2016 Cost of Data Breach Study: United States

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2016

2016[1] Cost of Data Breach Study: United States

Ponemon Institute, June 2016

Part 1. Introduction

IBM and Ponemon Institute are pleased to present the *2016 Cost of Data Breach Study: United States*, our 11th annual benchmark study on the cost of data breach incidents for companies located in the United States. The average cost for each lost or stolen record containing sensitive and confidential information increased from $217 to $221. The total average cost that organizations paid increased from $6.53 million to $7.01 million.

United States study at a glance

- 64 companies participated
- $7.01 million is the average total cost of data breach
- 7% increase in total cost of data breach
- $221 is the average cost per lost or stolen record
- 2% increase in cost per lost or stolen record

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States 11 years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia, India, Italy, Japan, Brazil, the United Arab Emirates and Saudi Arabia and, Canada. This year we have expanded the research to include South Africa. To date, 509 U.S. organizations have participated in the benchmarking process since the inception of this research.

This year's study examines the costs incurred by 64 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 that the costs presented in this research are not hypothetical, but are from actual data loss incidents. They are based upon cost estimates provided by individuals we interviewed over a ten-month period in the companies that are represented in this research.

The number of breached records per incident this year ranged from 5,125 to 101,520 records. The average number of breached records was 29,611. 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, including them in the study would artificially skew the results.

Seven global megatrends in the cost of data breach research

Over the many years studying the data breach experience of 2,013 organizations in every industry, the research has revealed the following seven megatrends.

1. Since first conducting this research, the cost of a data breach has not fluctuated significantly. This suggests that it is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies.

2. The biggest financial consequence to organizations that experience a data breach is lost business. Following a data breach, organizations need to take steps to retain customers' trust to reduce the long-term financial impact.

3. Most data breaches continue to be caused by criminal and malicious attacks. These breaches also take the most time to detect and contain. As a result, they have the highest cost per record.

[1] 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 2015 calendar year.

4. Organizations recognize that the longer it takes to detect and contain a data breach the more costly it becomes to resolve. Over the years, detection and escalation costs in our research have increased. This suggests investments are being made in technologies and in-house expertise to reduce the time to detect and contain breaches.

5. Regulated industries, such as healthcare and financial services, have the most costly data breaches because of fines and the higher than average rate of lost business and customers.

6. Improvements in data governance programs will reduce the cost of data breach. Incident response plans, appointment of a CISO, employee training and awareness programs and a business continuity management strategy continue to result in cost savings.

7. Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches. This year's study revealed a reduction in the cost when companies participated in threat sharing and deployed data loss prevention technologies.

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

The cost of data breach sets new record high. According to this year's benchmark findings, data breaches cost companies an average of $221 per compromised record – of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach, such as investments in technologies or legal fees.

The total average organizational cost of data breach reaches a new high. In the past 11 years, the most costly organizational breach occurred in 2011, when companies spent an average $7.24 million. In 2013, companies experienced a net decrease in total data breach cost to $5.40 million. This year, the total average cost is $7.01 million.

Measures reveal why the cost of data breach increased. The average total cost of a data breach grew by 7 percent and the average per capita cost rose by 2 percent. Abnormal churn of existing customers increased by 3 percent. 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 by 5 percent.

Certain industries have higher data breach costs. Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research had a per capita cost well below the overall mean value.

Malicious or criminal attacks continued to be the primary cause of data breach. Fifty percent of incidents involved a malicious or criminal attack, 23 percent of incidents were caused by negligent employees, and 27 percent involved system glitches that included both IT and business process failures.

Malicious attacks were most costly. Companies that had a data breach due to malicious or criminal attacks had a per capita data breach cost of $236, significantly above the mean of $221. In contrast, system glitches or human error as the root cause had per capita costs below the mean ($213 and $197, respectively).

Certain factors decreased the cost of data breach. Incident response plans and teams in place, extensive use of encryption, employee training, BCM involvement or extensive use of DLP reduced the cost of data breach. Data breaches due to third party error, extensive cloud migration or a rush to notify increased the cost.

The more records lost, the higher the cost of data breach. This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

The more churn, the higher the per capita cost of data breach. Companies that experienced less than 1 percent churn, or loss of existing customers, had an average organizational cost of data breach of $5.4 million and those experiencing churn greater than 4 percent had an average cost of data breach of $12.1 million.

Certain industries were more vulnerable to churn. Financial, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research organizations tend to experience a relatively low abnormal churn.

Detection and escalation costs are at a record high. These costs include 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 dramatically from $0.61 million to $0.73 million, suggesting that companies are investing more heavily in these activities.

Notification costs increased slightly. 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 mail contacts or email bounce-backs and inbound communication set-up. This year's average notification costs increased slightly from $0.56 million in 2015 to $0.59 million in the present year.

Post data breach costs increased. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. These costs increased from $1.64 million in 2015 to $1.72 million in this year's study.

Lost business costs increased. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The current year's cost of $3.97 million represents an increase from $3.72 million in 2015. The highest level of lost business cost was $4.59 million in 2009.

Companies continue to spend more on indirect costs than direct costs. Indirect costs include the time employees spend on data breach notification efforts or investigations of the incident. 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. This year the indirect costs were $145 and direct costs were $76.

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 $221.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a ten-month period. Recruiting organizations for the 2016 study began in January 2015 and interviews were completed in March 2016. In each of the 64 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 64 organizations to participate in this study. Data breaches ranged from a low of about 5,125 to slightly more than 101,500 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 11 years ago, we have studied the data breach experiences of 509 U.S. organizations.

Part 2. Key Findings

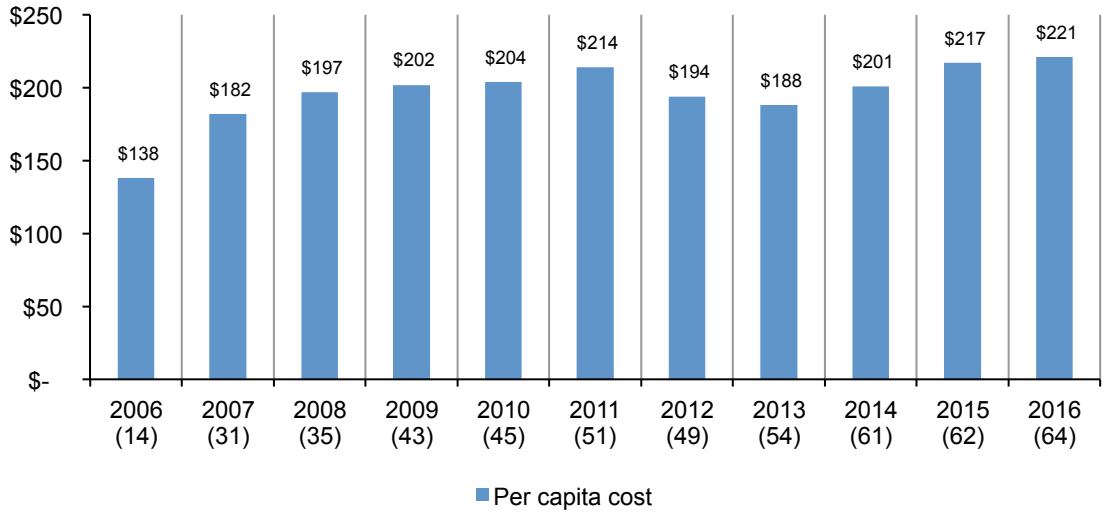
In this section we provide the detailed findings of this research. Topics are presented in the following order:

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

Understanding the cost of data breach

The cost of data breach sets new record high. Figure 1 reports the average per capita cost of a data breach since the inception of this research series 11 years ago.[2] According to this year's benchmark findings, data breaches cost companies an average of $221 per compromised record – of which $145 pertains to indirect costs, which include abnormal turnover or churn of customers and $76 represents the direct costs incurred to resolve the data breach such as investments in technologies or legal fees.

