2015 Cost of Data Breach Study: Canada

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
May 2015

Ponemon Institute© Research Report

2015[1] Cost of Data Breach Study: Canada

Ponemon Institute, May 2015

Part 1. Introduction

IBM and Ponemon Institute are pleased to present the *2015 Cost of Data Breach: Canada* our first benchmark study on the cost of data breach incidents for companies located in Canada. In this inaugural study, the average per capita cost of data breach is $250 and the average total organizational cost is $5.32 million.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States 10 years ago. Since then, we have expanded the study to include the United Kingdom, France, Australia, Italy, Japan, Germany, India and Brazil and the United Arab Emirates and Saudi Arabia.

Canada at a glance

- 21 Canadian companies participated
- $5.32 million is the average total cost of data breach
- $250 is the average cost per lost or stolen record
- 52% of data breaches involved malicious or criminal attacks

This year's study examines the costs incurred by 21 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 5,199 to 74,550 and the average number of breached records was 20,456. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and to include them in the study would skew the results.

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

The biggest component of the per capita cost of data breach is detection and escalation. According to the benchmark findings, data breaches cost companies an average of $250 per compromised record. The highest component pertains to detection & escalation costs at $91. Post data breach response (ex-post response) and lost business were $67 and $84, respectively. Notification costs represented only $8 per compromised record.

Total organizational cost of data breach. The total average cost of data breach for the 21 companies represented in this research was $5.32 million. The largest cost component was lost business at $1.99 million on average. The smallest cost component was notification at $0.12 million on average.

Certain industries have higher data breach costs. Financial, services, technology and energy had a per capita data breach cost substantially above the overall mean of $250. Public sector, education, and consumer organizations had a per capita cost well below the overall mean value.

Malicious or criminal attacks cause the most data breaches. Fifty-two percent of incidents involved a data theft (exfiltration) or criminal misuse. System glitch and employee negligence or human error both represents 24 percent of all data breaches.

[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 2014 calendar year.

Malicious attacks are most costly. Companies that experienced malicious attacks had a per capita data breach cost of $279, which is above the mean. In contrast, companies that experienced system glitches ($223) or employee negligence ($214) had per capita costs below the mean value.

Certain factors reduce the cost of data breach. Incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement, CISO appointments, business continuity management and insurance protection decreased the per capita cost. However, third party involvement, lost or stolen devices, quick notification and engagement of consultants increased the cost.

The more records lost, the higher the cost of the data breach. In this year's study, the cost ranged from $2.15 million for data breaches involving 10,000 or fewer lost or stolen records to $9.52 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 could be $1.85 million, well below the mean of $5.32 million. When companies had a churn rate of greater than 4 percent, the average cost could be $10.10 million.

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

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 $250 (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 2015 study began in January 2014 and interviews were completed in March 2015. In each of the 21 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 21 organizations to participate in this study. Data breaches ranged from a low of 5,199 to a high of 74,550 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 Canada 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.

