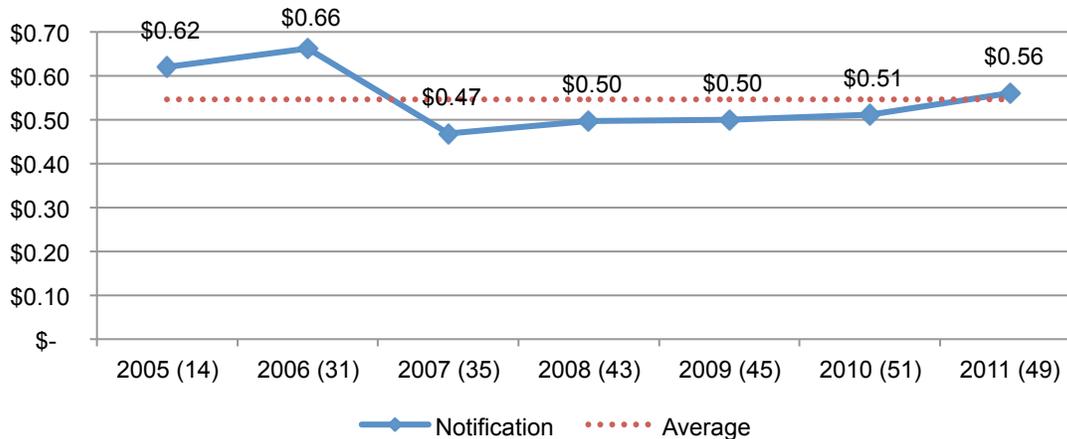
\$000,000 omitted



Notification costs increase. Figure 17 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 \$511,454 in 2010 to \$561,495. The highest notification cost over seven years was \$662,269, which occurred in 2006. This increase could be attributed to the fact that more than 45 states have data breach notification laws and there are other regulatory requirements.

Figure 17. Average notification costs over seven years

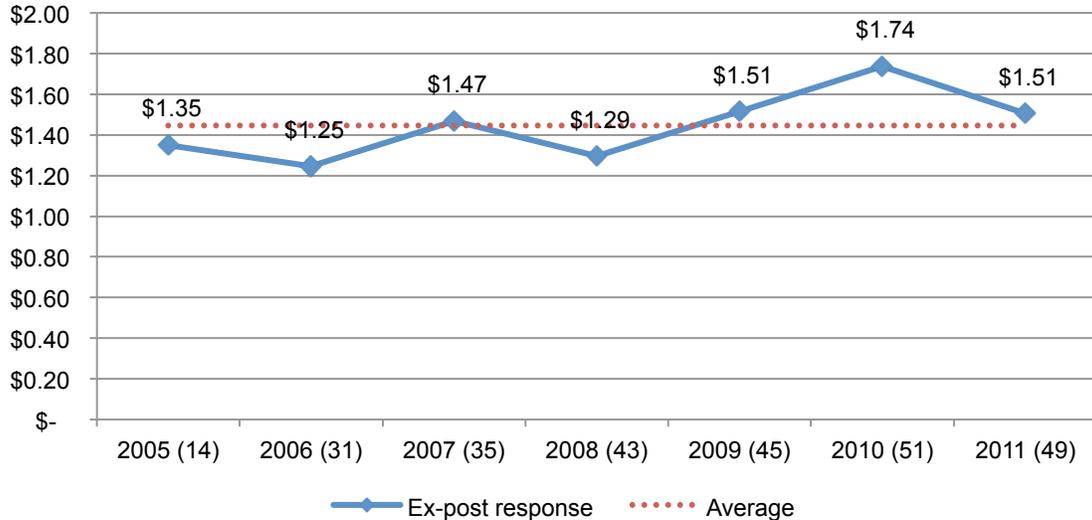
\$000,000 omitted



Post data breach costs decline. Figure 18 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 a seven-year high of \$1,738,761 in 2010 to \$1,505,049 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 as offers of discounts or identity protection services.