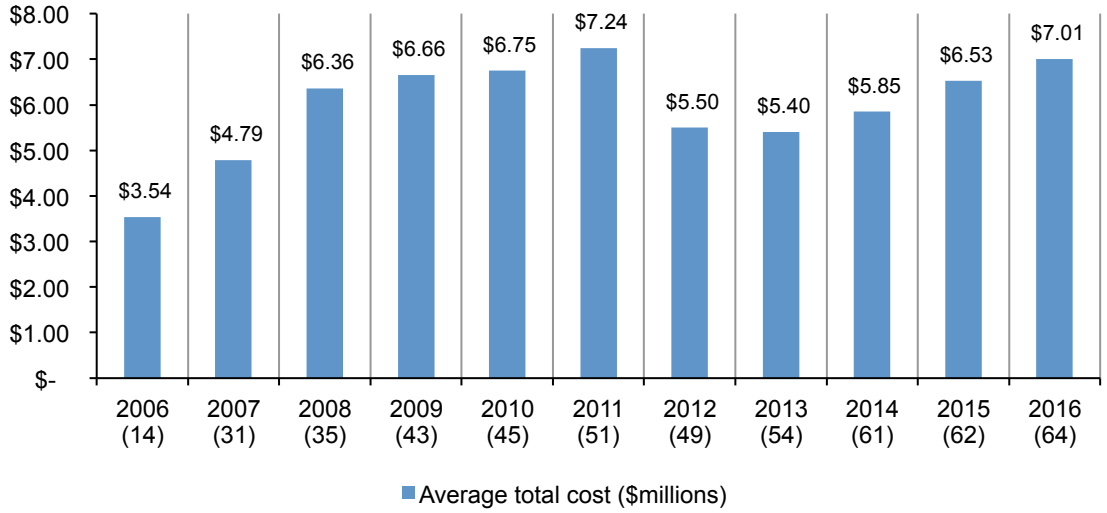
Figure 1. The average per capita cost of data breach over 11 years
Bracketed number defines the benchmark sample size



[2]Per 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.

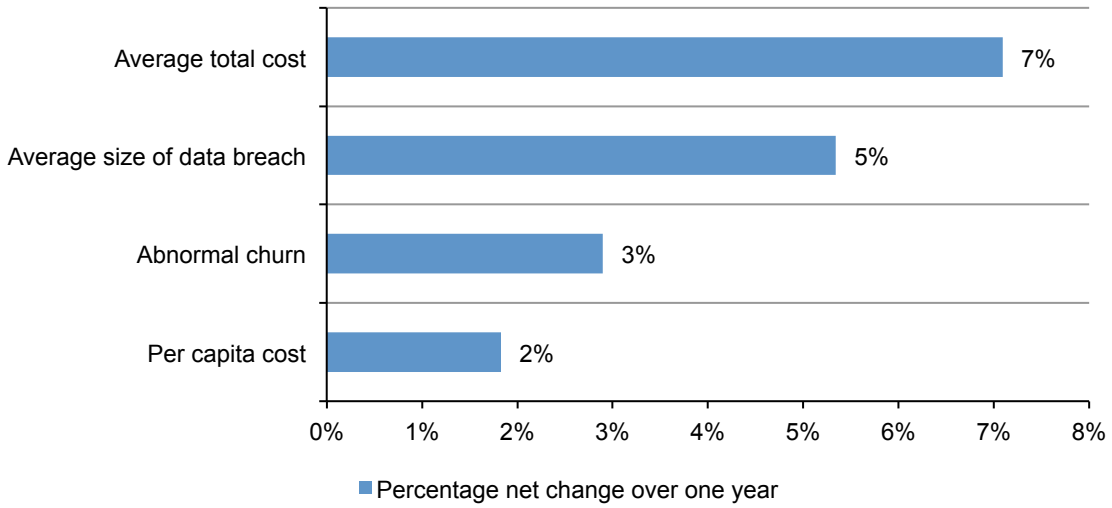
The total average organizational cost of data breach increased. Figure 2 shows interesting trends in the total average cost of data breach over the course of 11 years. The most costly organizational breach occurred in 2011 when companies spent an average $7.24 million. In 2013, companies experienced a net decrease in total data breach cost to $5.40 million. This year, the total average cost rose to $7.01 million.

Figure 2. The average total organizational cost of data breach over 11 years
(millions)



Measures reveal why the cost of data breach increased. Figure 3 reports the four net changes from last year's report. The average total cost of a data breach grew by 7 percent and the average per capita cost rose by 2 percent. Abnormal churn of existing customers increased by 3 percent. 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 5 percent.