Part 2. Key Findings

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

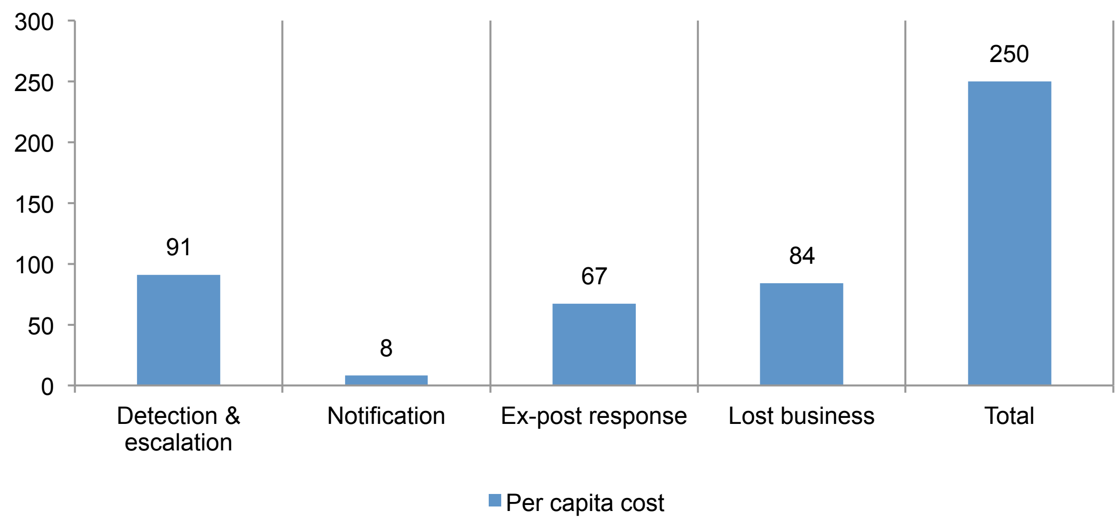
- Understanding the cost of data breach
- The root causes of data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records and customer turnover
- Trends in the cost components of data breach
- Recommendations on how to mitigate the risk and consequences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

Understanding the cost of data breach

The biggest component of the per capita cost of data breach is detection and escalation. Figure 1 reports the average per capita cost of a data breach for 21 companies.[2] According to the benchmark findings, data breaches cost companies an average of $250 per compromised record. The highest component pertains to detection & escalation costs at $91.

These costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and boards of directors. Post data breach response (ex-post response) and lost business were $67 and $84, respectively. Notification costs represented only $8 per compromised record.

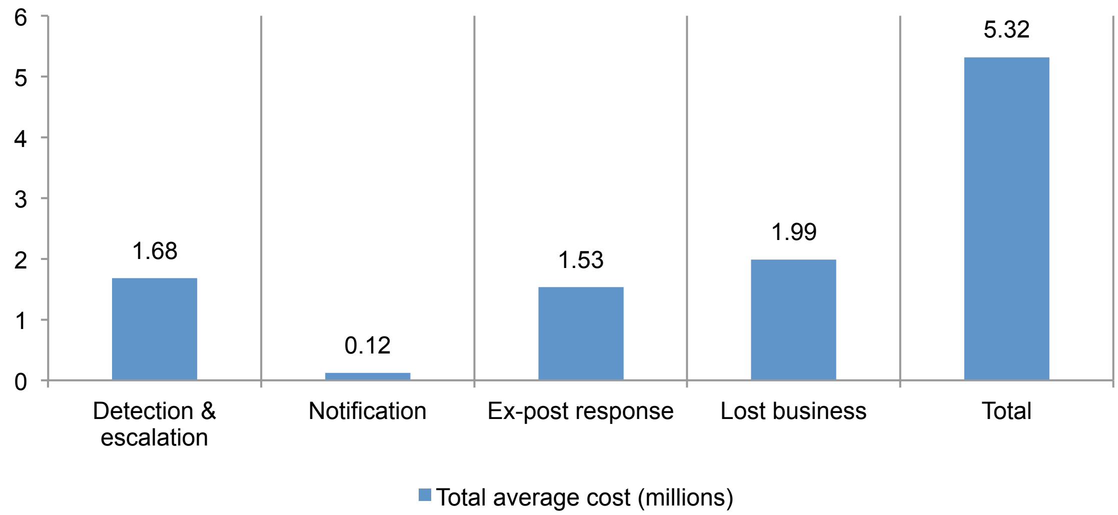
Figure 1. The average per capita cost of data breach
Measured in Canadian dollars



[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.

