Final Document

Sponsored by

Symantec

2011 Cost of Data Breach Study: Australia

Benchmark Research Conducted by

Ponemon Institute LLC

Report: March 2012

2011 Cost of Data Breach Study: Australia

Ponemon Institute, March 2012

Part 1. Executive Summary

Symantec Corporation and the Ponemon Institute are pleased to present *2011 Cost of Data Breach: Australia*, our third annual benchmark study concerning the cost of data breach incidents for Australian-based companies. For organisations in Australia, the cost of a data breach continues to rise. In 2011 the cost of one compromised record increased from AUD $128 to $138.

Australia is unique among the countries covered in our annual research. As yet there are no data breach notification regulations. Australian privacy laws are contained in a variety of Commonwealth, State and Territory Acts. In June 2010, the Australian Government released the exposure draft of legislation containing proposed Australian Privacy Principles (APPs), which will eventually unify all Australian data privacy regulations and include data breach notification. Additionally, in November 2010, the new Office of the Australian Information Commissioner absorbed the Office of the Privacy Commissioner (OPC), the office responsible for best practices in handling personal identifiable information (PII) in Australia.

Our current analysis of the actual data breach experiences of 22 Australian companies from 10 different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response. We also analyse the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn rates.

Ponemon Institute conducted its first *Cost of a Data Breach* study in the United States seven years ago. Since then, we have expanded the study to include France, Germany, the United Kingdom and Australia. This year we are conducting the first *Cost of Data Breach* studies in Italy, India and Japan. The initial study established objective methods for quantifying specific activities that result in direct, indirect and opportunity costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law. To maintain consistency from prior years, our methods for quantifying data breach costs has remained relatively constant.

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

- **The cost of data breach has steadily increased**. For the third consecutive year, the cost per lost or stolen record and the total organisational cost increased. In 2010, the cost was $128 and increased $10 to $138. We define a record as information that identifies an individual whose personal information has been compromised in a data breach.

  The average total organisational cost of data breach increased from $2 million in 2010 to $2.16 million in 2011. This increase suggests the need for organisations to improve their ability to respond to the breach.

- **Fewer customers are abandoning the organisation following the data breach**. Although only a slight decrease in average churn rates, fewer customers are leaving organisations following a data breach. The average abnormal churn decreased from 3.5 percent in 2010 to 3.4 percent this year. However, certain industries, such as technology and communications companies, are more susceptible to customer churn, which causes their data breach costs to be higher than other industries. Taking steps 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**. Thirty-six percent of organisations say the root cause was malicious or criminal attacks. This

decreased slightly from 37 percent in 2010. This type of breach is also the most costly. Thirty-two percent of breaches involved negligent employees or contractors and 32 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. Organisations should also continue to look into addressing both internal risks arising from negligent personnel and system glitches as combined these sum up to 64 percent of root causes.

- **Lost business costs increased sharply.** This is the highest reported since first studying data breach costs in 2009. 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.

- **Certain organisational factors reduce the overall cost**. If the organisation has a CISO with overall responsibility for enterprise data protection the average cost of a data breach can be reduced as much as $35 per compromised record. If the organisation engages outside consultants to assist with the breach response, it can save on average $45 per record. A CISO with overall responsibility for enterprise data protection can result in a reduction of as much as $35 per compromised record. Quick response (less than 30 days) can save Australian organisations $30 per record. When considering the average number of records lost or stolen, these factors can provide significant and positive financial benefits.

  Certain attributes or factors of the data breach also can increase the overall cost. Specifically, having a data breach caused by a third party mistake can cost an average of $49 more per compromised record, losing a laptop or other mobile device can increase the cost an average of $36 or having a data breach for the first time adds an additional $2 per record.

- **Detection and escalation costs increased slightly.** Detection and escalation costs increased from approximately $730,000in 2010 to $770,000 this year. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion. This increase suggests that organisations should assess what processes and technologies are needed to improve their ability to detect and investigate data breaches.