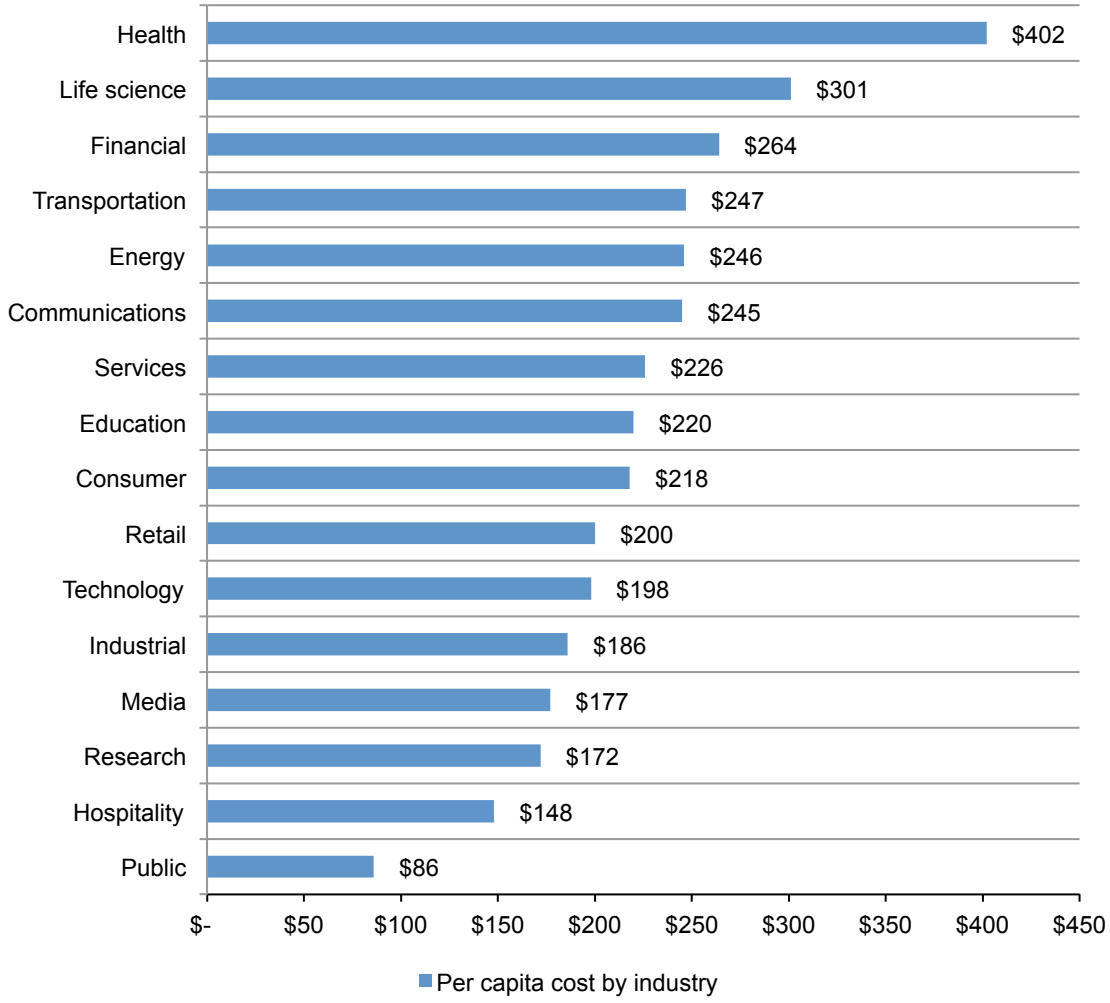
Figure 3. Cost of data breach measures
Net change defined as the difference between the 2016 and 2015 results



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, life science and financial services tend to have a per capita data breach cost that is substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research have a per capita cost well below the overall mean value.

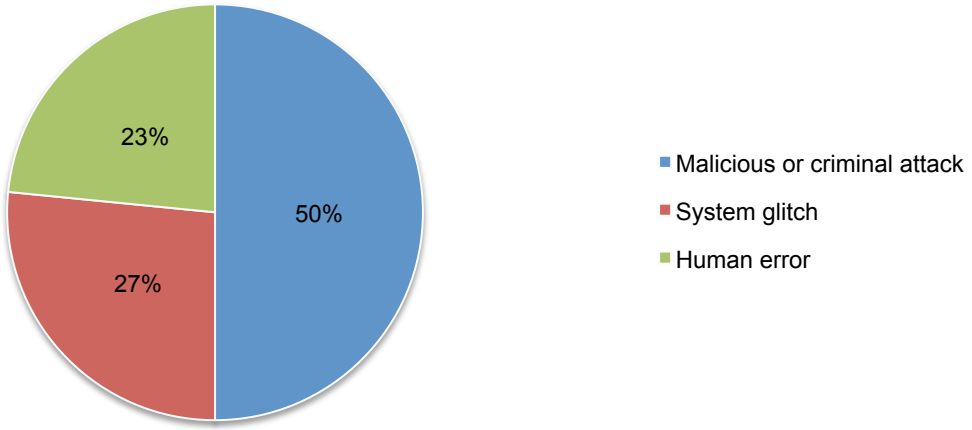
Figure 4. Per capita cost by industry classification of benchmarked companies



The root causes of data breach

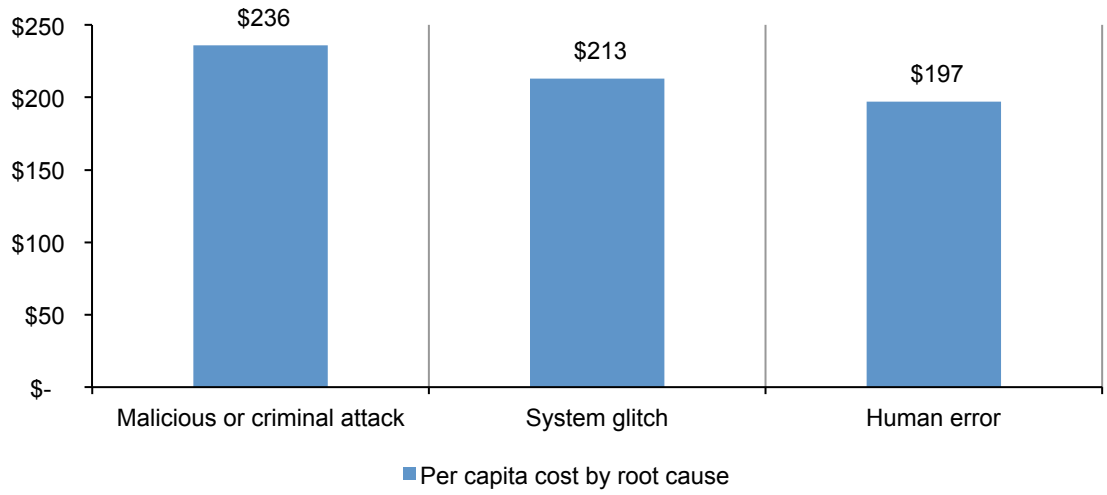
Malicious or criminal attacks continued to be the primary cause of data breach.[3] Figure 5 provides a summary of the main root causes of data breach for all 64 organizations. Fifty percent of incidents involved a malicious or criminal attack, 23 percent concerned negligent employees and 27 percent involved system glitches that includes both IT and business process failures.[4]

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 an average per capita data breach cost of $236, significantly above the mean of $221. In contrast, system glitches or human error as the root cause had per capita costs significantly below the mean ($213 and $197, respectively).

