2013 Cost of Data Breach Study: Australia

Benchmark research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
May 2013
Part 1. Executive Summary

Symantec Corporation and Ponemon Institute are pleased to present the 2013 Cost of Data Breach: Australia, our fourth annual benchmark study concerning the cost of data breach incidents for companies located in Australia. Ponemon Institute research indicates that data breaches continue to have serious financial consequences for organisations. In this year’s study, the average per capita cost of data breach has once again increased from $138 to $141.

Ponemon Institute conducted its first Cost of Data Breach study in the United States eight years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, India, Italy, Japan and, for the first time this year, Brazil. To date, 78 Australian organisations have participated in the benchmarking process since the inception of this research series.

This year’s study examines the costs incurred by 21 Australian companies in 10 industry sectors after those companies experienced the loss or theft of protected personal data and then had to notify breach victims as required by various laws. It is important to note the costs presented in this research are not hypothetical but are from actual data loss incidents. They are based upon cost estimates provided by individuals interviewed over a ten-month period in companies represented in this research.

The number of breached records per incident this year ranged from approximately 5,707 records to more than 65,521 records. This year the average number of breached records was 20,252. We do not include organisations that had data breaches in excess of 100,000 because they are not representative of most data breaches and including them in the study would skew the results. The cost for the 21 data breach case studies in this year’s report is presented in Appendix 1.

The report examines a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-poste) response. We also analyse the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates.

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

- **The per capita cost of data breach has steadily increased.** For the fourth consecutive year, the cost per lost or stolen record and the total organisational cost increased. In 2011, the cost was $138 and increased by $3 to $141 in 2012. We define a record as information that identifies an individual whose personal information has been compromised in a data breach.

- **The total average cost of data breach significantly increased.** The average total organisational cost of data breach increased from $2.16 million in 2011 to $2.72 million in 2012 – a 23 percent increase in one year.

- **Fewer customers are abandoning the organisation following the data breach.** Average churn rates decreased from 3.4 percent to 2.9 percent, which means fewer customers are leaving organisations following a data breach. Despite declining churn, certain industries, such as financial, service companies and technology are more susceptible to high customer churn, which causes their data breach costs to be higher than other industries. Taking steps

---

1 The Cost of Data Breach report is dated as a 2013 publication. Please note that all data breach incidents studied in this year’s report happened in the 2012 calendar year. Thus, all figures reflect the 2012 data breach incidents.

2 The need for data breach notification law was recommended by the Australian Law Reform Commission in 2008. Since then, however, there has been debate, but no clear legislative movement to enact mandatory notifications to breach victims.
to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.

- **Malicious or criminal attacks are most often the root cause of the data breach.** Forty-three percent of organisations say the root cause was malicious or criminal attacks. This increased from 36 percent in 2011. Thirty-three percent of breaches involved negligent employees or contractors and 24 percent say it was due to IT and business process failures. Accordingly, organisations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker.

- **Malicious or criminal attacks are the most costly data breaches.** The per capita cost of a data breach caused by data theft or abuse averaged $159. In comparison, the cost of a data breach involving a system glitch or negligent employee (human factor) cost $131 and $125 per compromised record, respectively.

- **Lost business costs decrease.** The cost associated with business losses decreased from $.84 million in 2011 to $.78 million in 2012. These costs refer to abnormal turnover of customers (a higher than average loss of customers for the industry or organisation), increased customer acquisition activities, reputation losses and diminished goodwill.

- **Detection and escalation cost increase sharply.** The costs associated with detection and escalation activities increased from $.77 million in 2011 to $1.40 million in 2012. This category refers to activities that enable a company to detect the breach and determine its root cause. It also includes upstream and lateral communications that are required to focus activities on the resolution of the data breach and keep management informed.

- **Ex-poste response costs increase significantly.** The costs associated with ex-poste response increased from approximately $.47 million in 2011 to $.81 million in 2012. Ex-poste response refers to all activities that attempt to address victim, regulator and plaintiff counsels’ concerns about the breach incident. This cost category also includes legal and consulting fees that attempt to reduce business risk and liability. Redress, identity protection services and free or discounted products are also included in this cost category.

- **Certain organisational factors decrease the overall cost.** If the organisation has a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as $5 per compromised record. In addition, a strong security posture and the appointment of a CISO saved as much as $10 and $7 per compromised record, respectively. Finally engaging outside consultants to assist with the breach response also saved $3 per record.