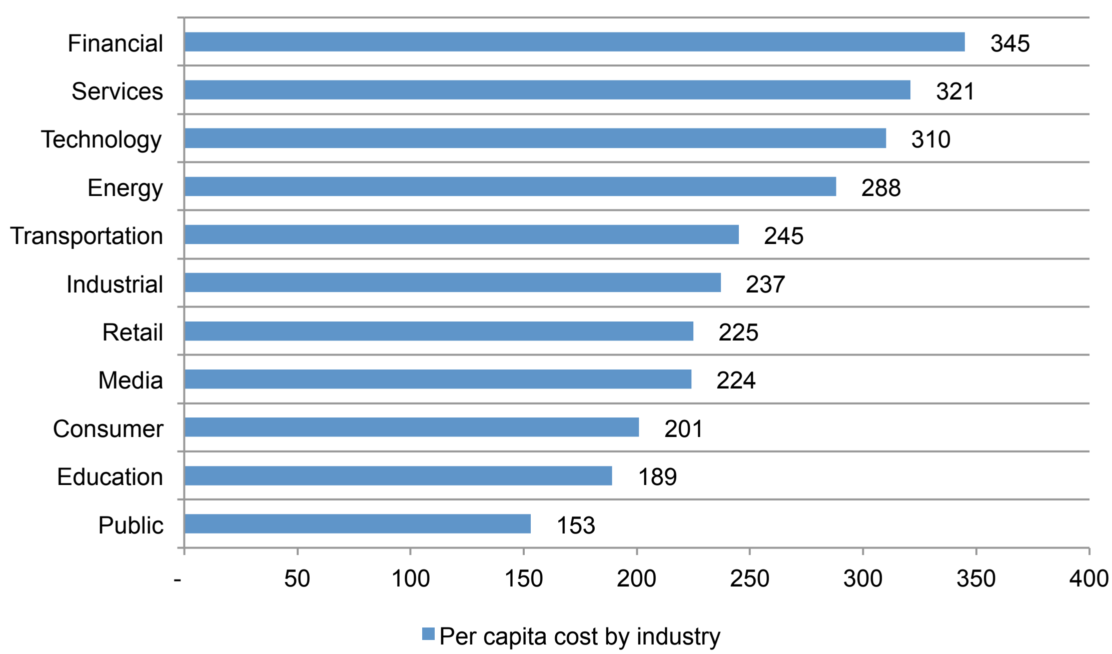
Total organizational cost of data breach. Figure 2 shows the total average cost of data breach for 21 companies was $5.32 million. The largest cost component was lost business at $1.99 million on average. The smallest cost component was notification at $0.12 million on average.

Figure 2. The average total organizational cost of data breach
Measured in Canadian dollars (millions)



Certain industries have higher data breach costs. Figure 3 reports the per capita costs for the 2015 study by industry classification. While a small sample size prevents us from generalizing industry cost differences, financial, services, technology and energy had a per capita data breach cost substantially above the overall mean of $250. Public sector, education, and consumer organizations had a per capita cost well below the overall mean value.

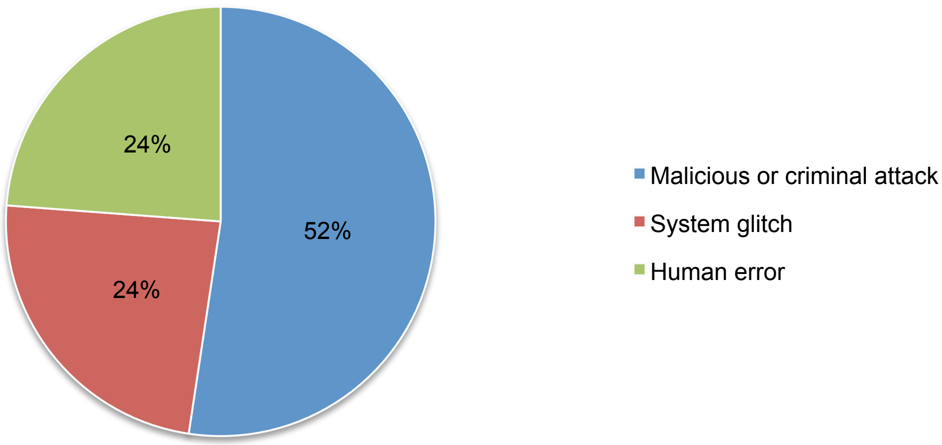
Figure 3. Per capita cost by industry classification of benchmarked companies
Measured in Canadian dollars