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



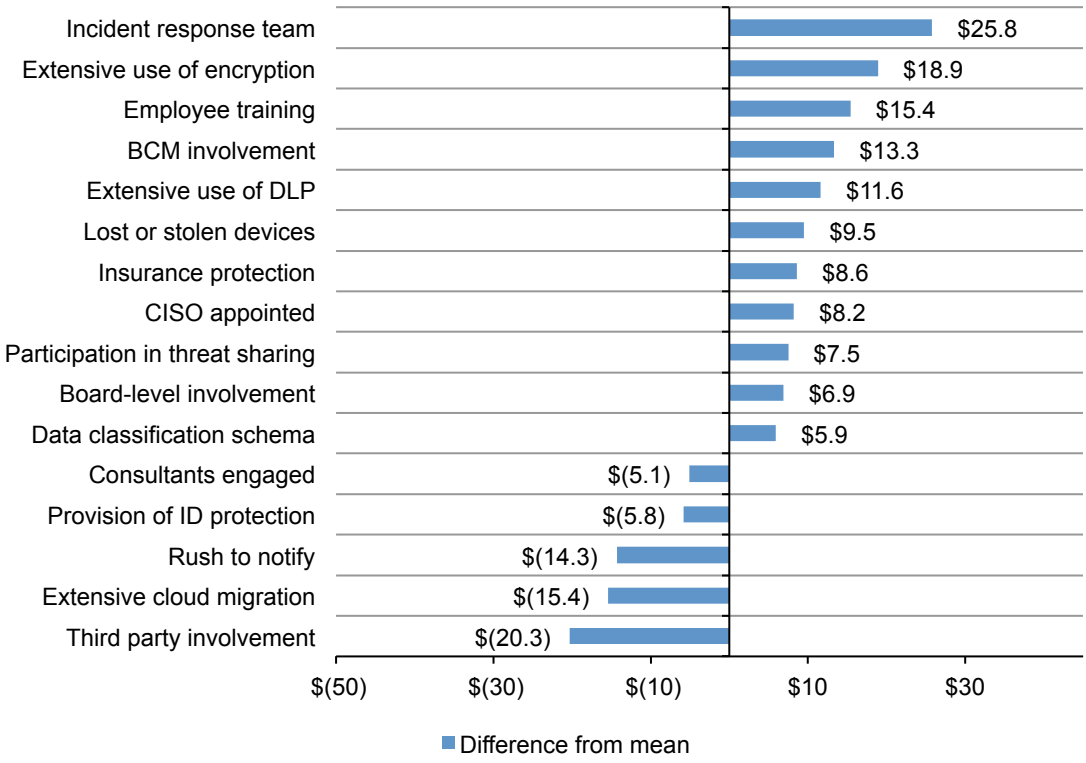
[3]Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Hackers or criminal insiders (employees, contractors or other third parties) cause malicious attacks.
[4] The most common types of attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Factors that influence the cost of data breach

Certain factors reduced the cost of data breach. As shown in Figure 7, having an incident response plan and team in place, extensive use of encryption, employee training, BCM involvement and extensive use of data loss prevention technologies are viewed as reducing the cost of data breach.

Data breaches due to third party error, extensive migration to the cloud or rush to notify increased data breach costs. For example, an incident response team can decrease the average cost of data breach from $221 to $195.20 (decrease = $25.80). In contrast, third party breaches increased the average cost to $241.30 (increase = $20.30).

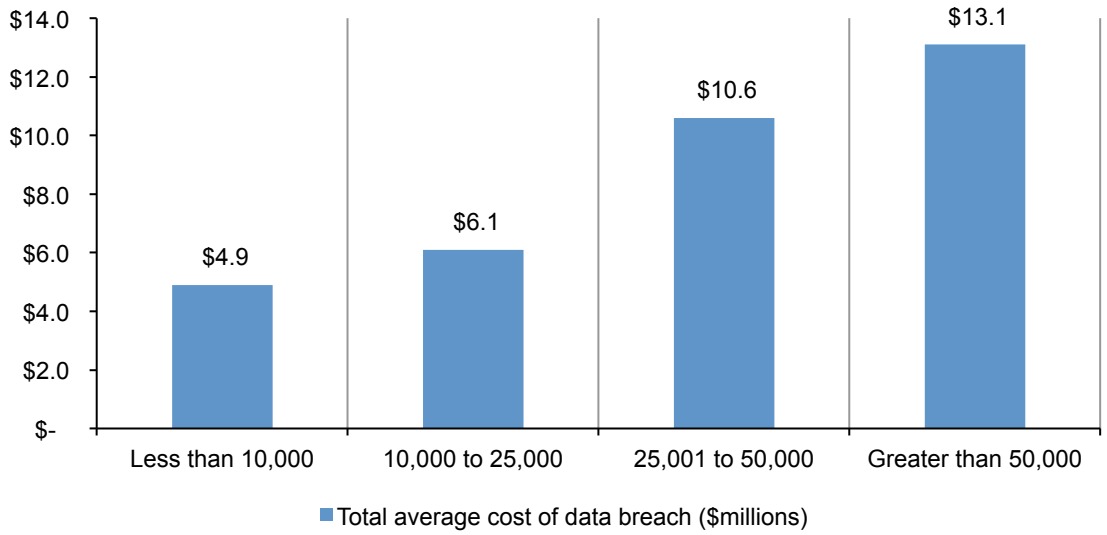
Figure 7. Impact of 16 factors on the per capita cost of data breach



Trends in the frequency of compromised records and customer turnover

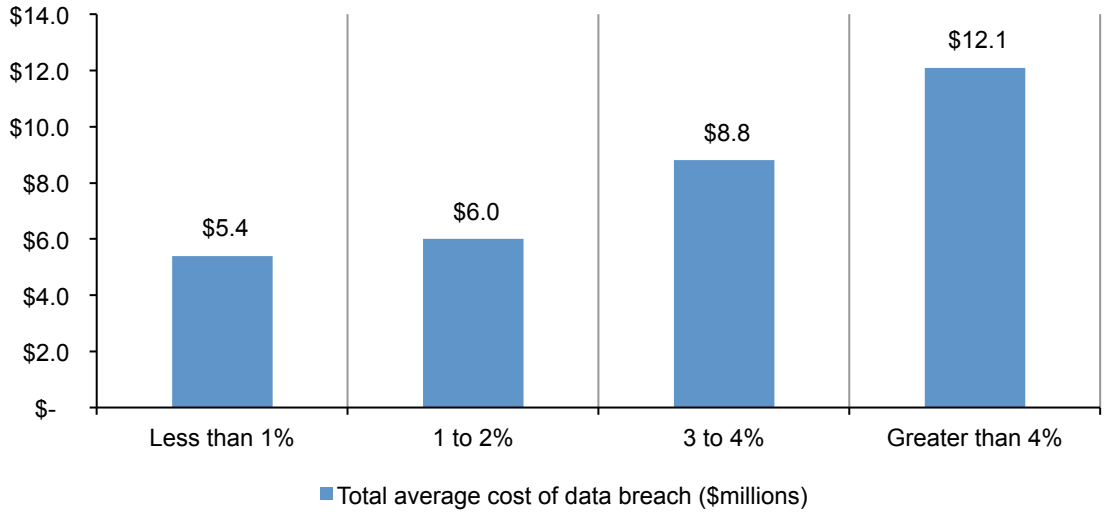
The more records lost, the higher the cost of data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for 64 benchmarked companies in ascending order by the size of the breach incident. This year, companies that had data breaches involving less than 10,000 records spent an average of $4.9 million to resolve the data breach and those companies with the loss or theft of more than 50,000 records spent $13.1 million.

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



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. Companies that experienced less than 1 percent churn, or loss of existing customers, had an average organizational cost of data breach of $5.4 million and those experiencing churn greater than 4 percent spent $12.1 million.