- **Certain organisational factors increase the overall cost.** For example, data breaches caused by or occurring at a third-party organisation such as a vendor or business partner increased per capita cost by $12. Data breach incidents involving the loss or theft of data bearing devices increased data breach cost by as much as $8 per compromised record. Finally, quick notification of the data breach increased per capita cost by $5.
Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a ten-month period. Recruiting organisations for the 2012 study began in January 2012 and interviews were completed in December. In each of the 21 participating organisations, we spoke with IT, compliance and information security practitioners who are knowledgeable about their organisation’s data breach and the costs associated with resolving the breach. For privacy purposes we do not collect any organisation-specific information.

How do you calculate the cost of data breach?

To calculate the average cost of data breach, we collect both the direct and indirect expenses paid by the organisation. Direct expenses include engaging forensic experts, outsourced hotline support, free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates. For a detailed explanation about Ponemon Institute’s benchmark methodology, please see Part 4 of this report.

How does benchmark research differ from survey research? The unit of analysis in the Cost of Data Breach study is the organisation. In survey research, the unit of analysis is the individual. As discussed previously, we recruited 21 organisations to participate in this study.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as those involving millions of lost or stolen records?

The average cost of a data breach in our research does not apply to catastrophic breaches. Primarily because these are not typical of the breaches most organisations experience. In order to be representative of the population of Australian organisations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than 100,000 compromised records.

Are you tracking the same organisations each year?

Each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company’s industry, headcount, geographic footprint and size of data breach. Since starting this research in 2009, we have studied the data breach experiences of 78 Australian organisations.
Part 2. Key Findings

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

- Cost of data breach per record and organisation
- Cost of data breach by industry
- Root cause of data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following cost components: detection and escalation, notification, lost business, direct and indirect and post data breach
- Preventive measures taken after the breach
- Percentage changes in cost categories

The cost of data breach increases. Figure 1 reports the average per capita cost of data breach.\(^3\) For four consecutive years the average per capita cost increased. According to this year’s benchmark findings, data breaches cost companies an average of $141 per compromised record – of which $81 pertains to indirect costs including abnormal turnover or churn of customers and $60 are direct costs incurred to resolve the data breach. Last year’s average per capita cost was $138 with an average indirect cost of $82.

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

\(^3\)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 cost of data breach over four years as shown in Figure 2 has trended upward. The total cost of data breach increased from $2.16 million in 2011 to $2.72 million in 2012.

Figure 2. The average total organisational cost of data breach over four years
$000,000 omitted

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009 (16)</td>
<td>$1.97</td>
</tr>
<tr>
<td>2010 (19)</td>
<td>$2.00</td>
</tr>
<tr>
<td>2011 (22)</td>
<td>$2.16</td>
</tr>
<tr>
<td>2012 (21)</td>
<td>$2.72</td>
</tr>
</tbody>
</table>

Key cost of data breach measures. Both the average per capita and organisational cost of data breach increased. Figure 3 reports four key metrics that show mixed results. The average total data breach cost increased by 23 percent over the past year. The 16 percent decrease in abnormal churn rate suggests organisations are more successful in retaining the loyalty of consumers and customers. In the context of this paper, 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 2012 and 2011 results

<table>
<thead>
<tr>
<th>Metric</th>
<th>Net Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average total cost</td>
<td>23%</td>
</tr>
<tr>
<td>Average size of data breach</td>
<td>6%</td>
</tr>
<tr>
<td>Per capita cost</td>
<td>2%</td>
</tr>
<tr>
<td>Abnormal churn</td>
<td>-16%</td>
</tr>
</tbody>
</table>
Certain industries have higher data breach costs. Figure 4 reports the per capita costs for the 2012 study by industry classification. While a small sample size prevents us from generalising industry cost differences, the pattern of 2012 industry results is consistent with prior years. Accordingly, financial, industrial and service companies tend to have a per capita cost higher than the mean, while companies in retail, public sector and hospitality have a per capita cost significantly below the mean.

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

- Financial: $234
- Industrial: $166
- Services: $154
- Communications: $154
- Energy: $153
- Consumer: $119
- Technology: $111
- Hospitality: $100
- Public sector: $100
- Retail: $97
Malicious or criminal attacks are the primary root causes of a data breach. Figure 5 provides a summary of the main root causes of a data breach for all 21 organisations. Forty-three percent experienced a malicious or criminal attack. Thirty-three percent of incidents involved a negligent employee or contractor (human factor), and another 24 percent involved system glitches, including a combination of both IT and business process failures.