Figure 18. Average ex-post response costs over seven years

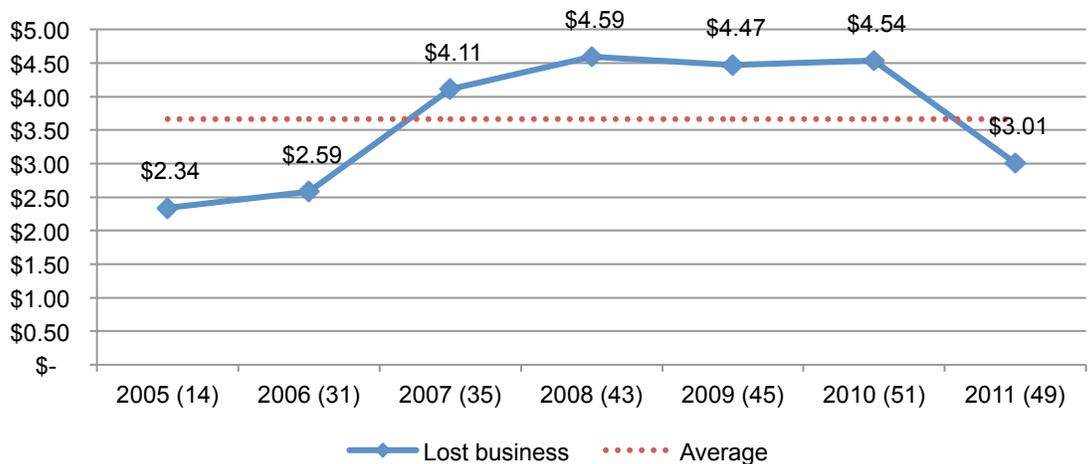
\$000,000 omitted



Lost business costs declined sharply. Figure 19 reports lost business costs associated with data breach incidents over seven years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs sharply decreased from \$4,536,380 in 2010 to \$3,007,015. The highest cost for lost business during the seven years is \$4,592,214, which occurred in 2008.

Figure 19. Average lost business costs over seven years

\$000,000 omitted

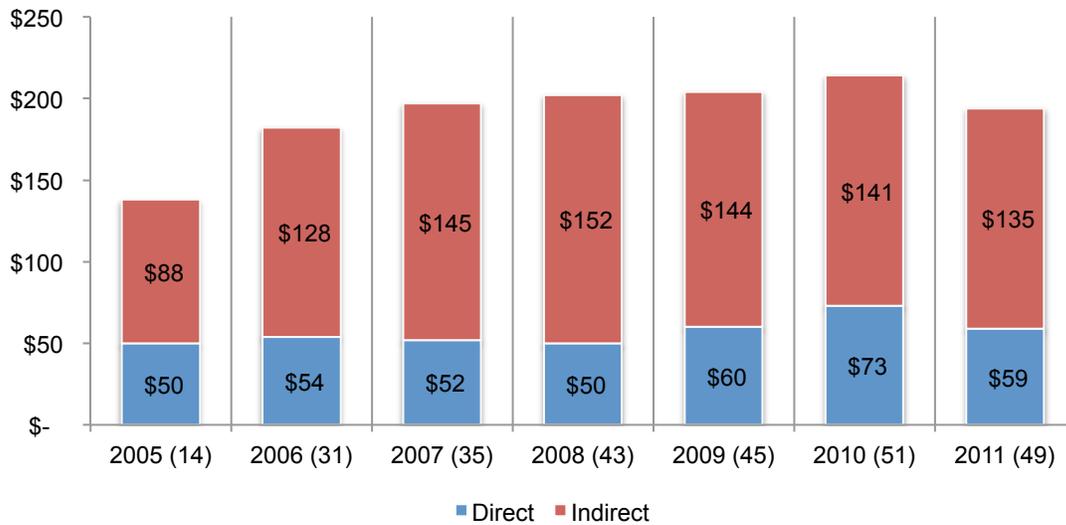


Direct costs of data breach declined but indirect costs increased. For purposes of this study, direct costs refer to the direct expense outlay to accomplish a given activity such as hiring a law firm or offering victims identity protection services. Indirect costs are related to the amount of time, effort and other organizational resources spent such as using existing employees to help in the data breach notification efforts or in the investigation of the incident.

Figure 20 reports the direct and indirect cost components of data breach on a per capita basis. In essence, the cost of data breach per compromised record decreased by \$20 – from \$214 in 2010 to \$194 in 2011.

