2016 Cost of Data Breach Study: Canada

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2016
Part 1. Introduction

IBM and Ponemon Institute are pleased to present the 2016 Cost of Data Breach: Canada, our second benchmark study on the cost of data breach incidents for companies located in Canada. The average per capita cost of data breach increased from $250 to $278 and the average total organizational cost increased from 5.32 to $6.03 million.

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, France, Australia, Italy, Japan, Germany, India, Brazil, the United Arab Emirates and Saudi Arabia and, for the first time, South Africa. Since launching the study in Canada, 45 Canadian organizations have participated in this research.

This year’s study examines the costs incurred by 24 Canadian companies from 11 different industry sectors following the loss or theft of protected personal data and the notification of 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. The costs are based upon estimates provided by the individuals interviewed over a ten-month period in the companies represented in this research.

The number of breached records per incident this year ranged from 4,800 to 70,998 and the average number of breached records was 21,200. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and to include them in the study would skew the results.

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 data breach has not fluctuated significantly. Thus, suggesting 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.

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 to 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 interesting findings and implications for organizations:

The cost of data breach increased. According to the benchmark findings, the per capita cost of data breach increased from an average of $250 per compromised record to $278. The total organizational cost of data breach increased from $5.32 million in 2015 to $6.03 in 2016.

Measures reveal why data breach costs increased. Since 2015 the average total cost of data breach increased 13 percent and the per capita cost increased by 11 percent. The average data size or number of records increased by 4 percent and abnormal churn increased 3 percent.

Certain industries have higher data breach costs. Services, financial and energy companies had a per capita data breach cost substantially above the overall mean of $278. Public sector and research had a per capita cost well below the overall mean value.

Malicious attacks were the primary root cause of the data breach and more costly to resolve. Fifty-four percent of data breaches were caused by malicious or criminal attacks. Twenty-one percent of breaches were caused by system glitches and 25 percent were caused by human error. Companies that experienced malicious attacks had a per capita data breach cost of $304, which is above the mean. In contrast, companies that experienced system glitches ($250) or employee negligence ($246) had per capita costs below the mean value.

Certain factors reduced the cost of data breach. Incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement or participation in threat sharing decreased the per capita cost. Data breaches caused by extensive migration to the cloud, third party errors or lost or stolen devices increased the cost.

The more records lost, the higher the cost of the data breach. In this year’s study, the cost ranged from $3.59 million for data breaches involving 10,000 or fewer lost or stolen records to $6.88 million for the loss or theft of more than 50,000 records.

The more churn, the higher the cost of data breach. If companies lost less than 1 percent of their existing customers, the average cost of a breach averaged $4.77 million, well below the mean of $6.03 million. When companies had a churn rate of greater than 4 percent, the average cost averaged $7.88 million.

Certain industries are more vulnerable to churn. Financial, transportation, and technology organizations experienced relatively high abnormal churn and public sector and industrial companies experienced a very low abnormal churn rate

Detection and escalation costs increased significantly. Detection and escalation costs include investigative activities, assessment and audit services, crisis team management and
communication to executive management and boards of directors. Average detection and escalation costs increased from $1.68 million to $1.94 million, suggesting companies are investing more heavily in these activities.

**Notification costs increased.** These costs include IT activities associated with creation of contract databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures and inbound communication set-up. The average cost increased from $0.12 million in 2015 to $0.18 million in 2016.

**Post data breach costs increased slightly.** These costs include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. The average ex-post response increased from $1.53 million in 2015 to $1.67 million in this year's study.

**Lost business costs increased.** This cost category typically includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. These costs increased from $1.99 million in 2015 to $2.24 million in 2016.

**Both direct and indirect per capita costs increased significantly.** The indirect cost of data breach includes costs related to the amount of time, effort and other organizational resources spent to resolve the breach. In contrast, direct costs are the actual expense incurred to accomplish a given activity such as purchasing technology or hiring a consultant.
Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual’s name plus a 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 $278 (Canadian dollars).

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 24 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 24 organizations to participate in this study. Data breaches ranged from a low of 4,800 to a high of 70,998 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 Canadian 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 first conducting the research in Canada last year, 45 organizations have participated.
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 increased**. Figure 1 reports the average per capita cost of a data breach for 24 companies.² According to the benchmark findings, the cost of data breach increased from $250 per compromised record to $278 – of which $159 pertains to indirect costs, which include abnormal turnover or churn of customers and $119 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 two years**

Measured in Canadian dollars

---

²Per 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 organizational cost of data breach increased. According to Figure 2, the total average cost of data breach for 24 companies increased from $5.32 million in 2015 to $6.03.

**Figure 2. The average total organizational cost of data breach over two years**
Measured in Canadian dollars (CA$ millions)

Measures reveal why the cost of data breach increased. Figure 3 shows that since last year the average total cost of a data breach increased by 13 percent and the per capita cost increased by 11 percent. The average data breach size or number of records increased by 4 percent and abnormal churn increased by 3 percent. In the context of this research, abnormal churn is defined as the greater than expected loss of customers in the normal course of business.