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

Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically caused the data breach as determined by the post data breach investigation. Figure 6 reports the average per capita cost of data breach for three conditions or root causes of the incident. The pattern of results in 2012 is consistent with previous results. Companies that experienced data misuse or theft (exfiltration) had the highest per capita cost ($159). Companies that experienced system glitches had an average per capita cost at $131. Employee or contractor negligence resulted in a per capita cost of $125.

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

---

4 Malicious and criminal attacks increased slightly from 36 percent in our 2011 study. The most common types of attacks include malware infections, criminal insiders, phishing scams and SQL injection.

5 Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation.
Seven factors that influence the cost of data breach. We identified seven factors that influence the cost consequences of a data breach incident. These attributes are as follows:

- **The company had an incident management plan.** Forty-three percent of organisations in our benchmark sample had a data breach incident management plan in place at the time of the data breach event.

- **The company had a relatively strong security posture at the time of the incident.** Forty-three percent of organisations had a security effectiveness score (SES) at or above the normative average. We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process.\(^6\)

- **CISO (or equivalent title) has overall responsibility for enterprise data protection.** Thirty-eight percent of organisations have centralised the management of data protection with the appointment of a C-level information security professional.

- **Data was lost due to third party error.** Thirty-three percent of organisations had a data breach caused by a third party, such as vendors, outsourcers and business partners.

- **The company notified data breach victims quickly.** Thirty-three percent of organisations notified data breach victims within 30 days after the discovery of data loss or theft.

- **The data breach involved lost or stolen devices.** Twenty-nine percent of organisations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.

- **Consultants were engaged to help remediate the data breach.** Thirty-three percent of organisations hired consultants to assist in their data breach response and remediation.

As shown in Figure 7, incident response plans, a strong security posture, CISO appointments and consulting support decreased the per capita cost of data breach. However, third party errors, quick notification and lost or stolen devices increased the per capita cost of data breach. Hence, a strong security posture reduced the average cost of data breach from $141 to $131 (decreased cost = $10). In contrast, a third party error increased the average cost to as much as $153 (increased cost = $12).

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

<table>
<thead>
<tr>
<th>Factor</th>
<th>Cost Impact  \</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party error</td>
<td>$12</td>
<td></td>
</tr>
<tr>
<td>Lost or stolen devices</td>
<td>$8</td>
<td></td>
</tr>
<tr>
<td>Quick notification</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td>Consultants engaged</td>
<td>$(3)</td>
<td></td>
</tr>
<tr>
<td>Incident response plan</td>
<td>$(5)</td>
<td></td>
</tr>
<tr>
<td>CISO appointment</td>
<td>$(7)</td>
<td></td>
</tr>
<tr>
<td>Strong security posture</td>
<td>$(10)</td>
<td></td>
</tr>
</tbody>
</table>

\(^6\)The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.
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 21 benchmarked companies in ascending order by the size of the incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year’s study, the cost ranged from $.92 to $8.39 million.

**Figure 8. Total cost of data breach by size of the data breach**
Regression = Intercept + (Size of Breach Event) x \( \beta \), where \( \beta \) denotes the slope.

The more churn, the higher the per capita cost of data breach. Figure 9 reports the distribution of per capita data breach costs in ascending rate of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn and per capita costs are linearly related. This pattern of results is consistent with benchmark studies completed in prior years.

**Figure 9. Distribution of abnormal churn rates in ascending order by per capita costs**
Regression = Intercept + (abnormal churn rate) x \( \beta \), where \( \beta \) denotes the slope.
Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate of benchmarked organisations for the present study. While a small sample size prevents us from generalising the affect of industry on churn rates, our 2012 industry results are consistent with prior years – wherein financial and service organisations experienced relatively high abnormal churn and public sector and retail companies experienced a relatively low abnormal churn. The implications are that industries with the highest churn rates could significantly reduce the cost 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

Public sector organisations utilize a different churn framework given that customers of government organisations typically do not have an alternative choice.
**Detection and escalation costs increase.** Figure 11 shows the distribution of costs associated with detection and escalation of the data breach event. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and boards of directors. As noted, average detection and escalation costs significantly increased from $0.77 million in 2011 to $1.40 million in the present study.

**Figure 11. Average detection and escalation costs over four years**

$000,000 omitted

![](image1)

**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 increased slightly from $0.076 million in 2011 to $0.088 million in 2012.

