

2014 Cost of Data Breach Study: United States

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
May 2014



2014¹ Cost of Data Breach Study: United States

Ponemon Institute, May 2014

Part 1. Introduction

IBM and Ponemon Institute are pleased to present the *2014 Cost of Data Breach Study: United States*, our ninth annual benchmark study on the cost of data breach incidents for companies located in the United States. This year's study reveals an interesting reversal in the costs associated with data breaches. The average cost for each lost or stolen record containing sensitive and confidential information increased from \$188 to \$201. The total average cost paid by organizations increased from \$5.4 million to \$5.9 million.

In the past two years, we reported a small but steady decline in what organizations were paying to deal with a data breach. This year both the cost of a data breach for organizations and the cost per lost or stolen record have increased. The primary reason for the increase is the loss of customers following the data breach due to the additional expenses required to preserve the organization's brand and reputation. In fact, the average rate of customer turnover or churn increased by 15 percent since last year.

For the first time our study looks at the likelihood of a company having one or more data breach occurrences in the next 24 months. Based on the experiences of companies participating in our research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or stolen and the company's industry. Specifically, U.S. public sector organizations and retail companies are far more likely to have a breach. Energy and industrial companies are least likely to have a breach. In all cases, it is more likely a company will have a breach involving 10,000 or fewer records than a mega breach involving more than 100,000 records.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States nine years ago. To date, 383 U.S. organizations have participated in the benchmarking process since the inception of this research. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia, India, Italy, Japan and Brazil. This year, we introduce data breach costs for a cluster of two middle-eastern nations – the United Arab Emirates and Saudi Arabia.

This year's study examines the costs incurred by 61 U.S. companies in 16 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 500 individuals we interviewed over a ten-month period in the companies that are represented in this research.

Interviews with the organizations represented in this year's benchmark study took place during a time of large and well-publicized data breaches, especially in retail. The occurrence of these breaches and the experiences reported in this year's study is evidence that sensitive and confidential information continues to be at risk.

The number of breached records per incident this year ranged from approximately 5,000 to slightly more than 100,000 records. The average number of breached records was 29,087. By design, we do not include cases involving more than 100,000 compromised records because they are not indicative of data breaches incurred by most organizations. Thus, to include them in the

¹ For the first time, this report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2013 calendar year.

study would artificially skew the results. The cost for all 61 data breach case studies in this year's report is presented in Appendix 1.

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

- **The cost of data breach increased.** Breaking a downward trend over the past two years, both the organizational cost of data breach and the cost per lost or stolen record have increased. On average the cost of a data breach for an organization represented in the study increased from \$5.4 million to \$5.9 million. The cost per record² increased from \$188 to \$201. We define a record as information that identifies the natural person (individual) whose information has been compromised in a data breach.
- **More customers terminated their relationship with the company that had a data breach.** In addition to the increase in cost, companies are losing more customers following a data breach. The average abnormal churn rate between 2013 and 2014 increased 15 percent. Certain industries, especially financial services, continue to be most susceptible to high churn in the aftermath of a material data breach.
- **Malicious or criminal attacks rather than negligence or system glitches were the main causes of data breach.** This year's study shows malicious or criminal attacks as the most frequently encountered root cause of data breaches by organizations in this study. Forty-four percent say the main cause of data breach was a malicious or criminal attack against the organization. Thirty-one percent of organizations say employee negligence (a.k.a. human factor) and 25 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 an average of \$246 per compromised record. In contrast, both system glitches and employee mistakes resulted in a much lower average per capita cost at \$171 and \$160, respectively.
- **The cost of lost business increased from \$3.03 million to \$3.2 million.** These costs include 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 nine years we studied this aspect of a data breach, the highest cost for lost business was \$4.59 million in 2009.
- **Business continuity management reduced the cost of a breach.** For the first time, the research reveals that having business continuity management involved in the remediation of the breach can reduce the cost by an average of \$13 per compromised record.
- **Certain organizational factors reduced the overall cost.** If the organization has a strong security posture or a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as \$21 and \$17 per record, respectively. Finally, appointing a CISO to lead the data breach incident response team reduced per capita cost by \$10.
- **Specific attributes or factors of the data breach increased the overall cost.** Data breaches caused by third parties increased per capita cost by \$25 and data breach incidents involving the loss or theft of data bearing devices increased per capita cost by as much as \$18 per record. Organizations that notified customers too quickly without a thorough assessment or forensic examination, incurred an average cost increase of \$15 more per record.

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

- **Post data breach response and detection costs increased slightly.** The costs associated with ex-post response increased from approximately \$1.41 million to \$1.60 million. 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 increased slightly from \$395,262 to \$417,700 over the past year. 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 for data breach resolution activities and to keep management informed.

- **Will your organization have a data breach?** As part of understanding the potential risk to an organization's sensitive and confidential information, we thought it would be helpful to understand the probability that an organization will have a data breach. To do this, we extrapolate a subjective probability distribution for the entire sample of participating companies on the likelihood of a material data breach happening over the next two years.

The results show that a probability of a material data breach over the next two years involving a minimum of 10,000 records is nearly 19 percent. In addition to overall aggregated results, we find that the probability or likelihood of data breach varies considerably by industry. Public sector organizations have the highest estimated probability of occurrence at 23.8 percent, while energy and utilities have the lowest rate of occurrence at only 7.5 percent.

Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual's name plus Social Security number, medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format. In our study, we have identified three main causes of a data breach. These are a malicious or criminal attack, system glitch or human error. The costs of a data breach can vary according to the cause and the safeguards in place at the time of the data breach.

What is a compromised record? We define a record as information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples can include a retail company's database with an individual's name associated with credit card information and other personally identifiable information. Or, it could be a health insurer's record of the policyholder with physician and payment information. In this year's study, the average cost to the organization if one of these records is lost or stolen is \$201.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews with more than 500 individuals conducted over a ten-month period. Recruiting organizations for the 2014 study began in January 2013 and interviews were completed in March 2014. In each of the 61 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 customer acquisition rates.

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. We recruited 61 organizations to participate in this study. Data breaches ranged from a low of about 5,000 to slightly more than 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 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 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 more than nine years ago, we have studied the data breach experiences of 383 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:

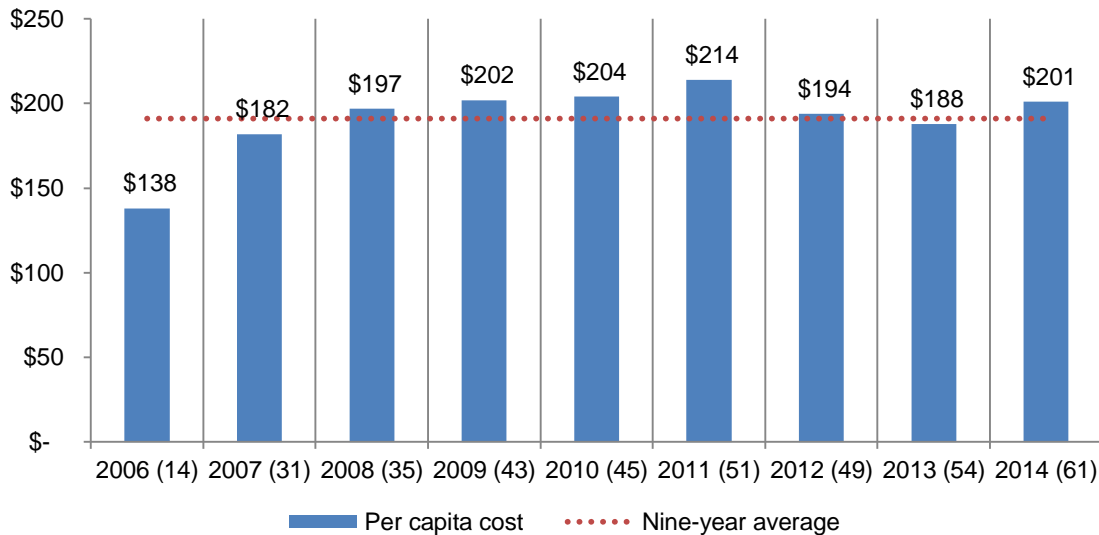
- Understanding the cost of data breach
- The root causes of data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records and customer turnover
- Trends in the cost components of data breach
- The likelihood that an organization will have a data breach
- Recommendations on how to mitigate the risk and consequences of a data breach