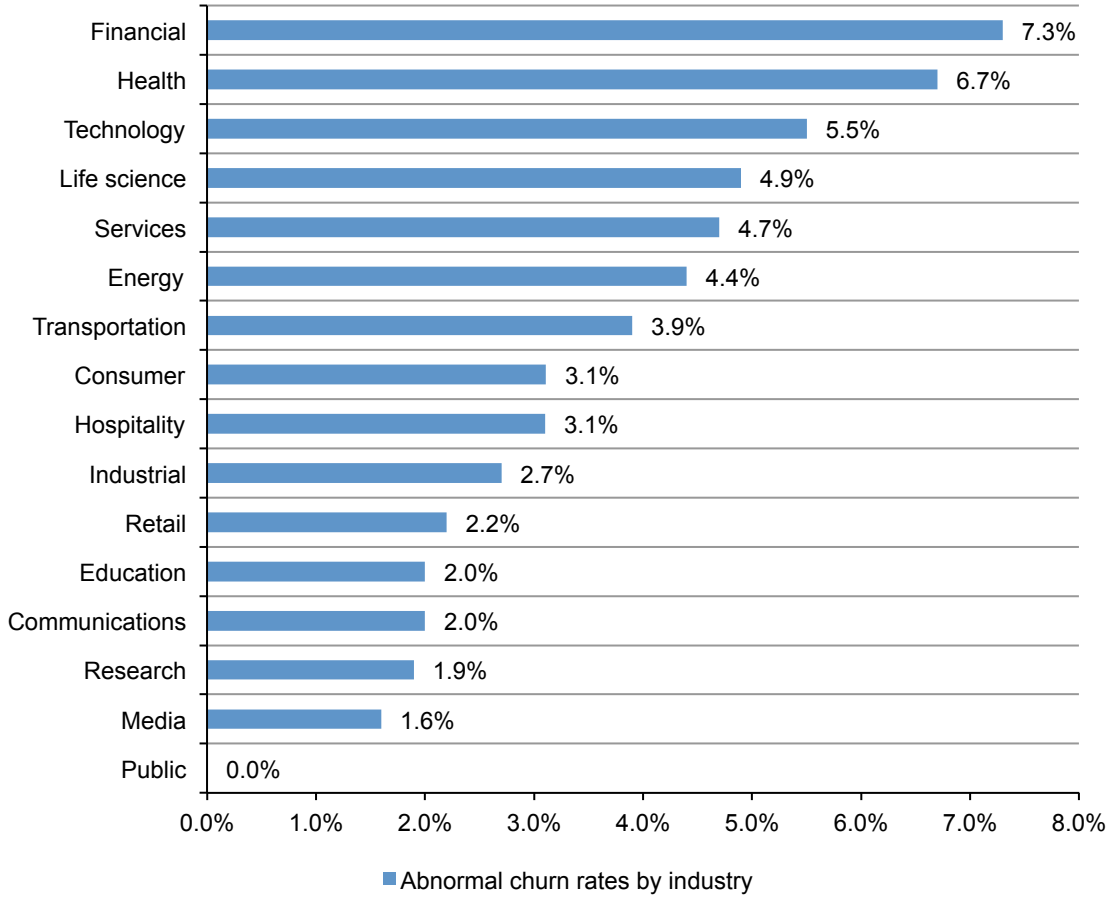
Figure 9. Total cost of data breach by abnormal churn rate



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, health, technology, life science and service organizations experienced a relatively high abnormal churn and public sector, media and research tend to experience a relatively low abnormal churn.[5]

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

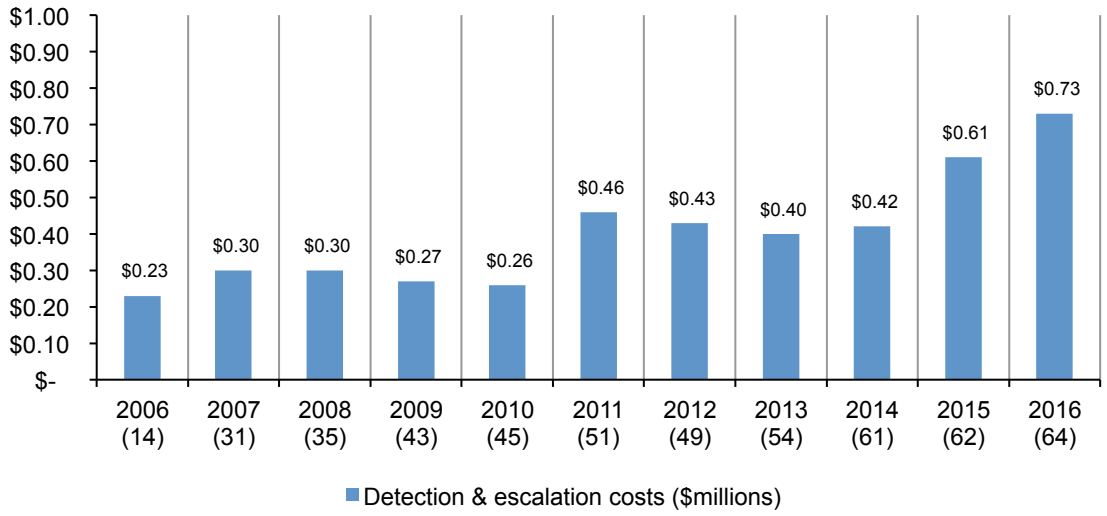


[5]Public sector organizations utilize a different churn framework, given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

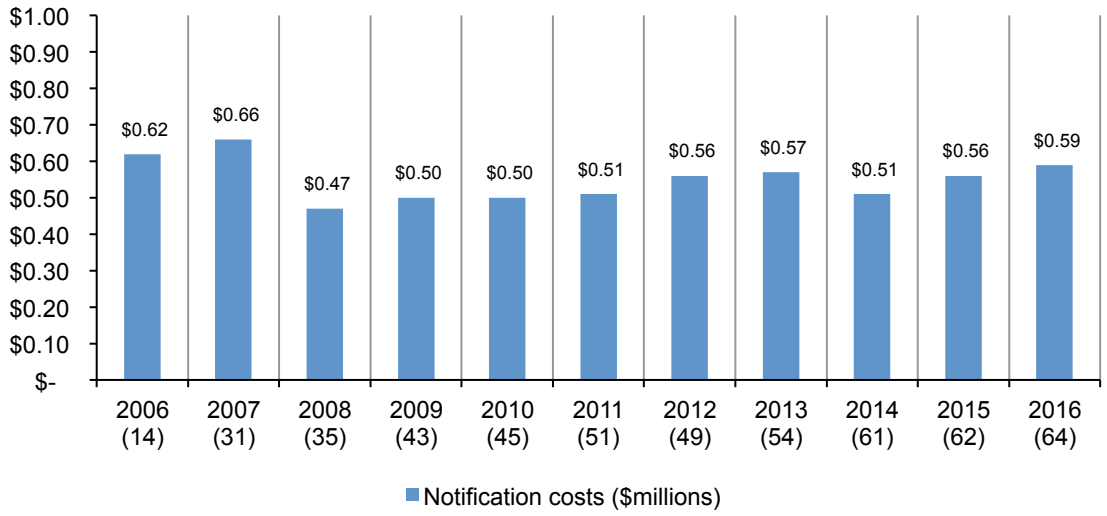
Detection and escalation costs reached a record high. Figure 11 shows the 11-year trend for such costs as forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs increased dramatically from $0.61 million in 2015 to $0.73 million in 2016, suggesting that companies are investing more heavily in these activities.