**Figure 12. Average notification costs over four years**

$000,000 omitted

![](image2)
**Post data breach cost has 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. Average ex-post response cost increased from $.47 million in 2011 to a four-year high of $.81 million in 2012.

**Figure 13. Average ex-post response costs over four years**

$000,000 omitted

Lost business costs decreased sharply. Figure 14 reports lost business costs associated with data breach incidents over four years. The cost category typically includes the turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs decreased from $.84 million in 2011 to $.78 million in 2012.

**Figure 14. Average lost business costs over four years**

$000,000 omitted
**Indirect decreased and 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 per compromised record actually decreased by $1 – from $82 in 2011 to $81 in 2012. In contrast, the direct per capita cost of data breach increased from $56 in 2011 to $60 in 2012.

**Figure 15. Direct and indirect per capita data breach cost over four years**
Preventive measures taken after the breach

In addition to measuring specific cost activities relating to the leakage of personal information, we report in Table 1 the preventive measures taken after the data breach. The most popular steps are: the expanded use of encryption (48 percent), additional manual controls (46 percent), training and awareness programs (40 percent) and the strengthening of perimeter controls (35 percent).

In this year’s study, the use of certain measures and controls changed significantly. The adoption of endpoint security solutions and data loss prevention (DLP) solutions had the greatest increase (6 percent). Security intelligence solutions rose in adoption by 5 percent.

<table>
<thead>
<tr>
<th>Table 1. Preventive measures and controls implemented after the data breach incident</th>
<th>FY 2009</th>
<th>FY 2010</th>
<th>FY 2011</th>
<th>FY 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded use of encryption</td>
<td>40%</td>
<td>43%</td>
<td>46%</td>
<td>48%</td>
</tr>
<tr>
<td>Additional manual procedures and controls</td>
<td>56%</td>
<td>55%</td>
<td>47%</td>
<td>46%</td>
</tr>
<tr>
<td>Training and awareness programs</td>
<td>52%</td>
<td>46%</td>
<td>44%</td>
<td>40%</td>
</tr>
<tr>
<td>Strengthening of perimeter controls</td>
<td>27%</td>
<td>30%</td>
<td>33%</td>
<td>35%</td>
</tr>
<tr>
<td>Identity and access management solutions</td>
<td>23%</td>
<td>19%</td>
<td>23%</td>
<td>27%</td>
</tr>
<tr>
<td>Other system control practices</td>
<td>24%</td>
<td>21%</td>
<td>25%</td>
<td>26%</td>
</tr>
<tr>
<td>Endpoint security solutions</td>
<td>10%</td>
<td>16%</td>
<td>19%</td>
<td>25%</td>
</tr>
<tr>
<td>Security intelligence solutions</td>
<td>11%</td>
<td>15%</td>
<td>18%</td>
<td>23%</td>
</tr>
<tr>
<td>Data loss prevention (DLP) solutions</td>
<td>15%</td>
<td>16%</td>
<td>15%</td>
<td>21%</td>
</tr>
<tr>
<td>Security certification or audit</td>
<td>13%</td>
<td>12%</td>
<td>10%</td>
<td>18%</td>
</tr>
</tbody>
</table>

*Please note that a company may be implementing more than one preventive measure.*
Cost changes of data breach categories over time

Since first conducting this research there have been minimum shifts in spending on data breaches. The most significant changes are investments in investigation and forensics followed by legal costs incurred to defend against regulatory actions.

Table 2 provides the percentage changes for 11 cost categories over four years. The two highest cost categories pertain to investigation and forensics and lost customer business.

<table>
<thead>
<tr>
<th>Table 2. Cost changes over four years</th>
<th>FY 2009</th>
<th>FY 2010</th>
<th>FY 2011</th>
<th>FY 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations &amp; forensics</td>
<td>26%</td>
<td>27%</td>
<td>28%</td>
<td>32%</td>
</tr>
<tr>
<td>Audit and consulting services</td>
<td>11%</td>
<td>10%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Outbound contact costs</td>
<td>10%</td>
<td>12%</td>
<td>12%</td>
<td>11%</td>
</tr>
<tr>
<td>Inbound contact costs</td>
<td>9%</td>
<td>8%</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>Public relations/communications</td>
<td>3%</td>
<td>3%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Legal services - defence</td>
<td>4%</td>
<td>3%</td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td>Legal services - compliance</td>
<td>6%</td>
<td>5%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Free or discounted services</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Identity protection services</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Lost customer business</td>
<td>22%</td>
<td>22%</td>
<td>22%</td>
<td>20%</td>
</tr>
<tr>
<td>Customer acquisition cost</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Part 3. Concluding observations and description about participating companies

Companies participating in our annual study continue to report an increase in both the average total cost and per capita cost of data breach. The most profitable investments as evidenced by the lower cost of a data breach are establishing a strong security posture, incident response planning, engaging external consultants, and appointing a CISO with enterprise-wide responsibility.