Understanding the cost of data breach

The cost of data breach increased. Breaking a two-year trend, the cost of data breach has increased. Figure 1 reports the average per capita cost of a data breach since the inception of this research series nine years ago.³ According to this year's benchmark findings, data breaches cost companies an average of \$201 per compromised record – of which \$134 pertains to indirect costs including abnormal turnover or churn of customers. Last year's average per capita cost was \$188 with an average indirect cost of \$128. As can be seen, the highest cost of \$214 per compromised record occurred in 2011

Figure 1. The average per capita cost of data breach over nine years

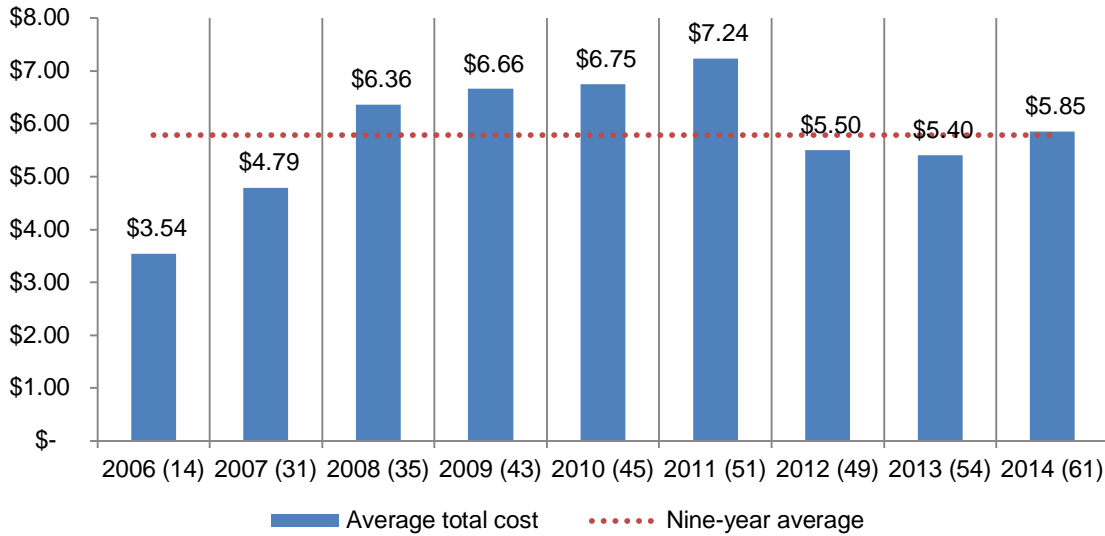
Bracketed number defines the benchmark sample size



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.

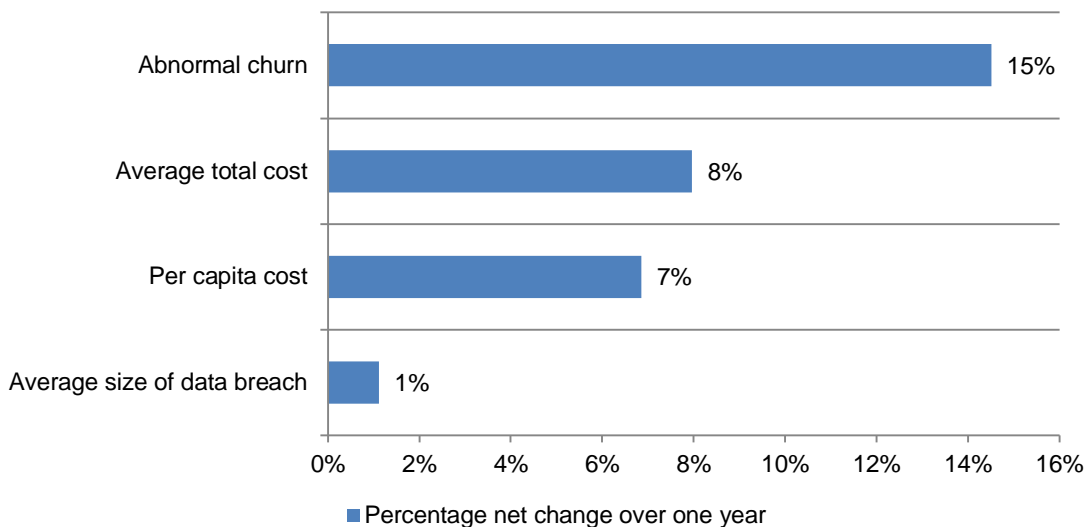
The total average organizational cost of data breach increased. Figure 2 shows that the total average cost of data breach over nine years steadily increased from a low of \$3.54 million in 2005 to a high of \$7.24 million in 2011. In 2013 we experienced a net decrease in total data breach cost to \$5.40 million. This year, the total average cost rose to \$5.85 million.

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



Measures reveal why the cost of data breach increased. Figure 3 reports the four net changes from last year's report. As discussed, the average total cost of a data breach grew by 8 percent and the average per capita cost rose by 7 percent. An increase in abnormal churn of existing customers by 15 percent was a major reason for a higher cost of data breach. In the context of this paper, abnormal churn is defined as a greater than expected loss of customers in the normal course of business. The average size of a data breach (number of records lost or stolen) increased 1 percent.

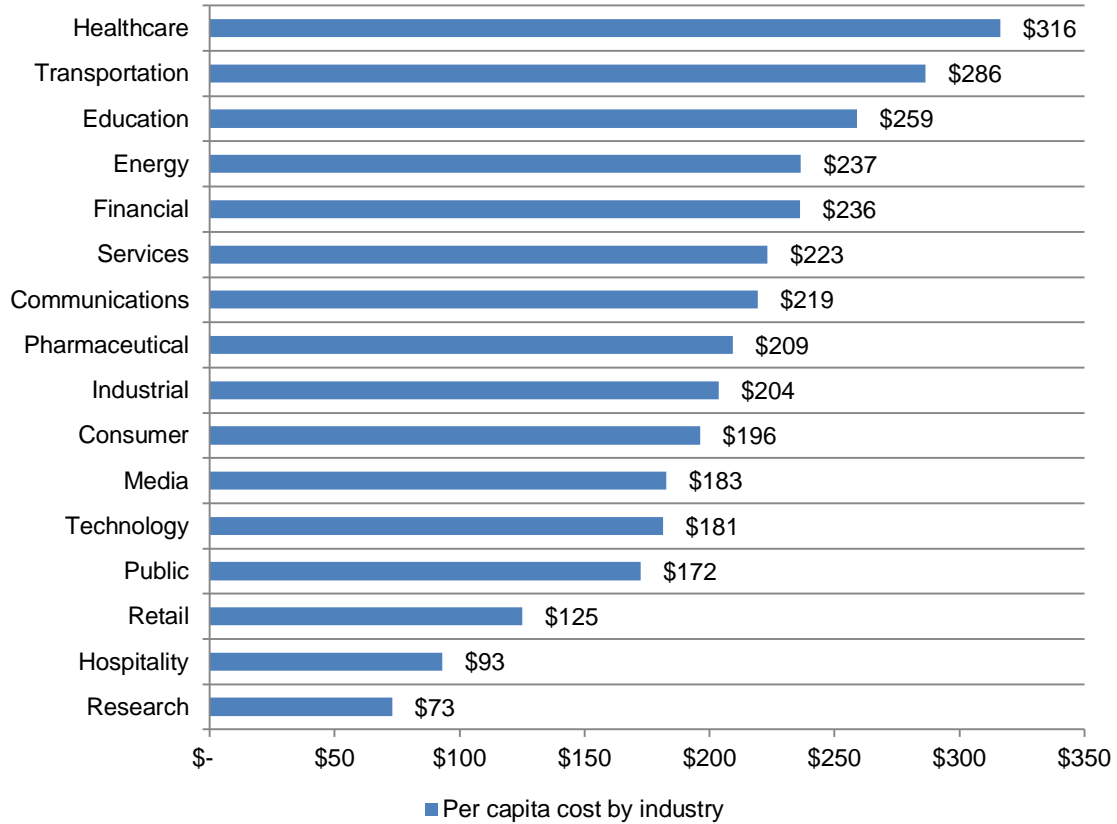
Figure 3. Changes in cost of data breach measures
Net change defined as the difference between the 2014 and 2013 results