The root causes of data breach

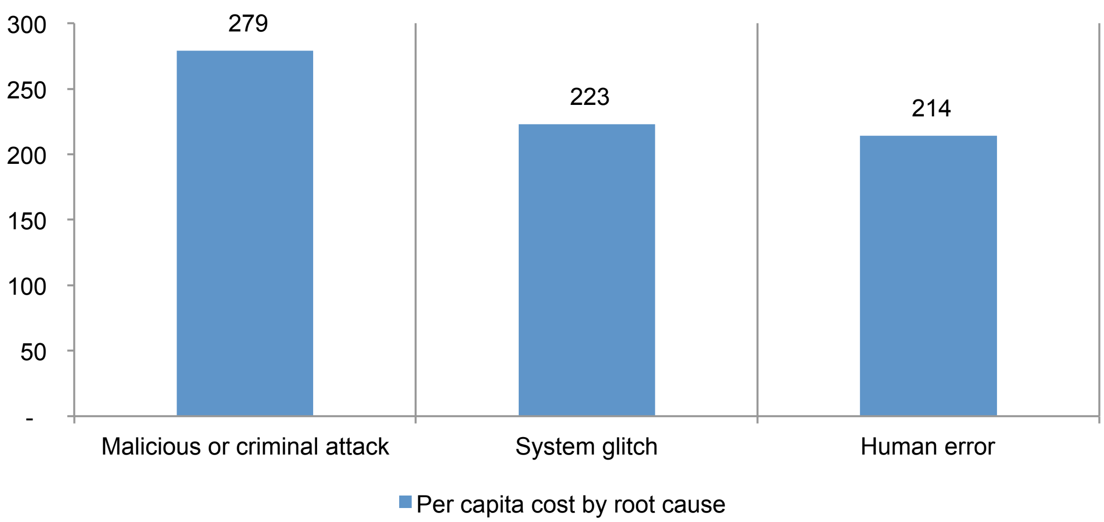
Malicious or criminal attacks cause the most data breaches.[3] Figure 4 provides the main root causes of data breach for all 21 organizations. Fifty-two percent of incidents involved a data theft (exfiltration) or criminal misuse.[4] System glitch and employee negligence or human error both represents 24 percent of all data breaches.

Figure 4. Distribution of the benchmark sample by root cause of the data breach



Malicious attacks are most costly. Figure 5 reports the per capita cost of data breach for the three root causes of the breach incident. Companies that experienced malicious attacks had a per capita data breach cost of $279, which is above the mean. In contrast, companies that experienced system glitches ($223) or employee negligence ($214) had per capita costs below the mean value.