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

In this report, we compare the results of the present study to those from prior years. It is important to note that each annual study involves a different sample of companies. In other words, we are not tracking the same sample of companies over time. To be consistent, we attempt to recruit and match companies with similar characteristics such as the company’s industry, headcount, geographic footprint and size of data breach.

Figure 16 shows the distribution of benchmark organisations by their primary industry classification. In this year’s study, 10 industries are represented. Consumer, financial services, public sector (government), and retail represent the four largest segments.

**Figure 16. Distribution of the benchmark sample by industry segment**
Part 4. How we calculate the cost of a data breach

Our study addresses core process-related activities that drive a range of expenditures associated with an organisation’s data breach detection, response, containment and remediation. The four cost centres are:

- **Detection or discovery**: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.

- **Escalation**: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.

- **Notification**: Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.

- **Ex-poste response**: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms. Redress activities also include ex-poste response such as credit report monitoring or the reissuing of a new account (or credit card).

In addition to the above process-related activities, most companies experience opportunity costs associated with the breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our Institute’s research shows that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover or churn rates as well as a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we use a cost estimation method that relies on the “lifetime value” of an average customer as defined for each participating organisation.

- **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.\(^8\)

- **Diminished customer acquisition**: The estimated number of target customers who will not have a relationship with the organisation 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 organisation’s churn or turnover.\(^9\) 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).

All participating organisations 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

---

\(^8\)In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organisation, 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.

\(^9\)In this study, we consider citizen, patient and student information as customer data.
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.\(^\text{10}\)

Data collection methods did not include actual accounting information, but instead relied upon a numerical estimation based upon 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, labour 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.

\[
\begin{array}{c}
\text{LL} \\
\rule{8cm}{0.5mm} \\
\text{UL}
\end{array}
\]

Post your estimate of direct costs here for [presented cost category]

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

The scope of data breach cost items contained within our benchmark instrument is limited to known cost categories that are applied to a broad set of business operations that handle personal information. We believe a study focused on business process – and not data protection or privacy compliance activities – yields a better quality of results.

\(^{10}\)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.
Figure 17 illustrates the activity-based costing schema used in our benchmark study. The cost centres we examine sequentially are: incident discovery, escalation, notification, ex-poste response and lost business.

**Figure 17: Schema of the data breach process**

![Diagram of the data breach process]

- **Before disclosure or notification of the incident**
  - Incident discovery
  - Escalation

- **After disclosure**
  - Notification
  - Ex-poste response
  - Lost business opportunities

**Examples of discovery and escalation activities:**
- Investigating the incident to determine the root causes of the data breach.
- Determining the data breach population (a.k.a. probable victims).
- Organising the incident response team.
- Orchestrating communication and public relation plans.
- Preparing notice documents and other required disclosures to data breach victims and regulators.
- Implementing call centre procedures and specialised training.

Within each cost centre, the research instrument required subjects to estimate a cost range to capture estimates of direct cost, indirect cost and opportunity cost, defined as follows:

- **Direct cost** – the direct expense outlay to accomplish a given activity.
- **Indirect cost** – the amount of time, effort and other organisational resources spent, but not as a direct cash outlay.
- **Opportunity cost** – the cost resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been reported to victims (and publicly revealed to the media).

To maintain complete confidentiality, the benchmark instrument did not capture any company-specific information. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

To keep the benchmarking process to a manageable size, we carefully limited items to only those cost activity centres 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.
Limitations

Our study utilises 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 Australian-based entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

- **Non-response**: The current findings are based on a small representative sample of benchmarks. Twenty-one companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.