Certain industries have higher data breach costs. Figure 4 reports the per capita costs for 16 industry sectors. While a small sample size prevents us from generalizing industry cost differences, the pattern of industry results is consistent with prior years.

Specifically, heavily regulated industries such as healthcare, transportation, education, energy, financial services, communications, pharmaceuticals and industrial companies tend to have a per capita data breach cost substantially above the overall mean of \$201. In contrast, retailers, hospitality companies and public sector organizations have a per capita cost well below the overall mean value.

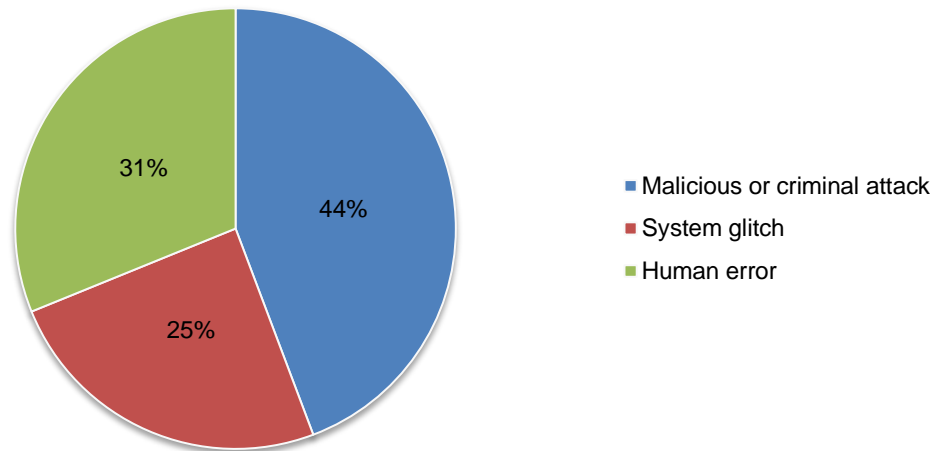
Figure 4. Per capita cost by industry classification of benchmarked companies



The root causes of data breach

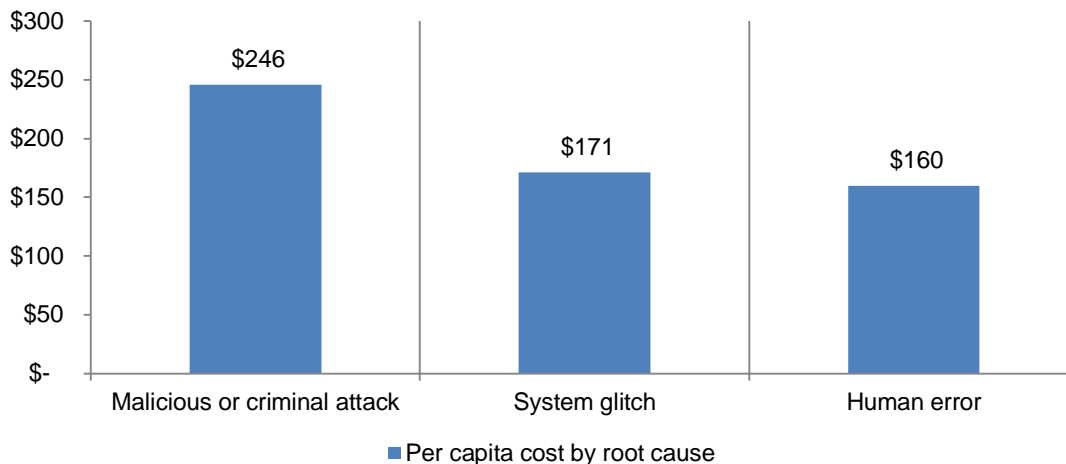
In this year's study, malicious or criminal attacks are most often the cause of data breach.⁴ Figure 5 provides a summary of the main root causes of data breach for all 61 organizations. Forty-four percent of incidents involved a malicious or criminal attack, 31 percent concerned negligent employees, and 25 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. These results are consistent with prior years, wherein the most costly breaches involve malicious acts against the company. Companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost of \$246, significantly above the mean of \$201. In contrast, system glitches or human error as the root cause had per capita costs significantly below the mean (\$171 and \$160, respectively).

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 are caused by hackers or criminal insiders (employees, contractors or other third parties).

⁵Malicious and criminal attacks increased from 41 percent in last year's study. The most common types of attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

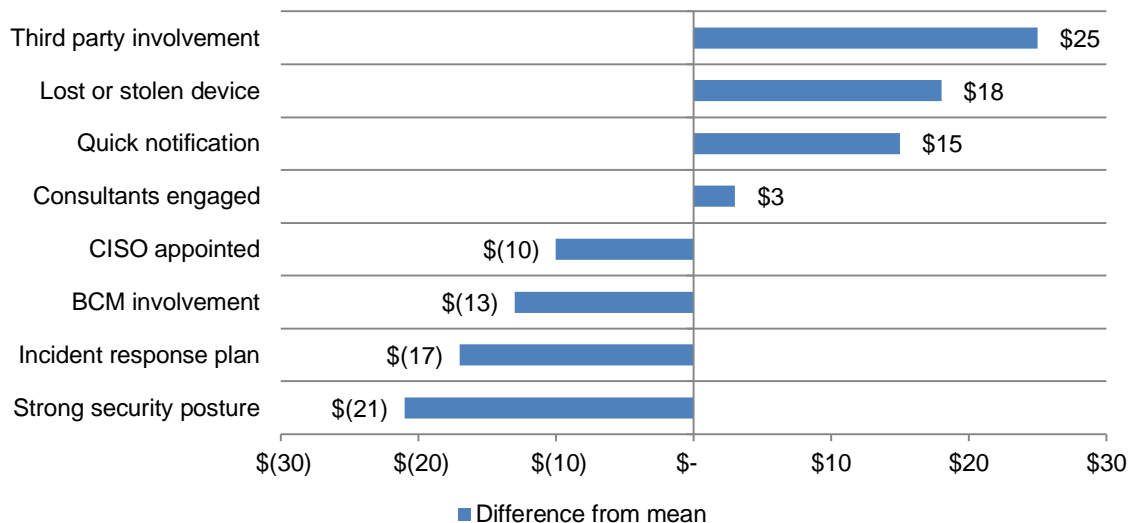
Factors that influence the cost of data breach

Table 1 lists eight key factors that affect the costs and consequences of data breach incidents.