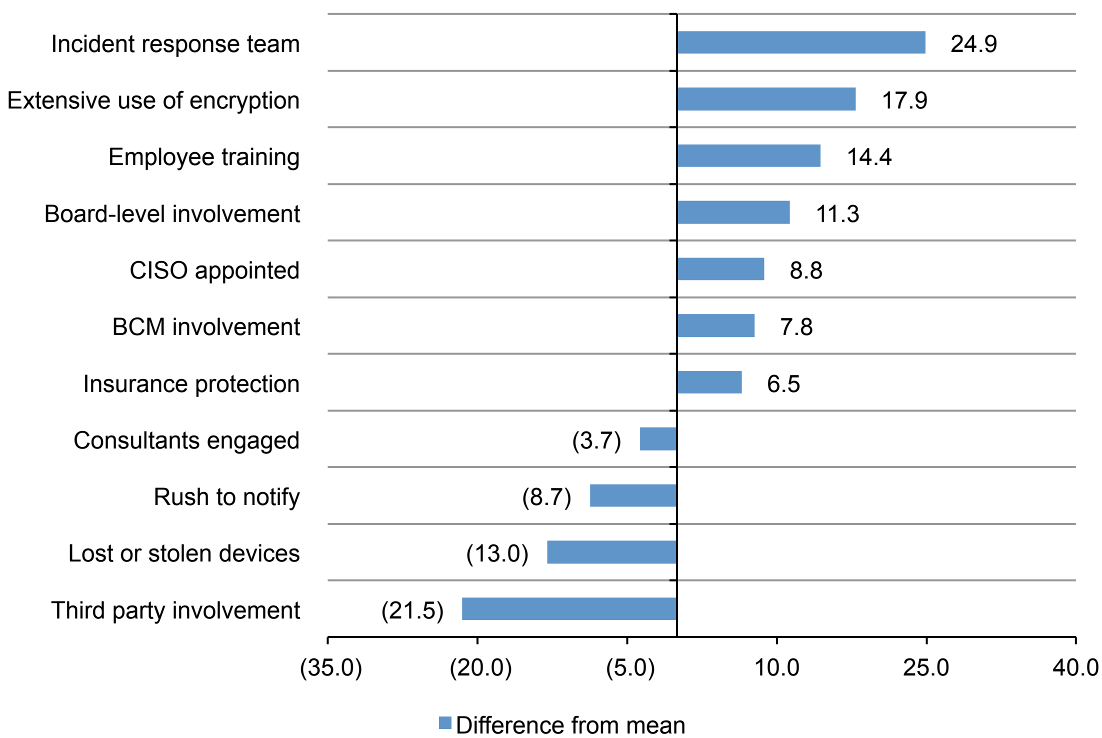
Figure 5. Per capita cost for three root causes of the data breach
Measured in Canadian dollars



[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 malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Certain factors reduce the cost of data breach. Incident response teams and plans, extensive use of encryption, employee training programs, board-level involvement, CISO appointments, business continuity management and insurance protection decreased the per capita cost (Figure 6). However, third party involvement, lost or stolen devices, quick notification and engagement of consultants increased the cost. Hence, the availability of an incident response team reduced the per capita cost by $24.9 to $225.10 (decrease = $24.9). In contrast, a third party error increase the cost by $21.5 to $271.5 (increase = $21.50) .

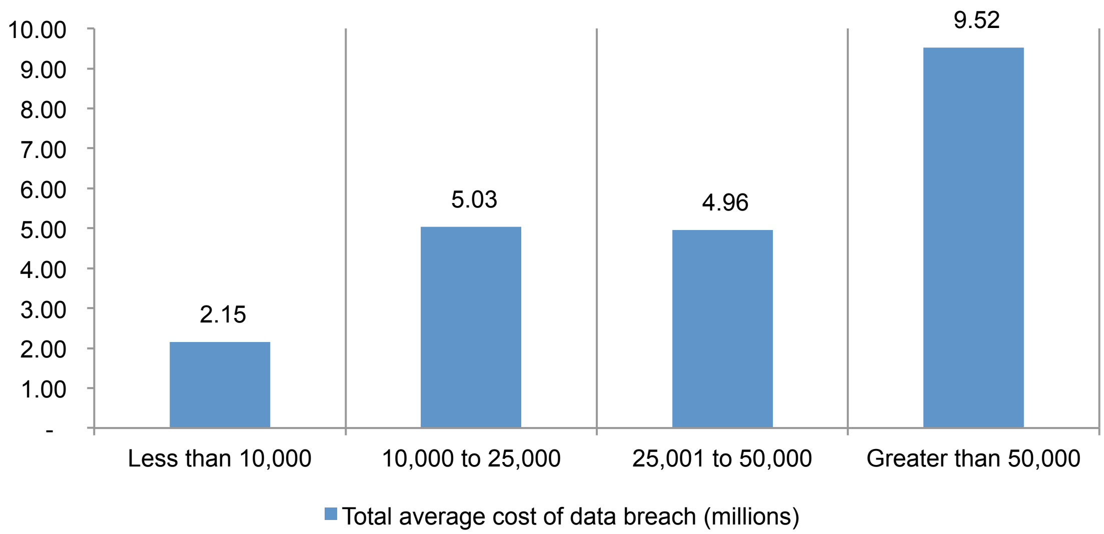
Figure 6. Impact of 11 factors on the per capita cost of data breach
Measured in Canadian dollars