Approximately, \$14 (70 percent) of this decrease pertains to direct cost. In the present study, indirect cost represents 70 percent of total per capita cost, which is an increase from 66 percent in 2010.

Figure 20. Direct and indirect per capita data breach cost over seven years



Organizations with a positive security posture are more successful in reducing the impact of a data breach. We measured the security posture of each participating company using the Security Effectiveness Score (SES) as part of the benchmarking process.⁵ Figure 21 reports the SES Index for 49 organizations. The SES range of possible scores is +2 (most favorable) to -2 (least favorable). Compiled results for the present benchmark sample vary from a high of +1.84 to a low of -1.13, with a mean value at +0.157.

Figure 21. Distribution of Security Effectiveness Scores for 49 benchmark companies

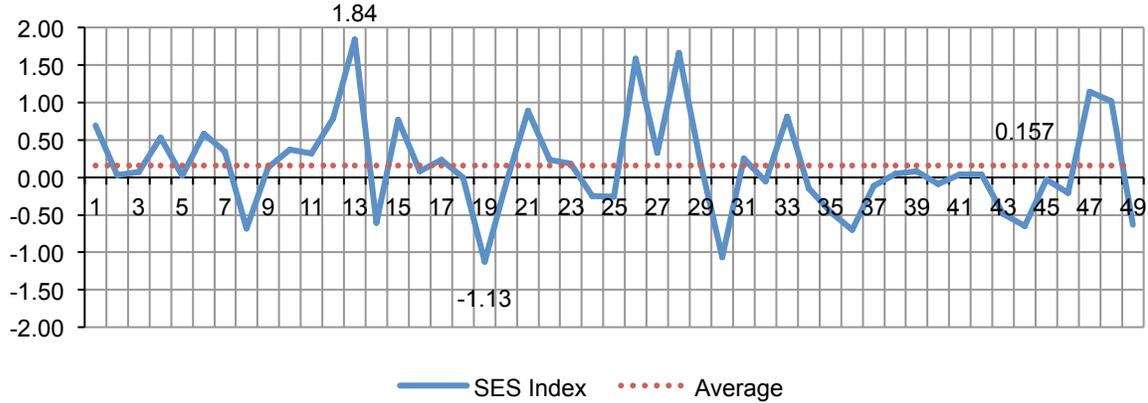
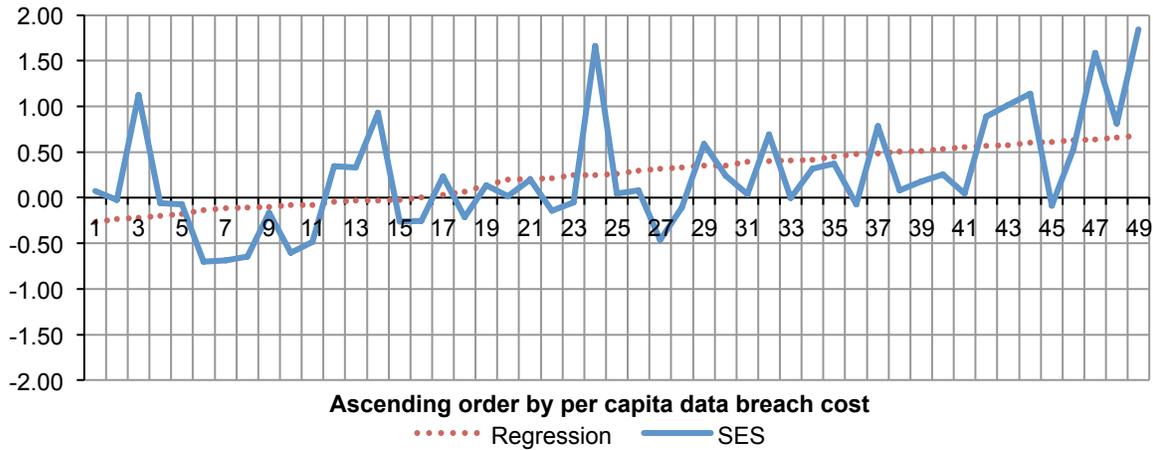


Figure 22 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, suggesting that the Security Effectiveness Score (SES) for each organization is inversely related to their per capita data breach cost. In other words, a strong security posture appears to moderate data breach costs.