Table 1 Eight factors that impact data breach cost	Percentage of companies exhibiting this attribute
Consultants were engaged to help remediate the data breach.	49%
The data breach involved lost or stolen devices (including mobile devices such as smart phones and tablets).	46%
The company notified data breach victims quickly (within 30 days after discovery of the incident).	43%
CISO (or equivalent title) has overall responsibility for enterprise data protection.	41%
The company had a relatively strong security posture at the time of the incident. ⁶	39%
The company had an incident management plan at the time of the data breach event.	38%
Data was lost due to third party errors, glitches or misuse that caused an incident.	36%
The company's business continuity management team provides substantial support in containing the negative impact of the incident.	33%

As shown in Figure 7, a strong security posture, incident response plan, BCM involvement and CISO leadership are viewed as reducing the cost of data breach. However, third party error, lost or stolen devices, quick notification and engagement of consultants to support the incident response team increased data breach cost. A strong security posture reduced the average cost of data breach from \$201 to \$180 (decrease = \$21). In contrast, third party breaches increased the average cost to \$226 (increase = \$25).

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



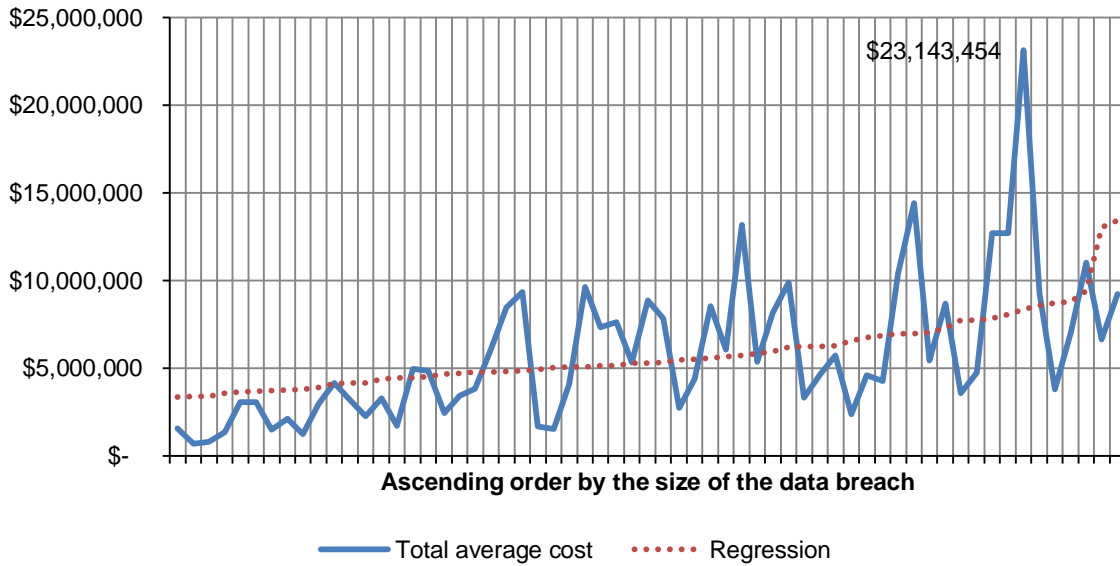
⁶This attribute is defined as the percentage of companies that achieved a Security Effective Score (SES) at or above the top third of all recorded results (i.e., scored norms). The SES was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding 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.

Trends in the frequency of compromised records and customer turnover

The more records lost, the higher the cost of data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for 61 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. This year, the cost ranged from \$688,250 to \$23.1 million.

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

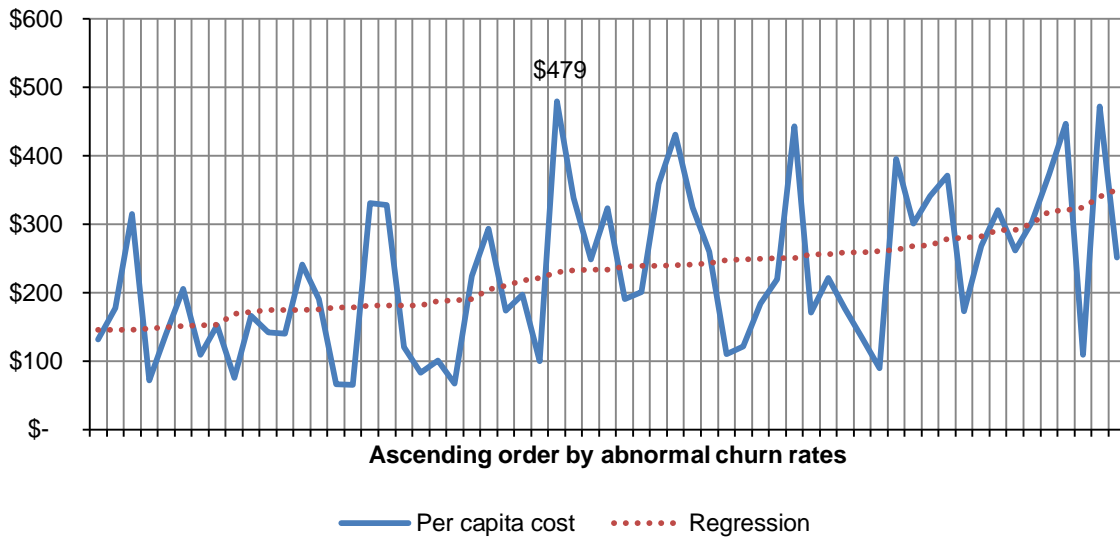
Regression = Intercept + {Size of Breach Event} x β , where β denotes the slope.



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

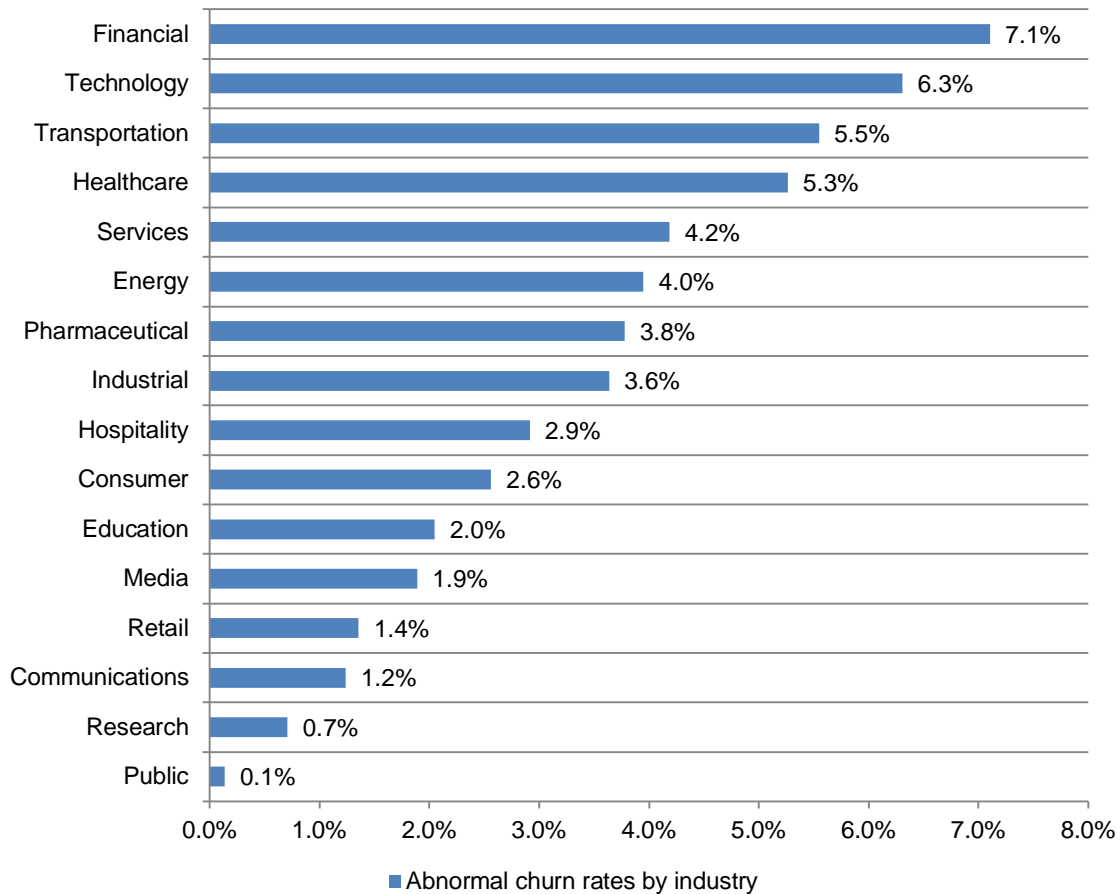
Regression = Intercept + {abnormal churn rate} x β , where β denotes the slope.