Trends in the frequency of compromised records and customer turnover

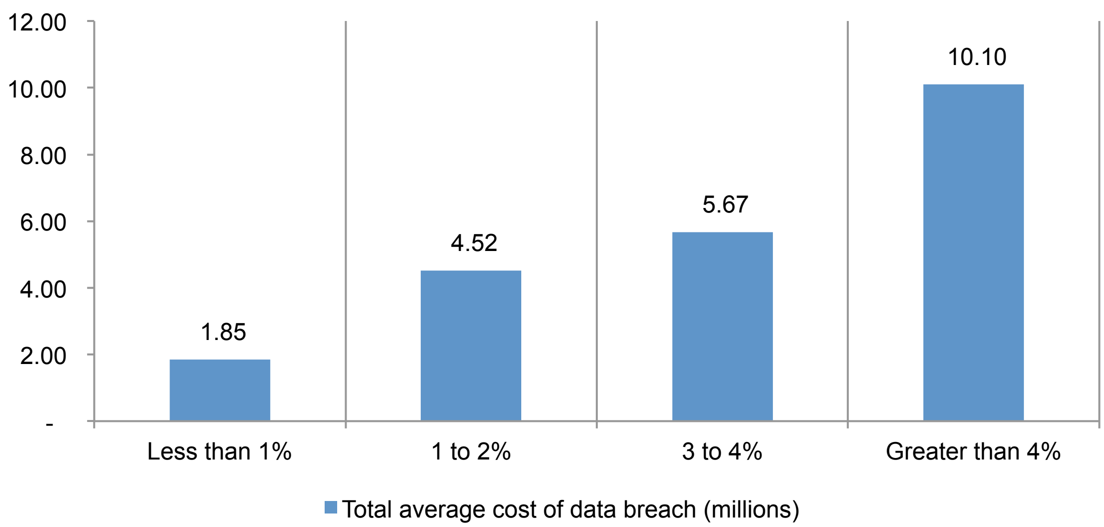
The more records lost, the higher the cost of the data breach. Figure 7 shows the relationship between the total cost of data breach and the size of the incident for 21 benchmarked companies in ascending order by the size of the breach incident. In this year's study, the cost ranged from $2.15 million for data breaches involving 10,000 or fewer to $9.52 million for the loss or theft of more than 50,000 records.

Figure 7. Total cost of data breach by size
Measured in Canadian dollars (millions)



The more churn, the higher the cost of data breach. Figure 8 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 $1.85 million, well below the mean of $5.32 million. When companies had a churn rate of greater than 4 percent, the average cost was $10.10 million.