Figure 11. Average detection and escalation costs over 11 years
($ millions)



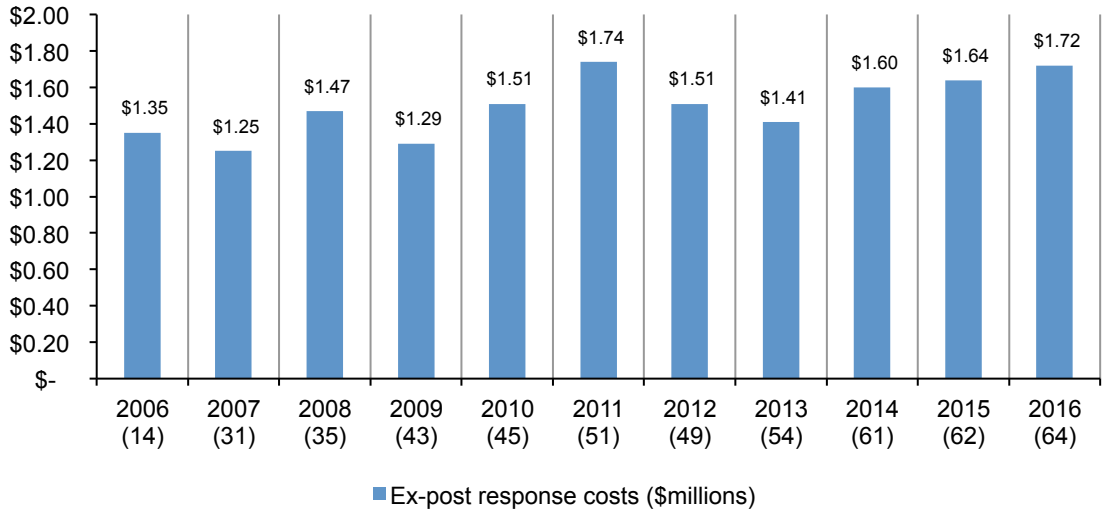
Notification costs increased slightly. Figure 12 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification costs increased slightly from $0.56 million in 2015 to $0.59 million in 2016.

Figure 12. Average notification costs over 11 years
($ millions)



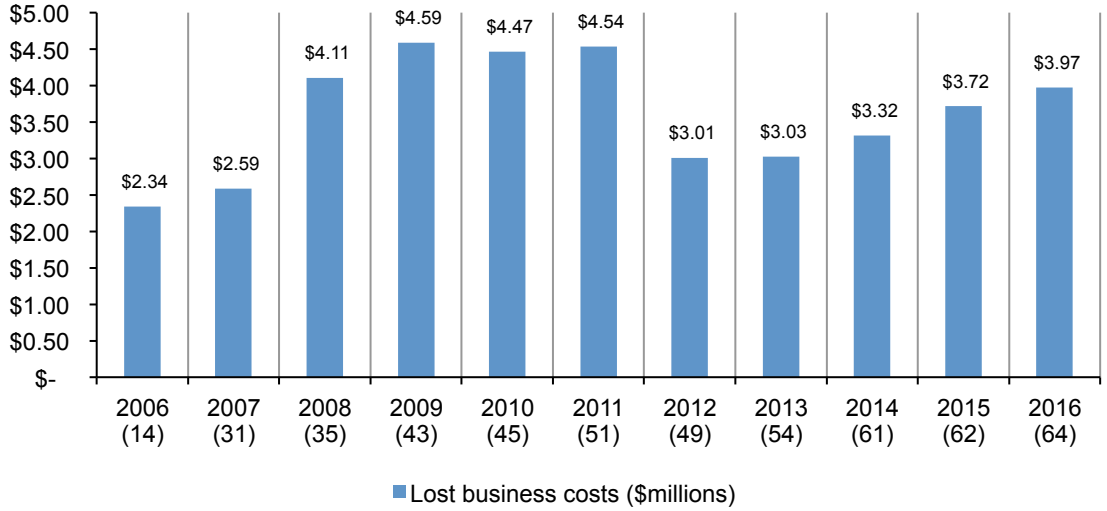
Post data breach costs increased. Figure 13 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. While average ex-post response costs decreased from an 11-year high of $1.74 million in 2011, they increased from $1.64 million in 2015 to $1.72 million in this year's study.

Figure 13. Average ex-post response costs over 11 years
($ millions)



Lost business costs grew slightly. Figure 14 reports lost business costs associated with data breach incidents over 11 years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen, lost business costs have increased since 2012. The current year's cost of $3.97 million represents an increase from $3.72 million in 2015. The highest level of lost business cost was $4.59 million in 2009.

Figure 14. Average lost business costs over 11 years
($ millions)

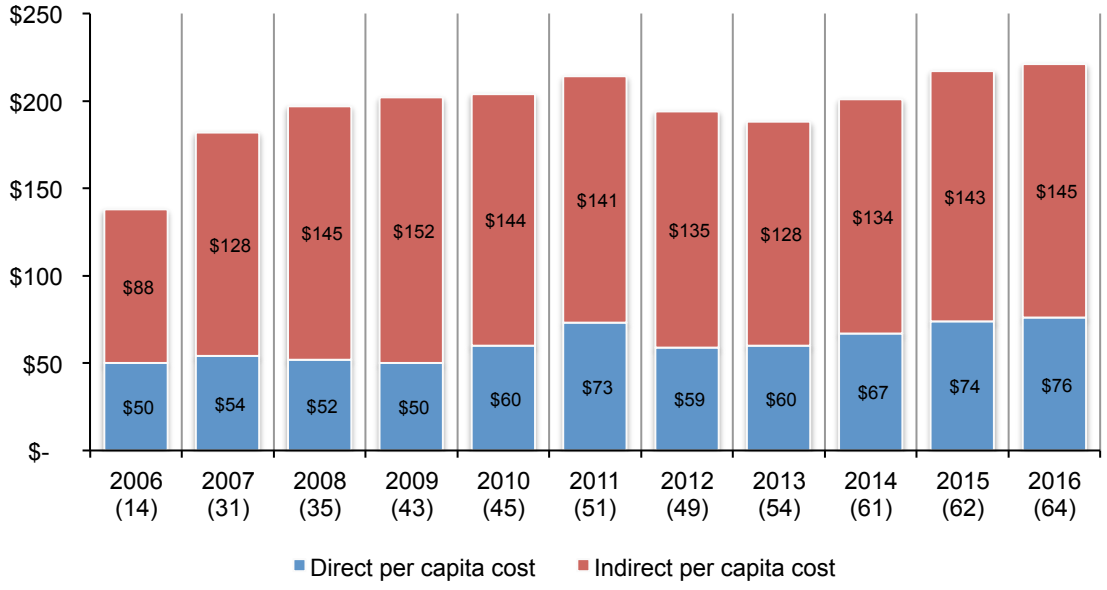


Companies continued to spend more on indirect costs than direct costs. Indirect costs pertain to what the company spends on existing internal resources to deal with the data breach. These costs could include the time employees spend on data breach notification efforts or investigations of the incident. Indirect costs also include the loss of brand value and reputation and customer churn.