Certain industries were 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, these industry results are consistent with prior years – wherein financial service, technology, transportation and health organizations experienced a relatively high abnormal churn and public sector, research, communications and retail organizations tend to experience a relatively low abnormal churn.⁷

The implication 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



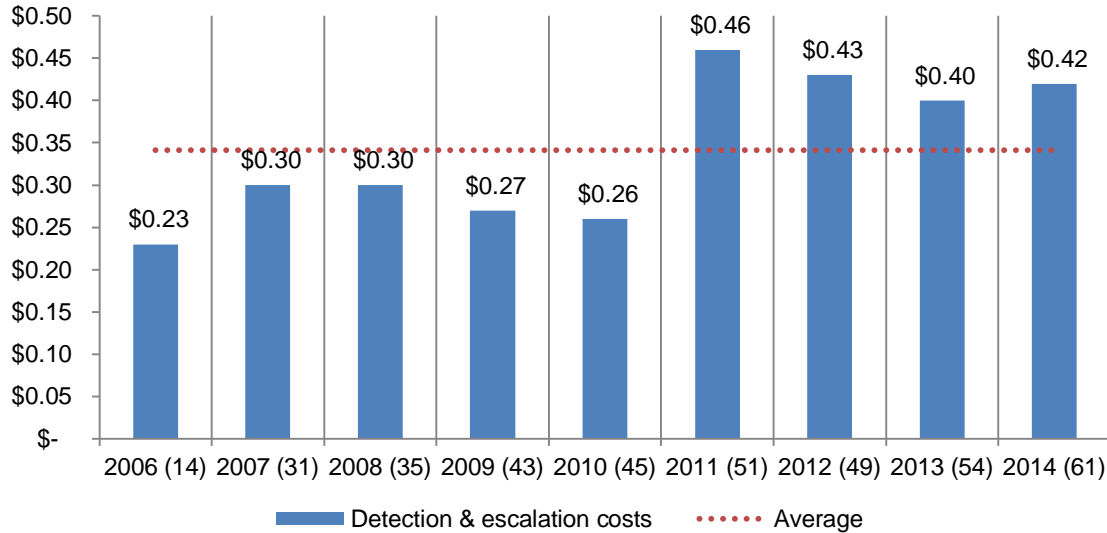
⁷Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

Detection and escalation costs increased. Figure 11 shows the nine-year trend for such costs as forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs increased slightly from \$0.40 million to \$0.42.

Figure 11. Average detection and escalation costs over nine years

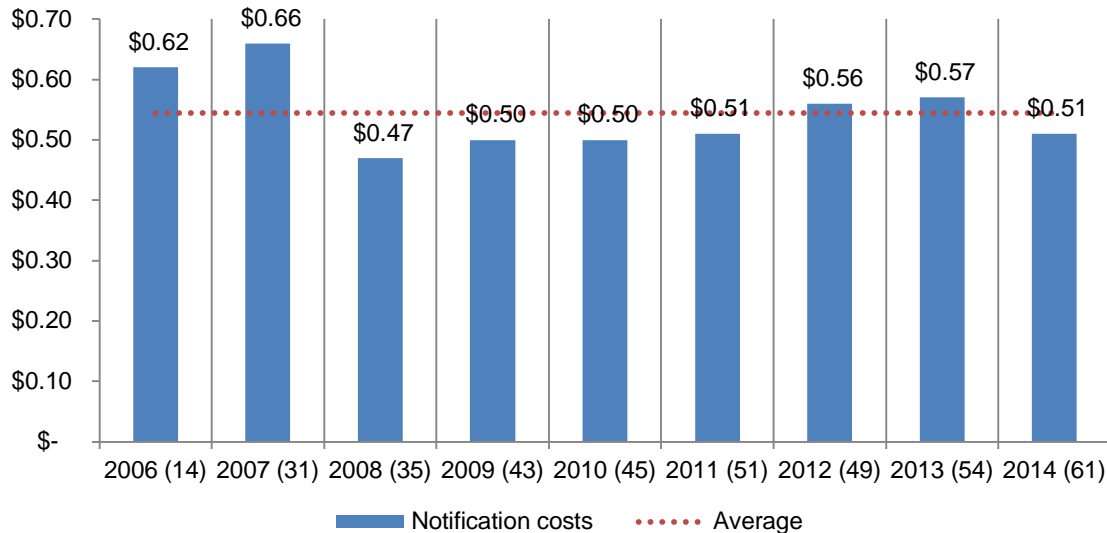
\$000,000 omitted



Notification costs decreased. 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 costs decreased slightly from \$0.57 million in 2013 to \$0.51 million in the present year.

Figure 12. Average notification costs over nine years

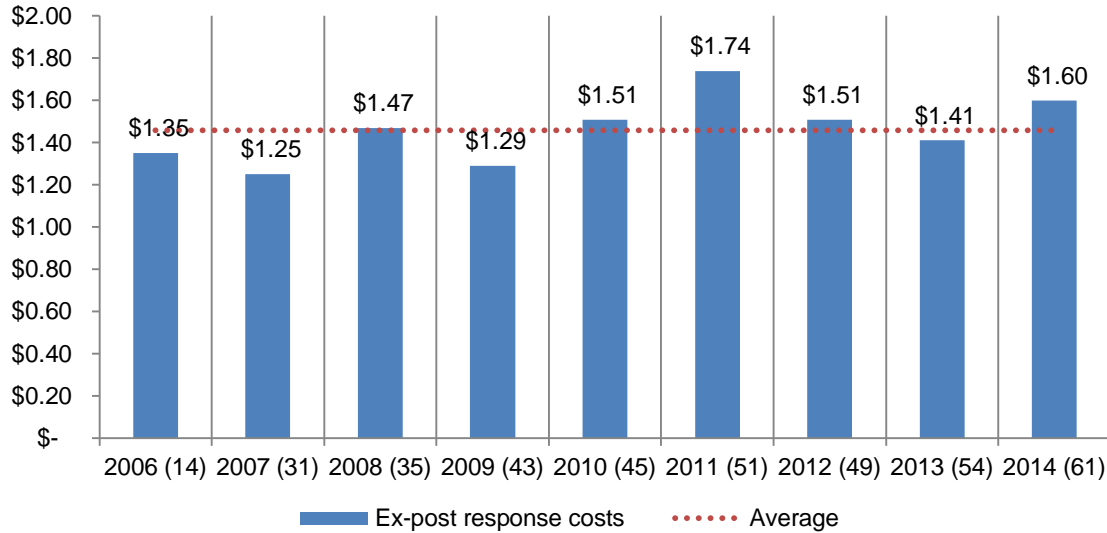
\$000,000 omitted



Post data breach costs increased. 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. While average ex-post response costs decreased from a nine-year high of \$1.74 million 2011, they increased from \$1.41 million in 2013 to \$1.60 million in this year's study.