Figure 22. Security Effectiveness Score (SES) in ascending value of per capita cost

Regression = Intercept + {Per Capita Cost} x β , where β denotes the slope.



⁵ The 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.

After the Breach

In addition to measuring specific cost activities relating to the leakage of personal information, we report in Table 1 the preventive measures implemented by companies after the data breach. The top preventive measures and controls implemented after the data breach are: additional training and awareness activities (53 percent), expanded use of encryption (52 percent), additional manual procedures and controls (49 percent), identity and access management solutions (47 percent) and data loss prevention technologies (45 percent).

Table 1. Preventive measures and controls implemented after the data breach	FY 2009	FY 2010	FY 2011
Training and awareness programs	67%	63%	53%
Additional manual procedures and controls	58%	54%	49%
Expanded use of encryption	58%	61%	52%
Identity and access management solutions	49%	52%	47%
Data loss prevention (DLP) solutions	42%	43%	45%
Other system control practices	40%	43%	38%
Endpoint security solutions	36%	41%	42%
Security certification or audit	33%	29%	19%
Security event management systems	22%	21%	26%
Strengthening of perimeter controls	20%	22%	25%

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

Table 2 provides the percentage changes for 11 cost categories over six years. As can be seen, most cost categories appear to be relatively stable over time. However, legal defense costs have steadily increased from 6 percent in 2006 to 15 percent in 2011. In contrast, inbound contact costs have decreased from 10 percent in 2006 to 5 percent in 2011.

Table 2. Cost changes over six years	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
Investigations & forensics	8%	8%	9%	8%	11%	11%
Audit and consulting services	10%	10%	11%	12%	10%	9%
Outbound contact costs	9%	7%	6%	6%	5%	6%
Inbound contact costs	10%	8%	6%	5%	6%	5%
Public relations/communications	1%	3%	1%	1%	1%	1%
Legal services - defense	6%	8%	9%	14%	14%	15%
Legal services - compliance	3%	3%	1%	2%	2%	3%
Free or discounted services	2%	1%	2%	1%	1%	1%
Identity protection services	3%	2%	2%	2%	2%	3%
Lost customer business	39%	41%	43%	40%	39%	37%
Customer acquisition cost	8%	9%	9%	9%	9%	9%
Total	100%	100%	100%	100%	100%	100%

Part 3. Observations and description about participating companies

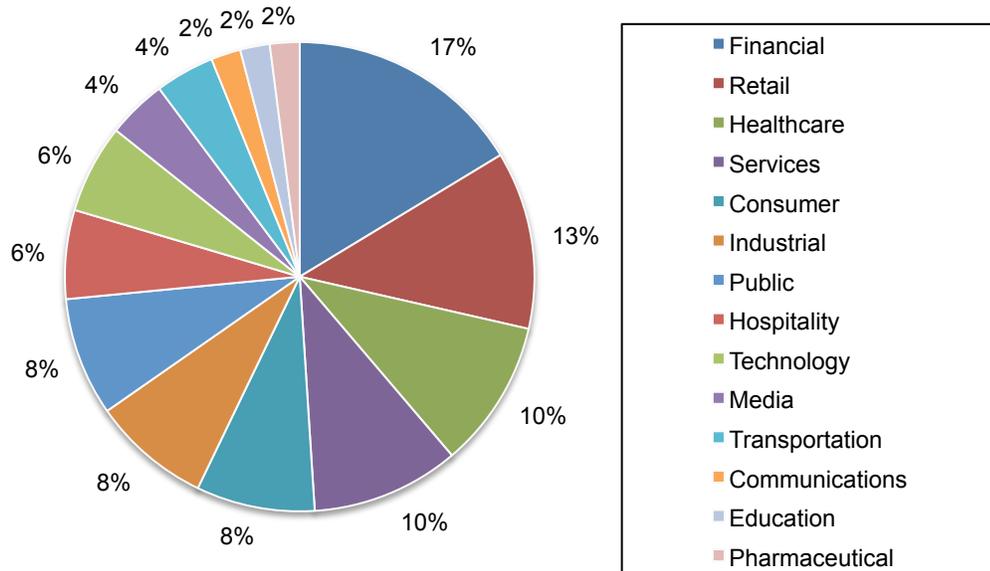
For the first time, companies participating in our annual study report that their data breaches were smaller in scale and resulted in a lower rate of churn. We conclude that companies' investment in improving their data protection practices is paying off. The most profitable investments as evidenced by the lower cost of a data breach are the appointment of a CISO with enterprise-wide responsibility and the engagement of external consultants.