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.

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 $4 – from $217 in 2015 to $221 in 2016. Indirect and direct costs both increased by $2 per compromised record.

Figure 15. Direct and indirect per capita data breach costs over 11 years



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

Companies participating in our annual study report higher costs to respond to and remediate a data breach. This increase can be attributed to investing in detection and escalation activities and lost business. The most profitable investments companies can make to mitigate the risk of future breaches are incident response plans, extensive use of encryption, participation in threat sharing, employee training, business continuity management and data loss prevention technologies.

Table 1 reports the preventive measures implemented by companies after the data breach. The most popular measures and controls implemented after the data breach have been fairly consistent. This year, the number one activity is training (52 percent) followed by expanded use of encryption (49 percent) and endpoint security solutions (48 percent).

Since 2010, the most significant increases in the investment in controls and activities are endpoint security solutions (+12 percent) and other system control practices (+10 percent). The biggest decreases concern investments in additional manual procedures and controls (-17 percent) and training and awareness programs (-15 percent).

Table 1 **Data loss prevention controls and activities**	2010	2011	2012	2013	2014	2015	2016
Endpoint security solutions	36%	41%	42%	40%	53%	50%	48%
Training and awareness programs	67%	63%	53%	51%	51%	50%	52%
Expanded use of encryption	58%	61%	52%	57%	50%	52%	49%
Additional manual procedures and controls	58%	54%	49%	46%	43%	40%	41%
Data loss prevention (DLP) solutions	42%	43%	45%	49%	39%	39%	38%
Identity and access management solutions	49%	52%	47%	43%	39%	40%	41%
Security intelligence solutions	22%	21%	26%	28%	34%	37%	39%
Other system control practices	40%	43%	38%	34%	33%	32%	30%
Strengthening of perimeter controls	20%	22%	25%	23%	21%	19%	18%
Security certification or audit	33%	29%	19%	19%	20%	19%	21%

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

Table 2 reports 11 general cost categories on a percentage basis over 10 years. Since first conducting the research, there have been interesting shifts in spending on data breaches. However, the costs have remained fairly consistent since last year's report. Lost customer business, legal services (defense) and investigations and forensics continue to have the highest level of spending.

Table 2 **Cost change**	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Investigations and forensics	8%	8%	9%	8%	11%	11%	12%	13%	14%	15%
Audit and consulting services	10%	10%	11%	12%	10%	9%	8%	7%	7%	6%
Outbound contact costs	9%	7%	6%	6%	5%	6%	5%	4%	3%	4%
Inbound contact costs	10%	8%	6%	5%	6%	5%	5%	6%	5%	4%
Public relations/ communications	1%	3%	1%	1%	1%	1%	1%	1%	1%	2%
Legal services - defense	6%	8%	9%	14%	14%	15%	15%	16%	16%	15%
Legal services - compliance	3%	3%	1%	2%	2%	3%	4%	3%	4%	3%
Free or discounted services	2%	1%	2%	1%	1%	1%	1%	2%	1%	0%
Identity protection services	3%	2%	2%	2%	2%	3%	4%	2%	2%	2%
Lost customer business	39%	41%	43%	40%	39%	37%	36%	38%	39%	40%
Customer acquisition cost	8%	9%	9%	9%	9%	9%	9%	8%	8%	9%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Part 3. Mean time to identify and contain a data breach

Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC) metrics are used to determine the effectiveness of their organization's incident response and containment processes. The MTTI metric helps organizations to understand the time it takes to detect that an incident has occurred, and the MTTC metric measures the time it takes for a responder to resolve a situation and ultimately restore service.

As shown in Figure 16, it took an average of more than six months to detect that an incident has occurred and almost two months to contain the incident.

Figure 16. Mean time to identify (MTTI) and mean time to contain (MTTC)

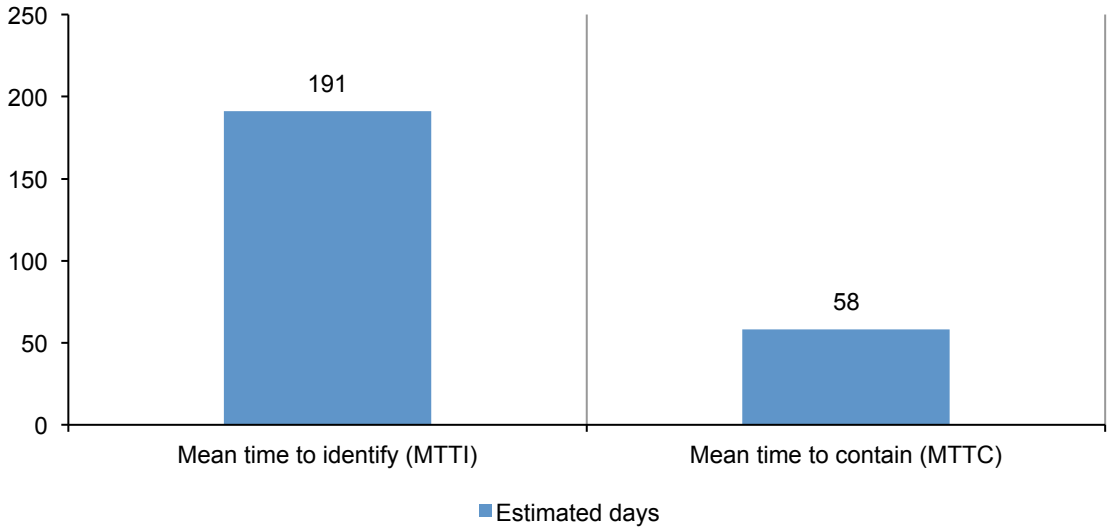
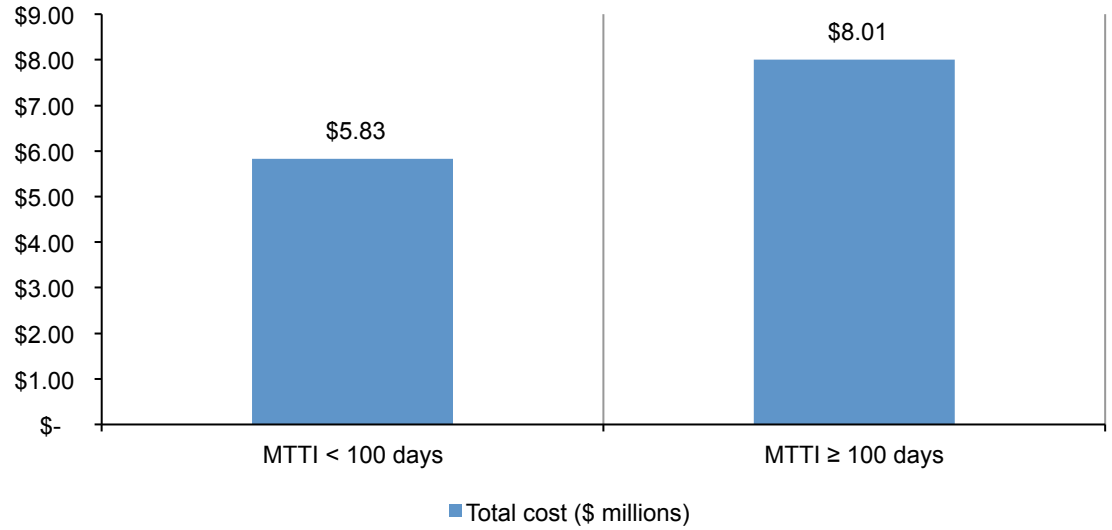