- **Notification costs increased slightly.** Notification refers to the steps taken to report the breach of protected information to appropriate personnel within a given time period following the incident. As mentioned, Australian organisations at present are not required to notify victims.[1] The costs to notify victims of the breach increased in this year's study from approximately $76,000 to $77,000.

[1] 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. See: Michael Lee's article, "Australia divided over data breach laws" in

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a nine-month period. Recruiting organisations for the 2011 study began in January 2011 and interviews were completed in December. In each of the 22 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 22 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 the ones experienced by Sony or Epsilon?

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 57 Australian organisations.

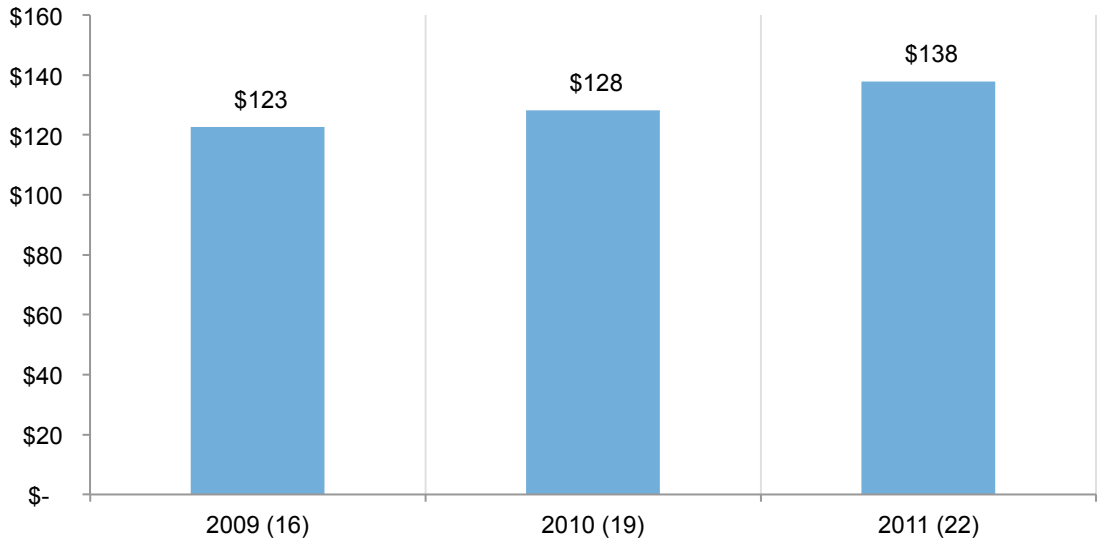
Part 2. Key Findings

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

- Cost of data breach: per record, organisational and industry
- Root causes of a data breach
- Attributes that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following costs: detection and escalation, notification, lost business, direct and indirect and post data breach

The per record and organisational cost of data breach continues to increase. Figure 1 reports the average per capita cost of data breach.[2] As can be seen, for three consecutive years the average per capita cost has increased. According to this year's benchmark findings, data breaches cost companies an average of $138 per compromised record – of which 60 percent pertains to indirect costs. This includes abnormal turnover or churn of existing and future customers. Last year's average per capita cost was $128, of which 59 percent was indirect cost.

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



[2]Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of compromised records.

The total average cost of data breach over three years as shown in Figure 2 is trending upward. The total cost of data breach increased from $2 million to $2.16 million.

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

Both per capita and average organisational cost of data breach increased. Figure 3 reports four key metrics that show mixed results. Both per capita cost and the average total data breach cost increased by 8 percent over the past year. The 3 percent decrease in abnormal churn rate suggests organisations are more successful in retaining the loyalty of consumers and customers. The average data breach size has declined slightly by 2 percent, suggesting fewer records are being lost or stolen.