**Figure 3. Cost of data breach measures**
Net change defined as the difference between the 2016 and 2015 results
Certain industries had higher data breach costs. Figure 4 reports the per capita costs for the 2016 study by industry classification. While a small sample size prevents us from generalizing industry cost differences, we find that services, financial, energy and technology companies had a per capita data breach cost substantially above the overall mean of $278. Public sector, research and consumer organizations had a per capita cost well below the overall mean value.

Figure 4. Per capita cost by industry classification of benchmarked companies
Measured in Canadian dollars

- Services: $413
- Financial: $386
- Energy: $368
- Technology: $359
- Media: $299
- Industrial: $255
- Retail: $247
- Transportation: $221
- Consumer: $199
- Research: $195
- Public: $112
The root causes of data breach

Malicious or criminal attacks caused the most data breaches.\(^3\) Figure 5 provides a summary of the main root causes of data breach for all 24 organizations. Fifty-four percent of incidents involved a malicious or criminal attack, 25 percent concerned negligent employees and 24 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

[Diagram showing root causes: 54% malicious or criminal attack, 25% system glitch, 21% human error]

Malicious attacks are most costly. Figure 6 reports the per capita cost of data breach for the three root causes of the breach incident. Malicious attacks had a per capita data breach cost of $304, which is above the mean. In contrast, companies that experienced system glitches ($250) or employee negligence ($246) had per capita costs below the mean value.

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

[Bar chart showing per capita costs: $304 for malicious or criminal attack, $250 for system glitch, $246 for human error]

\(^3\)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. Incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement or participation in threat sharing decreased the per capita cost (Figure 7) significantly. However, data breaches caused by extensive migration to the cloud, third party error or lost or stolen devices increased the cost. Hence, the availability of an incident response team reduced the per capita cost to $253 (decrease = $25). In contrast, a third party error increased the cost to $300.5 (increase = $22.50).

Figure 7. Impact of 16 factors on the per capita cost of data breach
Measured in Canadian dollars

- Incident response team: $25.00
- Extensive use of encryption: $19.10
- Employee training: $15.50
- Board-level involvement: $12.30
- Participation in threat sharing: $9.80
- CISO appointed: $8.90
- BCM involvement: $8.20
- Extensive use of DLP: $7.80
- Insurance protection: $6.70
- Data classification schema: $5.60
- Provision of ID protection: -$3.33
- Consultants engaged: -$5.50
- Rush to notify: -$7.80
- Lost or stolen devices: -$12.90
- Third party involvement: -$16.80
- Extensive cloud migration: -$22.50

Difference from mean (CA$)
Trends in the frequency of compromised records and customer turnover

The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for 24 benchmarked companies in ascending order by the size of the breach incident. In this year’s study, the cost ranged from $3.59 million for data breaches involving 10,000 or fewer to $6.88 million for the loss or theft of more than 50,000 records.

Figure 8. Total cost of data breach by size
Measured in Canadian dollars (CA$ millions)

The more churn, the higher the cost of data breach. Figure 9 reports the distribution of per capita data breach costs in ascending rate of abnormal churn. If companies lost less than 1 percent of their existing customers, the average cost of a breach was $4.77 million. When companies had a churn rate of greater than 4 percent, the average cost was $7.88 million.

Figure 9. Total cost of data breach by abnormal churn rate
Measured in Canadian dollars (CA$ millions)
Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate of benchmarked organizations for the present study. While a small sample size prevents us from generalizing the effect of industry on abnormal churn rates, our results show marked variation – wherein financial, transportation, technology and services organizations experienced relatively high abnormal churn and public sector and industrial companies experienced a very low abnormal churn rate.\(^5\)

The implication of these findings 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**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Abnormal Churn Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>6.0%</td>
</tr>
<tr>
<td>Transportation</td>
<td>4.6%</td>
</tr>
<tr>
<td>Technology</td>
<td>4.5%</td>
</tr>
<tr>
<td>Services</td>
<td>3.9%</td>
</tr>
<tr>
<td>Consumer</td>
<td>3.1%</td>
</tr>
<tr>
<td>Education</td>
<td>2.3%</td>
</tr>
<tr>
<td>Retail</td>
<td>2.3%</td>
</tr>
<tr>
<td>Media</td>
<td>2.1%</td>
</tr>
<tr>
<td>Energy</td>
<td>1.9%</td>
</tr>
<tr>
<td>Industrial</td>
<td>1.8%</td>
</tr>
<tr>
<td>Public</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

\(^5\)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 increased.** These costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and boards of directors. As shown in Figure 11, average detection and escalation costs increased from $1.68 million in 2015 to $1.94 in 2016, suggesting companies are investing more heavily in these activities.

**Figure 11. Average detection and escalation costs over two years**
Measured in Canadian dollars (CA$ millions)

Notification costs increased. Figure 12 reports the distribution of notification costs for two years. Such costs include IT activities associated with creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set-up. This year’s average cost of notification increased from $0.12 to $0.18 million in 2016.