- **Sampling-frame bias**: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

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

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

- **Extrapolated cost results**: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.
### Appendix 1: Cost for 21 Data Breach Case Studies

<table>
<thead>
<tr>
<th>Cases</th>
<th>Size of breach</th>
<th>Detection &amp; escalation*</th>
<th>Notification*</th>
<th>Ex-post response*</th>
<th>Lost business*</th>
<th>Total*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13,573</td>
<td>514,744</td>
<td>28,563</td>
<td>111,364</td>
<td>261,766</td>
<td>916,437</td>
</tr>
<tr>
<td>2</td>
<td>30,420</td>
<td>987,114</td>
<td>46,334</td>
<td>821,039</td>
<td>562,594</td>
<td>2,417,081</td>
</tr>
<tr>
<td>3</td>
<td>17,237</td>
<td>870,780</td>
<td>60,763</td>
<td>657,817</td>
<td>5,566</td>
<td>1,594,926</td>
</tr>
<tr>
<td>4</td>
<td>19,371</td>
<td>938,537</td>
<td>74,950</td>
<td>436,647</td>
<td>393,860</td>
<td>1,843,994</td>
</tr>
<tr>
<td>5</td>
<td>18,098</td>
<td>700,320</td>
<td>586,164</td>
<td>517,017</td>
<td>6,553</td>
<td>1,810,054</td>
</tr>
<tr>
<td>6</td>
<td>17,336</td>
<td>568,310</td>
<td>76,026</td>
<td>521,004</td>
<td>575,357</td>
<td>1,740,697</td>
</tr>
<tr>
<td>7</td>
<td>10,808</td>
<td>529,112</td>
<td>41,396</td>
<td>595,259</td>
<td>7,496</td>
<td>1,173,263</td>
</tr>
<tr>
<td>8</td>
<td>19,544</td>
<td>1,582,989</td>
<td>92,643</td>
<td>367,521</td>
<td>129,355</td>
<td>2,172,508</td>
</tr>
<tr>
<td>9</td>
<td>28,637</td>
<td>1,645,293</td>
<td>17,304</td>
<td>868,966</td>
<td>816,041</td>
<td>3,347,604</td>
</tr>
<tr>
<td>10</td>
<td>39,382</td>
<td>1,084,237</td>
<td>33,453</td>
<td>2,087,218</td>
<td>2,125,933</td>
<td>5,330,841</td>
</tr>
<tr>
<td>11</td>
<td>60,071</td>
<td>3,309,616</td>
<td>231,483</td>
<td>2,870,873</td>
<td>1,978,634</td>
<td>8,390,606</td>
</tr>
<tr>
<td>12</td>
<td>12,676</td>
<td>739,628</td>
<td>69,292</td>
<td>501,452</td>
<td>551,699</td>
<td>1,862,071</td>
</tr>
<tr>
<td>13</td>
<td>20,315</td>
<td>1,229,874</td>
<td>9,213</td>
<td>608,905</td>
<td>1,261,394</td>
<td>3,109,386</td>
</tr>
<tr>
<td>14</td>
<td>15,218</td>
<td>1,184,337</td>
<td>30,751</td>
<td>511,248</td>
<td>605,834</td>
<td>2,332,170</td>
</tr>
<tr>
<td>15</td>
<td>13,619</td>
<td>791,247</td>
<td>89,572</td>
<td>360,592</td>
<td>852,397</td>
<td>2,093,808</td>
</tr>
<tr>
<td>16</td>
<td>12,228</td>
<td>874,976</td>
<td>110,796</td>
<td>259,835</td>
<td>665,476</td>
<td>1,911,083</td>
</tr>
<tr>
<td>17</td>
<td>32,558</td>
<td>1,143,386</td>
<td>159,207</td>
<td>1,982,061</td>
<td>1,895,324</td>
<td>5,179,978</td>
</tr>
<tr>
<td>18</td>
<td>16,184</td>
<td>1,293,715</td>
<td>30,368</td>
<td>914,657</td>
<td>348,939</td>
<td>2,587,679</td>
</tr>
<tr>
<td>19</td>
<td>5,707</td>
<td>253,595</td>
<td>31,954</td>
<td>223,082</td>
<td>587,492</td>
<td>1,096,123</td>
</tr>
<tr>
<td>20</td>
<td>8,454</td>
<td>848,428</td>
<td>12,169</td>
<td>317,718</td>
<td>811,311</td>
<td>1,989,626</td>
</tr>
<tr>
<td>21</td>
<td>13,855</td>
<td>791,757</td>
<td>30,205</td>
<td>1,549,267</td>
<td>1,878,772</td>
<td>4,250,001</td>
</tr>
</tbody>
</table>

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

Ponemon Institute LLC
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

As a member of the Council of American Survey Research Organisations (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.