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

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 23 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 23. 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.⁶
- 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.⁷ 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).

⁶In 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.

⁷In 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.⁸

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		UL
----	---	----

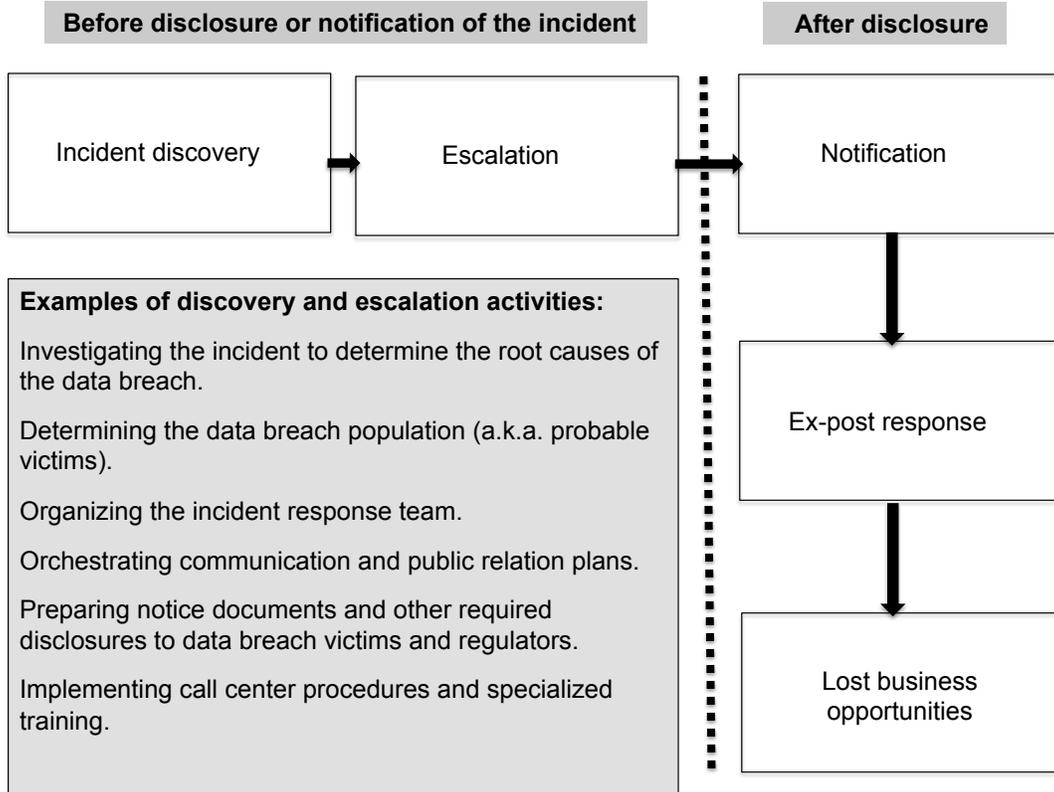
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

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.

⁸Our 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 24 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 24: 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. Forty-nine 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.

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.