**Figure 12. Average notification costs over two years**
Measured in Canadian dollars (CA$ millions)
Post data breach costs increased slightly. Figure 13 shows the two-year trend for costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response costs increased from $1.53 million in 2015 to $1.67 million in this year’s study.

**Figure 13. Average ex-post costs over two years**
Measured in Canadian dollars (CA$ millions)

![Ex-post response costs (CA$ millions)](image)

Lost business costs increased. Figure 14 reveals how lost business costs associated with data breach incidents have become more significant over the past two years. This cost category typically includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. These costs increased from $1.99 million to $2.24 million in the present year.

**Figure 14. Average lost business costs over two years**
Measured in Canadian dollars (CA$ millions)

![Lost business costs (CA$ millions)](image)
**Direct costs increased.** Figure 15 reports the direct and indirect cost components of data breach on a per capita basis. The indirect cost of data breach includes costs related to the amount of time, effort and other organizational resources spent to resolve the breach. In contrast, direct costs are the actual expense incurred to accomplish a given activity, such as purchasing technology or hiring a consultant. Indirect costs increased from $148 to $159. Direct costs increased $103 to $119.

**Figure 15. Direct and indirect per capita data breach costs over two years**  
Measured in Canadian dollars

![Graph showing direct and indirect per capita data breach costs from 2015 to 2016](image)
Recommendations on how to mitigate the risk and consequences of a data breach

Investments in incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement or participation in threat sharing were shown to reduce the per capita cost for Canadian companies.

Table 1 tracks the preventive measures implemented by companies after the data breach. The most popular measures or steps taken are training and awareness programs (63 percent), additional manual procedures and controls (50 percent), expanded use of encryption (46 percent) and security certification or audit (39 percent).

<table>
<thead>
<tr>
<th>Table 1. Preventive measures and controls implemented after the data breach</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training and awareness programs</td>
<td>57%</td>
<td>63%</td>
</tr>
<tr>
<td>Expanded use of encryption</td>
<td>43%</td>
<td>46%</td>
</tr>
<tr>
<td>Data loss prevention (DLP) solutions</td>
<td>19%</td>
<td>21%</td>
</tr>
<tr>
<td>Additional manual procedures and controls</td>
<td>52%</td>
<td>50%</td>
</tr>
<tr>
<td>Security intelligence systems</td>
<td>33%</td>
<td>36%</td>
</tr>
<tr>
<td>Strengthening of perimeter controls</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>Other system control practices</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>Security certification or audit</td>
<td>43%</td>
<td>39%</td>
</tr>
<tr>
<td>Endpoint security solutions</td>
<td>29%</td>
<td>33%</td>
</tr>
<tr>
<td>Identity and access management solutions</td>
<td>33%</td>
<td>38%</td>
</tr>
</tbody>
</table>

*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 two years. The two highest cost categories are lost customer business (34 percent) and investigations and forensics (25 percent).

<table>
<thead>
<tr>
<th>Table 2. Percentage cost categories over two years</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations and forensics</td>
<td>23%</td>
<td>25%</td>
</tr>
<tr>
<td>Audit and consulting services</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Outbound contact costs</td>
<td>5%</td>
<td>4%</td>
</tr>
<tr>
<td>Inbound contact costs</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Public relations/communications</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Legal services – defense</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Legal services – compliance</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Free or discounted services</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Identity protection services</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Lost customer business</td>
<td>34%</td>
<td>34%</td>
</tr>
<tr>
<td>Customer acquisition cost</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Part 3. Time to identify and contain data breaches impact cost

Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC) metrics are used to determine the effectiveness of an 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 more than five months to detect that an incident occurred and almost two months to contain the incident.

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

<table>
<thead>
<tr>
<th>Estimated days</th>
<th>MTTI &lt; 100 days</th>
<th>MTTI ≥ 100 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to identify (MTTI)</td>
<td>167 days</td>
<td>48 days</td>
</tr>
<tr>
<td>Mean time to contain (MTTC)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 $5.25 million. However, if the MTTI was greater than 100 days, the average cost rose significantly to $7.03 million.

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

<table>
<thead>
<tr>
<th>Total cost (CAS$ millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTTI &lt; 100 days</td>
</tr>
<tr>
<td>MTTI ≥ 100 days</td>
</tr>
</tbody>
</table>
Similarly, if the time it took to contain the breach was less than 30 days, the cost to contain the breach was $5.51 million. If it took 30 days or longer to contain the breach, the cost increased to $6.79 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, was the malicious or criminal act (239 days). Data breaches caused by human error took less time (170 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 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.\(^6\)

- **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, 11 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

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. 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

8Our sampling criteria only included companies experiencing a data breach between 1,000 and 100,000 lost or stolen records sometime during the past 12 months. We excluded catastrophic data breach incidents to avoid skewing overall sample findings.
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 | I | 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.

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 Canadian 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. Twenty-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.