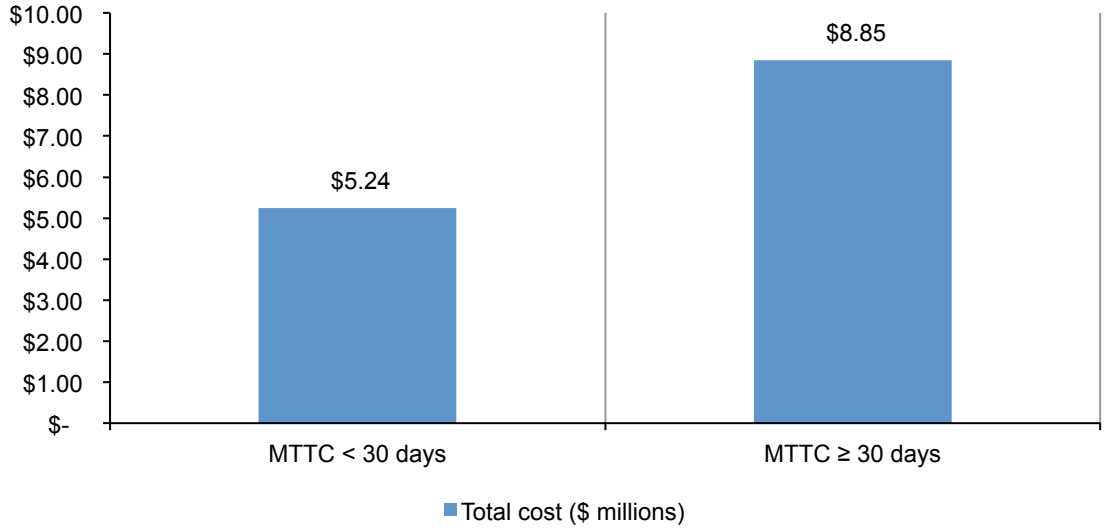
Figure 17 shows the importance of having an incident response plan in place. If the MTTI was less than 100 days, the average cost to identify the data breach was $5.83 million. However, if the MTTI is greater than 100 days, the average cost rose significantly to $8.01 million.

Figure 17. Mean time to identify the breach event (MTTI)



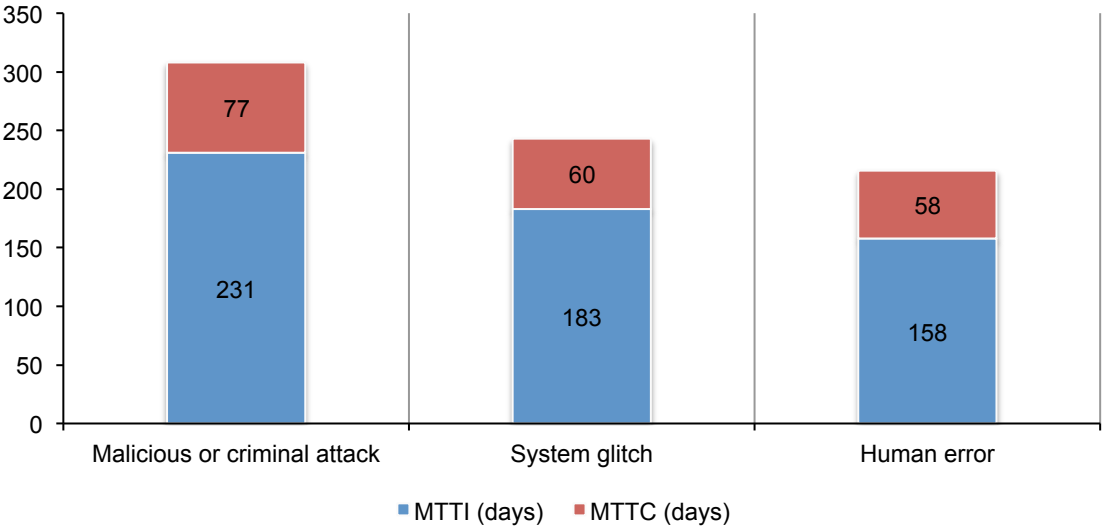
Similarly, if the time it takes to contain the breach was less than 30 days, the cost to contain the breach was $5.24 million. If it took 30 days or longer to contain the breach, the cost increased to $8.85 million, as shown in Figure 18.

Figure 18. Mean time to contain the breach event (MTTC)



The most difficult and time-consuming incident to detect and contain, as shown in Figure 19, is the malicious or criminal act (308 days). Data breaches caused by human error took less time to contain and detect (216 days).

Figure 19. Distribution of the benchmark sample by root cause of the data breach



Part 4. 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 in which they engage 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.[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 transactional payment information).

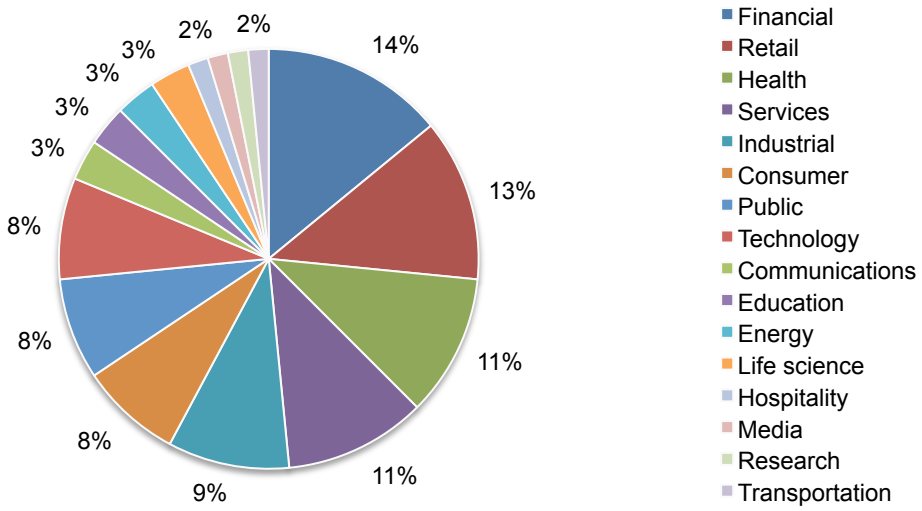
[6]In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector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

[7]In this study, we consider citizen, patient and student information as customer data.

Part 5. Organizational characteristics and benchmark methods

Figure 20 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 followed by retail, health and services.

Figure 20. 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.[8]

[8]Our 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 6. 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 that experienced 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-four companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.

- Sampling-frame bias: Because our sampling frame is judgmental, the quality of the 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 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/security/data-breach**

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.