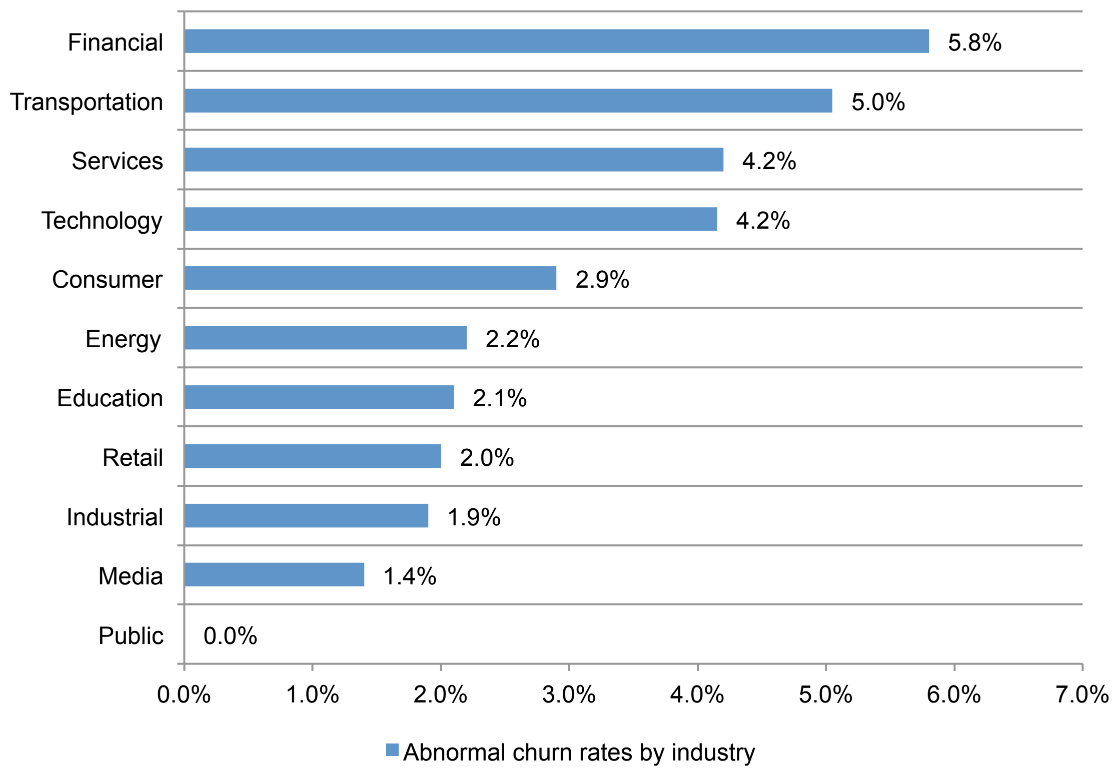
Figure 8. Total cost of data breach by abnormal churn rate
Measured in Canadian dollars (millions)



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 affect of industry on abnormal churn rates, our results show marked variation – wherein financial, transportation, services and technology organizations experienced relatively high abnormal churn and public sector and media 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 9. Abnormal churn rates by industry classification of benchmarked companies