Figure 13. Average cost for post data breach activities

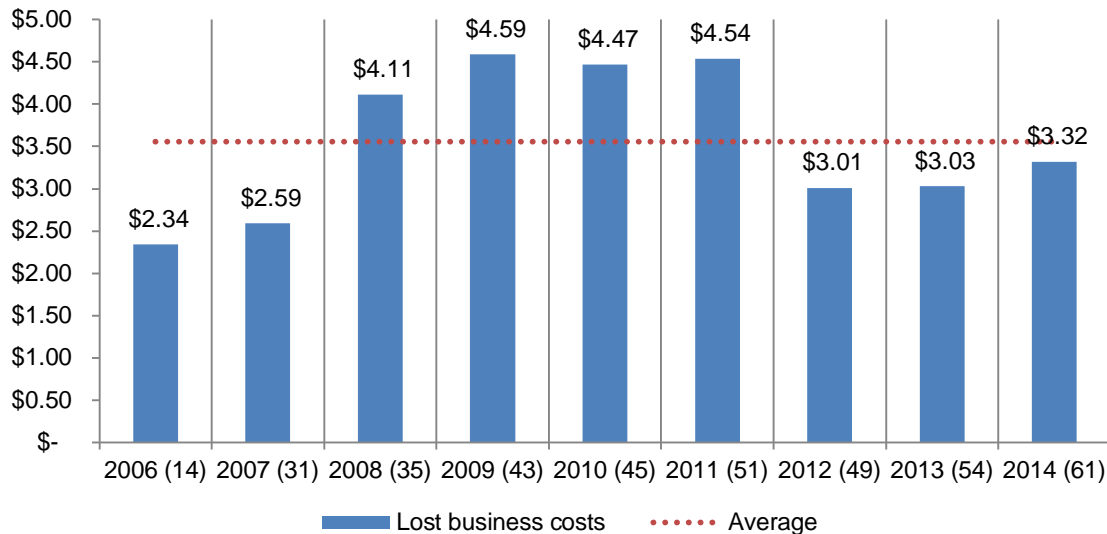
\$000,000 omitted



Lost business costs grew slightly. Figure 14 reports lost business costs associated with data breach incidents over nine years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen, lost business increased over the past two years. The current year's cost of \$3.32 million represents an increase from 2013 (\$3.03 million). The highest level of lost business cost was \$4.59 million in 2009.

Figure 14. Average lost business costs over nine years

\$000,000 omitted

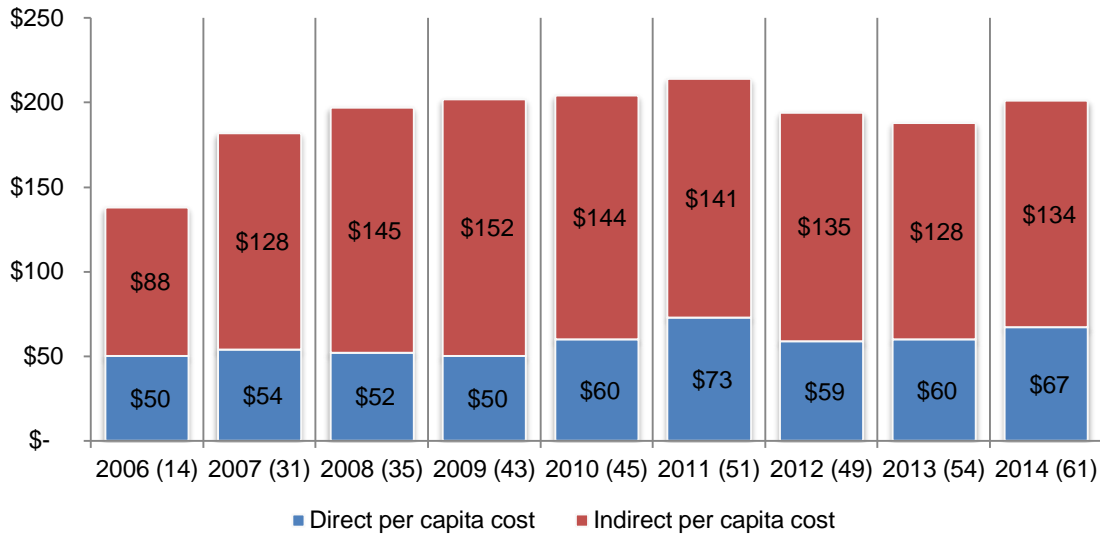


Companies continued to spend more on direct costs than indirect costs. Direct costs refer to what companies spend to minimize the consequences of a data breach and to assist victims. These costs include engaging forensic experts to help investigate the data breach, hiring a law firm and offering victims identity protection services.

Indirect costs pertain to what the company spends on existing internal resources to deal with the data breach. These costs could include the time employees spend on data breach notification efforts or investigations of the incident. Indirect costs also include the loss of brand value and reputation 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 increased by \$13 – from \$188 in 2013 to \$201 in 2014. Direct and indirect costs increased by \$7 and \$6 per compromised record, respectively.

Figure 15. Trends in direct and indirect costs of a data breach over nine years

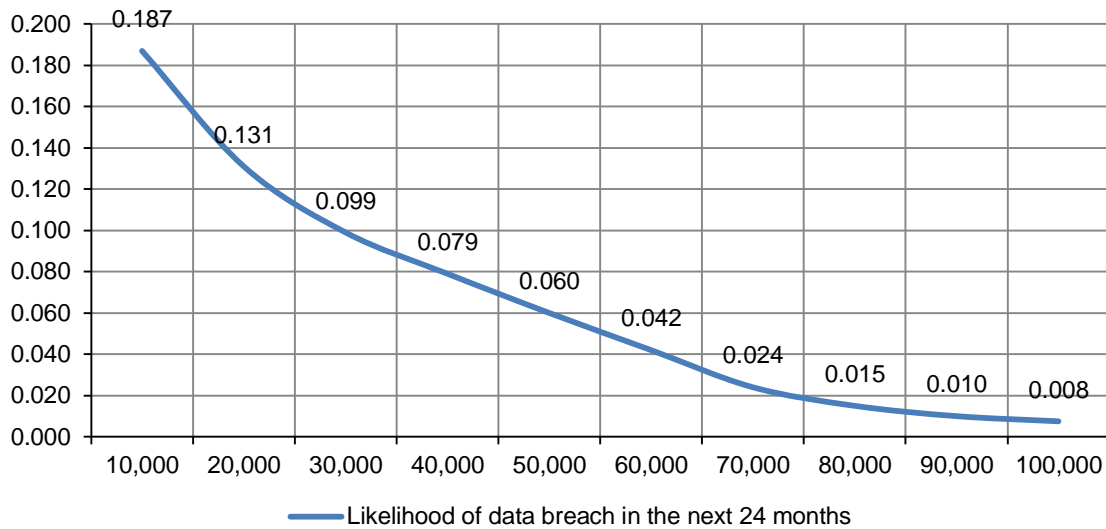


The likelihood that an organization will have a data breach

Companies are far more likely to have a small data breach than a mega breach. For the first time our research provides an analysis of the likelihood of one or more data breach occurrences in the next 24 months. Based on the experiences of organizations in our research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or stolen and the company's industry.