Appendix 1: Cost for 49 Data Breach Case Studies

Cases	Size of breach	Detection & escalation	Notification	Ex-post response	Lost business	Abnormal Churn
1	7,415	\$364,066	\$189,278	\$358,707	\$264,686	3.1%
2	20,781	\$1,516,498	\$558,995	\$2,135,823	\$1,981,035	0.1%
3	83,000	\$2,265,031	\$3,204,274	\$5,868,852	\$9,543,637	3.5%
4	75,466	\$999,900	\$1,030,174	\$4,551,834	\$1,969,169	3.5%
5	39,475	\$33,228	\$93,451	\$1,103,867	\$3,523,665	4.8%
6	51,000	\$1,610,856	\$539,960	\$1,968,853	\$2,668,352	3.5%
7	19,772	\$48,491	\$2,016,702	\$834,161	\$608,020	2.6%
8	34,739	\$1,608,744	\$350,970	\$8,620,766	\$3,083,080	8.7%
9	9,570	\$271,727	\$262,243	\$914,804	\$244,694	1.5%
10	42,632	\$89,961	\$887,069	\$4,228,653	\$9,189,517	4.3%
11	17,257	\$564,248	\$1,035,506	\$2,260,950	\$10,599	0.5%
12	10,985	\$117,648	\$674,183	\$835,205	\$2,547,427	7.0%
13	29,123	\$196,368	\$457,753	\$570,411	\$1,082,466	0.3%
14	6,500	\$59,775	\$43,615	\$316,967	\$145,851	0.1%
15	10,368	\$601,642	\$3,968	\$1,219,309	\$2,057,552	5.2%
16	19,826	\$294,363	\$692,840	\$1,240,986	\$3,237,872	3.8%
17	26,003	\$136,290	\$473,677	\$765,987	\$8,173,811	3.2%
18	8,265	\$93,367	\$365,254	\$474,781	\$580,727	0.0%
19	31,535	\$345,209	\$412,168	\$4,036,772	\$1,201,913	3.6%
20	42,000	\$473,964	\$216,931	\$1,289,803	\$3,480,796	2.4%
21	21,706	\$228,424	\$360,723	\$882,620	\$3,542,431	3.2%
22	68,337	\$545,878	\$483,825	\$1,884,182	\$8,241,205	3.8%
23	26,349	\$600,070	\$72,249	\$1,559,334	\$3,379,150	4.3%
24	20,870	\$247,852	\$178,428	\$1,678,829	\$4,386,054	5.4%
25	45,000	\$337,860	\$263,126	\$3,237,492	\$5,730,520	4.2%
26	20,693	\$1,281,959	\$699,854	\$2,561,919	\$2,932,997	2.6%
27	14,334	\$489,339	\$330,728	\$1,621,319	\$1,995,185	4.1%
28	6,372	\$54,815	\$302,102	\$266,173	\$49,584	2.2%
29	11,971	\$412,636	\$835,595	\$1,322,378	\$1,420,891	5.0%
30	32,115	\$583,060	\$342,096	\$313,976	\$2,055,410	2.0%
31	25,867	\$52,318	\$1,180,533	\$279,176	\$1,035,954	3.0%
32	14,362	\$64,758	\$154,210	\$856,430	\$1,210,642	3.6%
33	5,877	\$126,504	\$374,729	\$402,655	\$796,609	2.1%
34	12,156	\$213,773	\$498,840	\$1,106,660	\$2,017,603	5.2%
35	17,615	\$30,212	\$842,117	\$57,977	\$3,080,147	4.6%
36	19,017	\$269,012	\$107,768	\$287,180	\$1,045,430	3.4%
37	23,548	\$539,891	\$370,444	\$430,299	\$2,051,786	4.6%
38	32,819	\$554,667	\$565,311	\$1,547,199	\$8,040,884	5.2%
39	27,975	\$132,410	\$336,481	\$1,763,251	\$6,940,219	4.5%
40	32,116	\$182,882	\$248,070	\$703,118	\$3,830,568	0.6%
41	25,193	\$34,733	\$131,780	\$920,831	\$6,636,012	2.3%
42	18,870	\$81,685	\$893,157	\$134,935	\$351,518	1.9%
43	33,476	\$286,006	\$607,022	\$1,398,935	\$1,875,513	1.0%
44	98,559	\$25,287	\$5,310	\$800,442	\$5,425,950	3.4%
45	4,529	\$187,012	\$719,891	\$317,296	\$312,529	1.5%
46	53,213	\$183,043	\$668,152	\$3,075,313	\$6,537,664	2.3%
47	13,159	\$1,079,223	\$566,041	\$290,038	\$2,610,362	2.1%
48	11,535	\$89,639	\$115,331	\$175,639	\$2,033,518	6.2%
49	65,762	\$381,839	\$1,750,338	\$274,291	\$2,182,508	1.4%