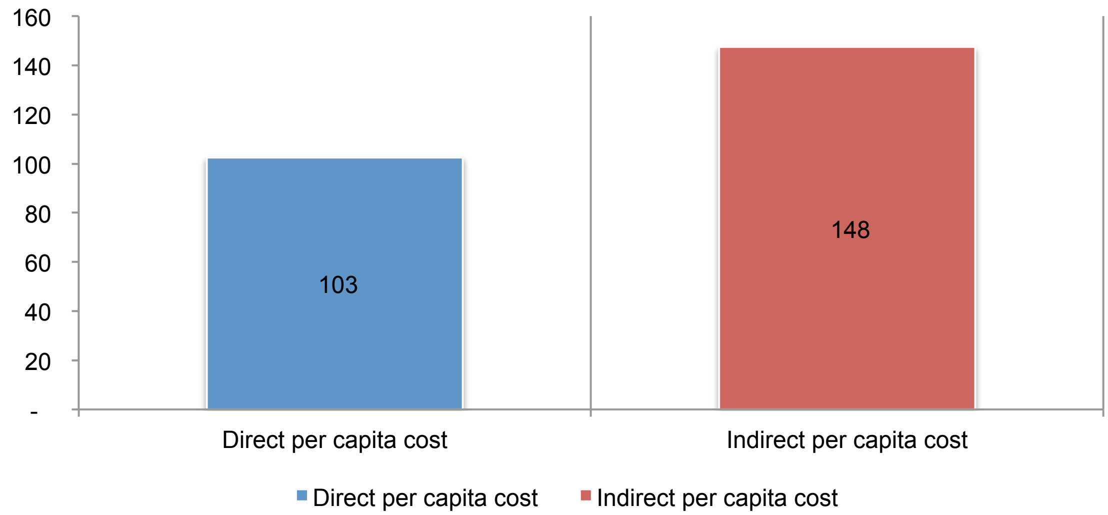


[5]Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

Indirect costs are higher than direct costs. Figure 10 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. Average indirect costs were $148. In contrast, direct costs are the actual expense incurred to accomplish a given activity such as purchasing a technology or hiring a consultant. These average direct costs were $103.

Figure 10. Direct and indirect per capita data breach costs
Measured in Canadian dollars



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

Investment in improving data protection practices is important to minimize the occurrence and financial consequences. An incident response plan in place, extensive use of encryption, employee training, board-level involvement, the appointment of a CISO with enterprise-wide responsibility, involvement of business continuity management in the remediation of the breach and insurance protection all appear to reduce data breach costs for Canadian companies.

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

In addition to measuring specific cost activities relating to the leakage of personal information, we report in Table 1 the preventive measures implemented by companies after the data breach. The most popular measures or steps taken are training and awareness programs (57 percent), additional manual procedures and controls (52 percent), expanded use of encryption (43 percent) and security certification or audit (43 percent).

Table 1. Preventive measures and controls implemented after the data breach	2015
Training and awareness programs	57%
Additional manual procedures & controls	52%
Expanded use of encryption	43%
Security certification or audit	43%
Security intelligence systems	33%
Identity and access management solutions	33%
Endpoint security solutions	29%
Data loss prevention (DLP) solutions	19%
Strengthening of perimeter controls	19%
Other system control practices	19%

*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 (23 percent).

Table 2. Percentage cost categories	2015
Lost customer business	34%
Investigations & forensics	23%
Audit and consulting services	10%
Customer acquisition cost	9%
Legal services – compliance	6%
Outbound contact costs	5%
Legal services – defense	4%
Free or discounted services	3%
Inbound contact costs	2%
Public relations/communications	2%
Identity protection services	2%
Total	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:

- <u>Detection or discovery</u>: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.
- <u>Escalation</u>: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- <u>Notification</u>: 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.
- <u>Post data breach</u>: 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 payment transactional information).

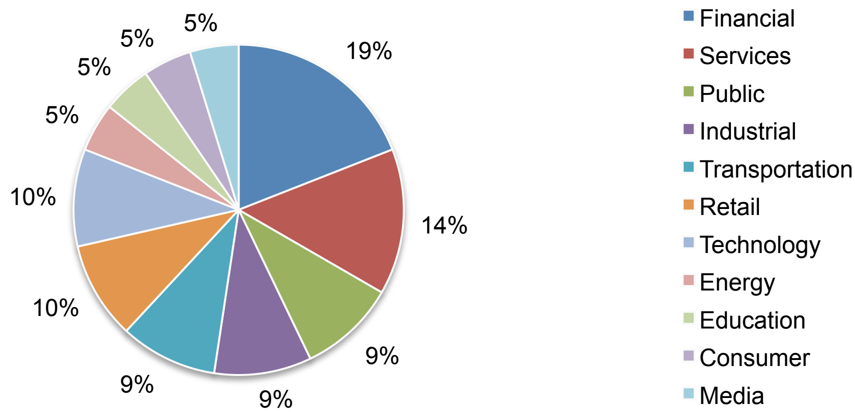
[6] In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector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

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

Part 4. Organizational characteristics and benchmark methods

Figure 11 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 11 industries are represented. The largest sectors are financial services and services.

Figure 11. 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]

[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.

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 Canadian 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. 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 results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

- Unmeasured factors: To keep the interview script concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

- Extrapolated cost results: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

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.

SEW03065-CAEN-00