Figure 16 shows the subjective probabilities of breach incidents involving a minimum of 10,000 to 100,000 compromised records.⁸ As can be seen, the likelihood of data breach steadily decreases as the size increases. While the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 19 percent over a 24-month period, the chances of a data breach involving a 100,000 records is less than one percent.

Figure 16. Probability of a data breach involving a minimum of 10,000 to 100,000 records

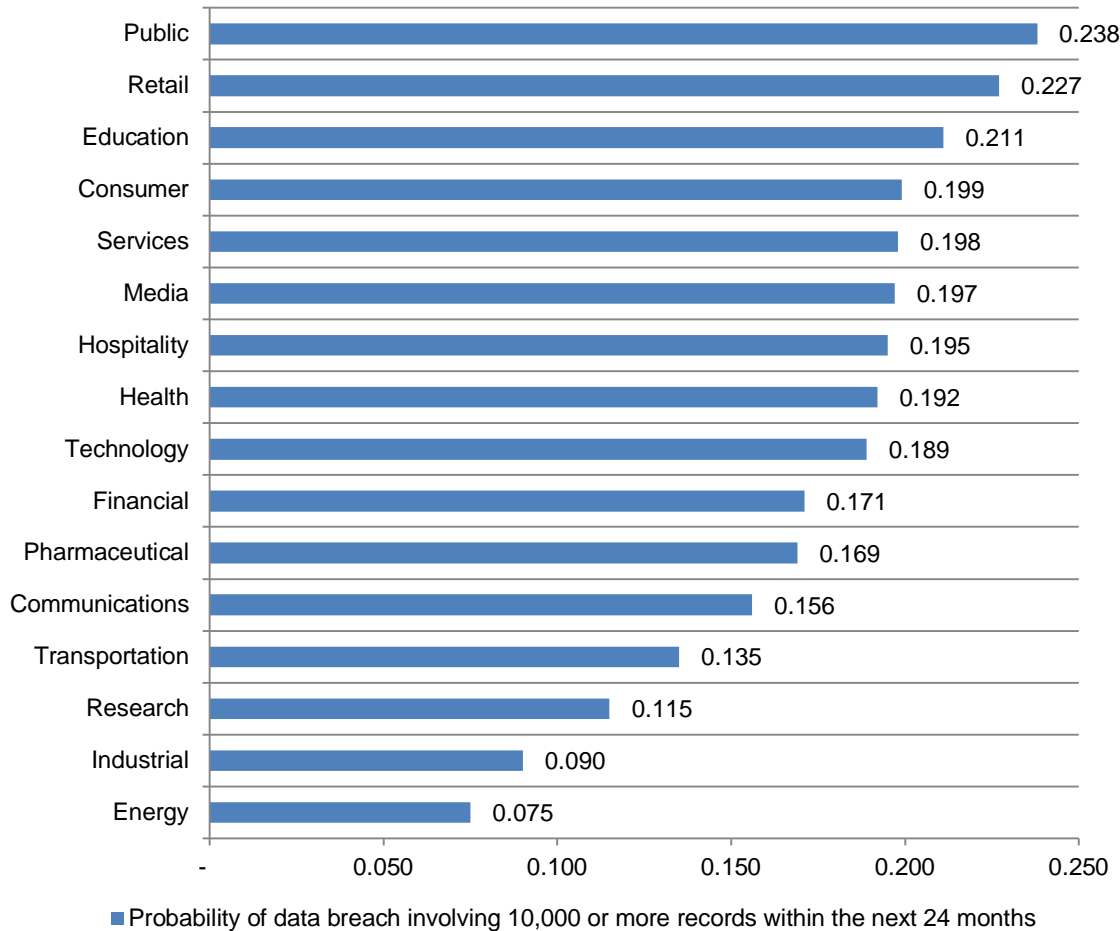


⁸Estimated probabilities were captured from sample respondents using a point estimation technique. Key individuals such as the CISO or CPO who participated in cost assessment interviews provided their estimate of data breach likelihood for 10 levels of data breach incidents (ranging from 10,000 to 100,000 lost or stolen records). The time scale used in this estimation task was the forthcoming 24-month period. An aggregated probability distribution was extrapolated for each one of the 61 participating companies.

Public sector and retail companies are more likely to have a data breach. Figure 17 summarizes the probability of a data breach involving a minimum of 10,000 records for 16 industry sectors. While a small sample size prevents us from generalizing industry differences, the estimated likelihood of a material data breach varies considerably across industries.

Public sector and retail companies have the highest estimated probability of occurrence. One possible explanation is the amount of confidential and sensitive information collected by these industries. Energy, industrial and research companies have the lowest probability of occurrence.

Figure 17. Probability of a data breach involving a minimum of 10,000 records by industry



Recommendations on how to mitigate the risk and consequences of a data breach

Companies participating in our annual study report that data breaches resulted in a higher rate of churn than in the past two years. Highly publicized data breaches and greater awareness of the risk of identity theft could be a reason why victims of breaches are terminating relationships with companies.

Once again we consider those factors that can reduce the cost of a data breach. The most profitable investments companies can make seem to be an incident response plan, a strong security posture, the involvement of business continuity management and the appointment of a CISO with enterprise-wide responsibility.

One of the goals of this research is to provide insights on what the potential costs of a data breach could be based upon certain characteristics. This understanding can lead to the better allocation of limited resources to the prevention, detection and resolution of a data breach. Consistently our research reveals the severe financial consequences from malicious or criminal acts. These data breaches can prove to be the most costly and should encourage the use of appropriate technologies and tools that prevent such threats.

In addition to measuring specific cost activities relating to the data breach incident, we report in Table 2 the preventive measures implemented by companies after this event. The most popular measures and controls implemented after the data breach have been fairly consistent.

This year, the number one activity focuses on endpoint security. Stepped up training and awareness programs and the expanded use of encryption (and possibly other cryptographic data protection methods) follow. This year, the use of endpoint security solutions increased the most from 2013 (net change = +13 percent). In contrast, the use of data loss prevention solutions decreased the most from 2013 (net change = -10 percent).

Table 2 Data loss prevention controls and activities	2010	2011	2012	2013	2014
Endpoint security solutions	36%	41%	42%	40%	53%
Training and awareness programs	67%	63%	53%	51%	51%
Expanded use of encryption	58%	61%	52%	57%	50%
Additional manual procedures and controls	58%	54%	49%	46%	43%
Data loss prevention (DLP) solutions	42%	43%	45%	49%	39%
Identity and access management solutions	49%	52%	47%	43%	39%
Security intelligence solutions	22%	21%	26%	28%	34%
Other system control practices	40%	43%	38%	34%	33%
Strengthening of perimeter controls	20%	22%	25%	23%	21%
Security certification or audit	33%	29%	19%	19%	20%

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

Table 3 reports 11 general cost categories on a percentage basis over eight years. 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. There is also greater interest in getting to the root of the breach. Organizations have steadily increased their level of spending on investigation and forensics.

Table 3								
General cost categories	2007	2008	2009	2010	2011	2012	2013	2014
Investigations & forensics	8%	8%	9%	8%	11%	11%	12%	13%
Audit and consulting services	10%	10%	11%	12%	10%	9%	8%	7%
Outbound contact costs	9%	7%	6%	6%	5%	6%	5%	4%
Inbound contact costs	10%	8%	6%	5%	6%	5%	5%	6%
Public relations/communications	1%	3%	1%	1%	1%	1%	1%	1%
Legal services - defense	6%	8%	9%	14%	14%	15%	15%	16%
Legal services - compliance	3%	3%	1%	2%	2%	3%	4%	3%
Free or discounted services	2%	1%	2%	1%	1%	1%	1%	2%
Identity protection services	3%	2%	2%	2%	2%	3%	4%	2%
Lost customer business	39%	41%	43%	40%	39%	37%	36%	38%
Customer acquisition cost	8%	9%	9%	9%	9%	9%	9%	8%
Total	100%	100%	100%	100%	100%	100%	100%	100%

Part 3. How we calculate the cost of data breach

To calculate the cost of data breach, we use a costing methodology called activity-based costing (ABC). This methodology identifies activities and assigns a cost according to actual use. Companies participating in this benchmark research are asked to estimate the cost for all the activities they engage in to resolve the data breach.