Figure 3: Reasons for increase in cost of data breach
Net change defined as the difference between the 2011 and 2010 results

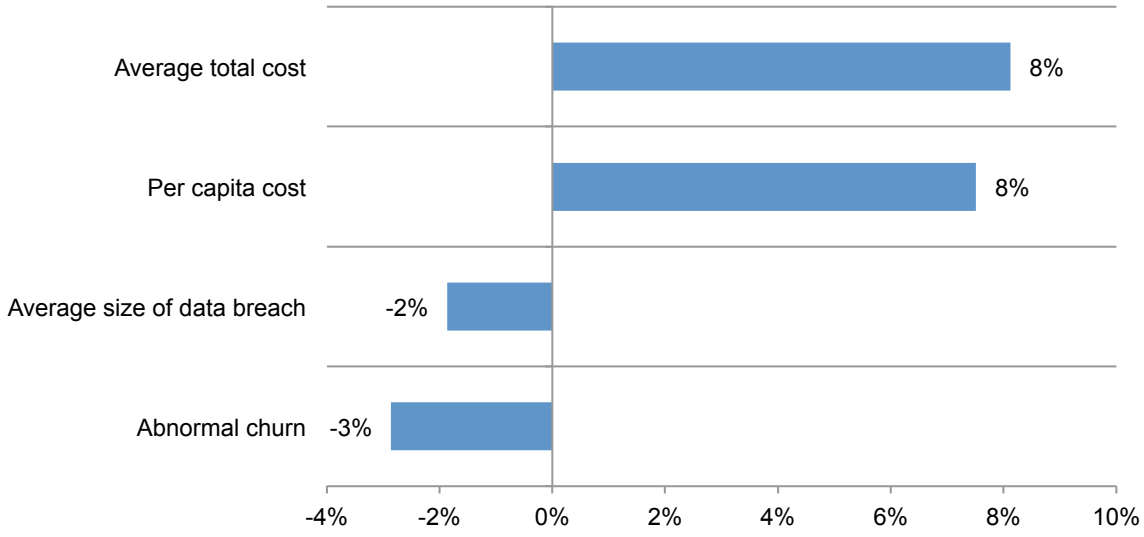
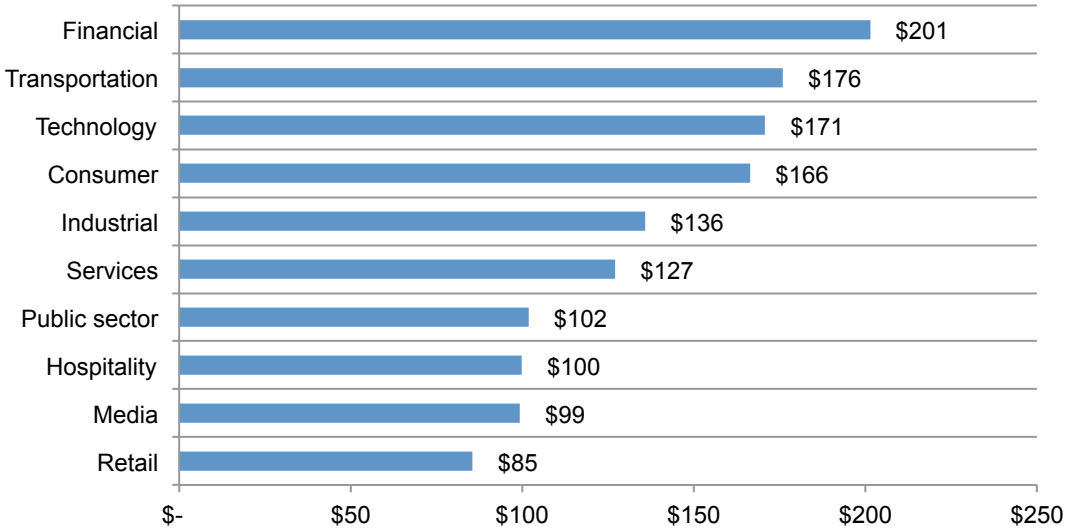