Typical activities for discovery and the immediate response to the data breach include the following:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specialized training

The following are typical activities conducted in the aftermath of discovering the data breach:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

Once the company estimates a cost range for these activities, we categorize the costs as direct, indirect and opportunity as defined below:

- *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).

Our study also looks at the core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. The costs for each activity are presented in the Key Findings section (Part 2). 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.
- Post data breach: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms. Post data breach activities also include 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.⁹
- 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.¹⁰ 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).

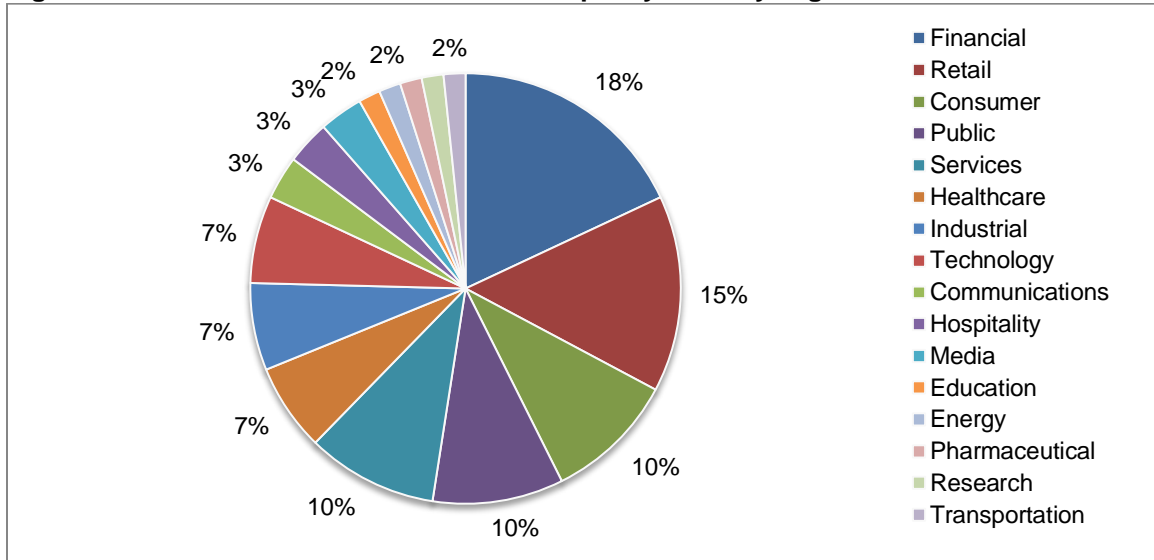
⁹In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector entities – where termination is costly or economically infeasible.

¹⁰In this study, we consider citizen, patient and student information as customer data.

Part 4. Organizational characteristics and benchmark methods

Figure 18 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 16 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Figure 18. Distribution of the benchmark sample by industry segment



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.¹¹

¹¹Our 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.

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.

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.

For purposes of 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.

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.

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. Sixty-one 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 61 Data Breach Case Studies US\$

Cases	Size of breach	Detection & escalation	Notification	Ex-post response	Lost business
1	9,068	424,236	170,249	403,009	270,898
2	22,152	1,963,031	547,453	2,348,228	2,470,098
3	53,636	2,266,502	3,553,131	5,454,390	11,869,431
4	102,859	835,249	1,053,343	5,154,557	2,215,885
5	27,431	50,460	70,009	1,234,041	4,730,935
6	57,941	1,576,451	597,739	1,809,258	3,077,631
7	21,533	68,954	2,626,039	810,447	606,882
8	27,939	1,350,701	389,761	8,797,510	2,655,658
9	8,767	374,361	261,415	1,096,394	379,606
10	40,254	394,492	163,192	3,968,393	9,911,511
11	18,744	662,484	1,296,366	1,882,005	8,727
12	7,737	144,227	431,045	541,339	1,946,720
13	25,349	243,240	543,548	704,499	1,271,342
14	5,207	58,741	34,028	412,101	183,380
15	12,274	751,202	3,880	1,343,606	2,058,341
16	18,811	382,994	806,038	1,659,799	3,239,168
17	21,750	144,217	507,221	703,918	8,274,567
18	8,460	87,026	250,015	489,032	676,324
19	22,314	423,177	386,050	5,461,335	1,355,054
20	33,162	512,723	197,074	979,311	4,064,619
21	29,183	236,313	323,790	749,357	4,065,914
22	63,773	619,349	453,460	2,157,222	7,790,592
23	40,777	699,628	82,656	1,288,963	3,377,423
24	18,993	255,130	205,398	2,043,898	5,986,377
25	40,098	415,129	178,211	4,282,599	5,540,723
26	24,204	1,813,631	834,043	2,799,688	2,415,624
27	16,154	382,349	449,912	2,002,906	2,032,139
28	5,364	73,199	406,504	267,320	68,255
29	12,797	454,083	683,041	932,674	1,108,053
30	32,839	695,506	216,110	313,805	2,090,921
31	36,075	40,811	686,218	319,039	1,319,816
32	12,841	69,376	151,989	713,047	1,334,800
33	6,893	125,029	320,520	385,561	527,628
34	8,220	279,836	445,989	756,092	1,582,124
35	18,094	41,226	636,958	59,630	2,713,915
36	15,728	214,241	100,509	297,395	1,122,742
37	25,709	636,442	507,549	661,519	2,595,756
38	32,765	719,129	693,283	1,845,376	6,656,006
39	30,310	185,852	389,116	1,814,960	5,742,462
40	38,098	198,470	404,109	2,319,567	1,669,717
41	43,202	116,883	374,282	2,001,610	6,194,765
42	55,736	98,304	437,258	1,562,983	7,178,995
43	48,469	91,437	536,461	2,002,498	10,065,389
44	15,042	24,896	79,760	1,139,748	2,057,294
45	20,263	113,436	706,159	125,641	734,800
46	47,370	237,471	382,929	1,848,924	1,122,439
47	47,650	158,408	327,752	881,831	3,388,595
48	26,628	45,591	137,729	1,128,649	7,234,888
49	21,329	95,852	969,137	128,919	332,061
50	32,854	414,180	311,003	1,565,099	2,372,262
51	23,882	151,634	357,923	2,206,731	6,158,343
52	23,757	229,523	242,696	962,330	3,893,728
53	19,480	29,907	99,810	1,406,573	7,804,041

Cases	Size of breach	Detection & escalation	Notification	Ex-post response	Lost business
54	17,776	103,270	971,177	763,450	631,173
55	39,124	215,692	555,722	2,116,578	1,404,762
56	98,948	31,122	4,214	641,017	5,974,198
57	4,760	259,219	689,206	308,531	305,569
58	50,567	167,370	908,203	3,692,805	7,954,108
59	15,737	1,489,118	354,980	392,957	2,723,677
60	10,275	90,951	115,026	161,260	2,651,921
61	57,183	446,241	445,055	1,297,839	1,631,754

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

Complete copies of all country reports are available at www.ibm.com/services/costofbreach.

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.