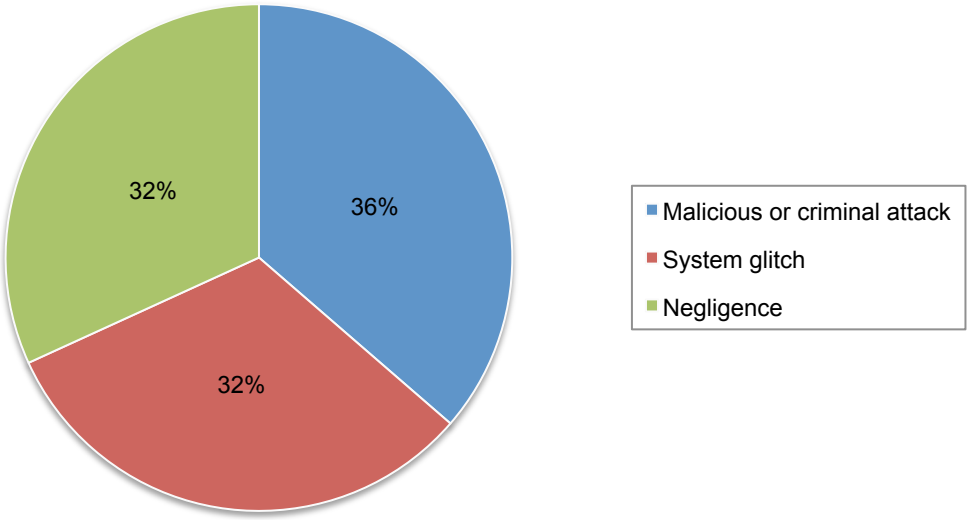
Figure 4 reports the per capita costs for the 2011 study by industry classification. While small sample size prevents us from generalizing industry cost differences, the pattern of 2011 industry results is consistent with prior years. Accordingly, financial companies tend to have a per capita cost higher than the men ($201) and retail companies have a per capita cost significantly below the mean ($85).

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



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 22 organisations. Thirty-six percent experienced a malicious or criminal attack. [3] Thirty-two percent of incidents involved a negligent employee or contractor, and another 32 percent involved system glitches, including a combination of both IT and business process failures.

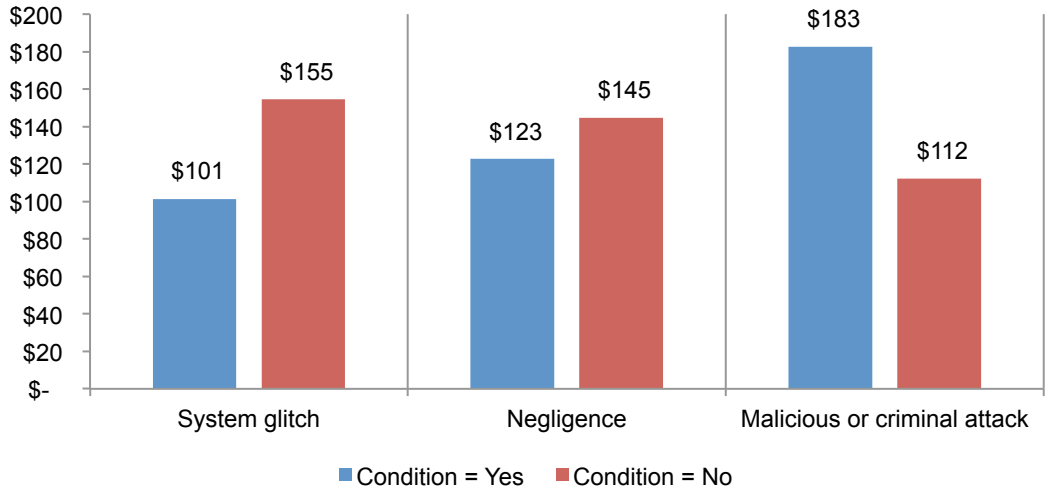
Figure 5. Distribution of the benchmark sample by root cause of the data breach



[3]Malicious and criminal attacks increased slightly from 38 percent in our 2010 study.

Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically cause the data breach as determined by the post data breach investigation. Figure 6 reports per capita cost of data breach for three conditions or root causes of the breach incident. Again, the pattern of results in 2011 is consistent with prior years, wherein the most costly breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experience malicious or criminal attacks have the highest per capita cost ($183), and companies experiencing system glitches have the lowest per capita cost ($101). Negligence results in a per capita cost of $123, which is below the overall mean of $138.

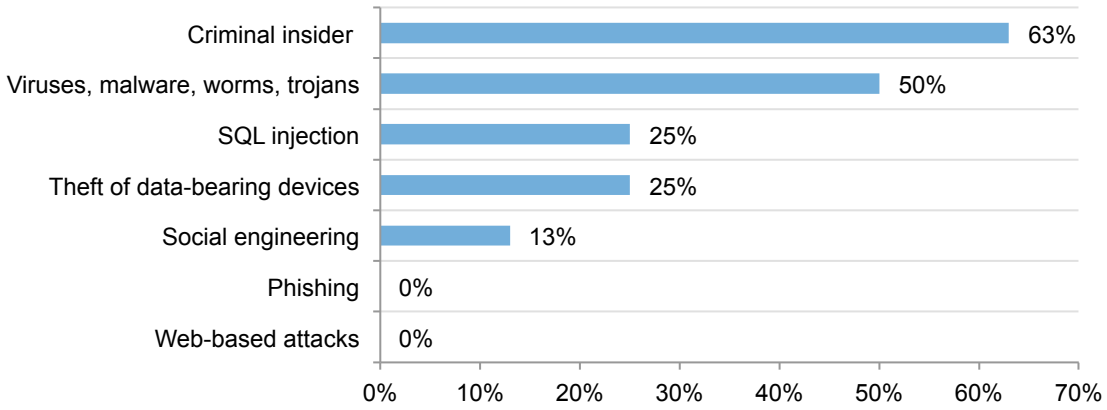
Figure 6. Per capita cost for three root causes of the data breach



Criminal attacks are mainly criminal insiders and electronic agents. In this year's report, we analysed the findings from the 8 organisations that report their data breach was caused by a malicious insider or hacker as previously described. Figure 7 summarises the types of criminal attacks experienced. Please note that a given company might have experienced two or more of these attacks.

The most salient attack condition pertains to criminal insiders (63 percent). Also half of this subsample experienced electronic agents such as viruses, malware, worms and trojans. The theft of data-bearing devices and SQL injection were experienced by 25 percent of this subsample

Figure 7. Analysis of malicious or criminal attacks experienced by 8 companies
More than one attack type may exist for each company



Six positive and negative attributes can influence the cost of a data breach. Over the years of conducting this research, we have identified six attributes that can influence the cost of a data breach. The percent of organisations in this study that have these attributes is shown in Figure 8.

- **First time the organisation had a data breach**. Fifty percent says the incident was their first data breach involving 1,000+ records.
- C**onsultant is engaged to help remediate the data breach**. As can be seen, 41 percent says their organisations engaged a consultant to assist in the data breach response or remediation.
- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Forty-one percent of participating organisations have centralized the management of data protection with the appointment of a C-level security professional.
- **The organisation notified data breach victims quickly**. Thirty-six percent says their organisations responded and provided notice about the data breach within 30 days of discovery.
- **Data was lost or stolen due to a third-party flub**. Thirty-six percent says their data breach involved one or more third parties – including outsourcers, cloud providers and business partners.
- **The data breach involved lost or stolen devices**. Thirty-two percent says the incident involved one or more lost or stolen data-bearing devices – which included laptops, smartphones, tablets and servers.

Figure 8. Defining attributes for the benchmark sample

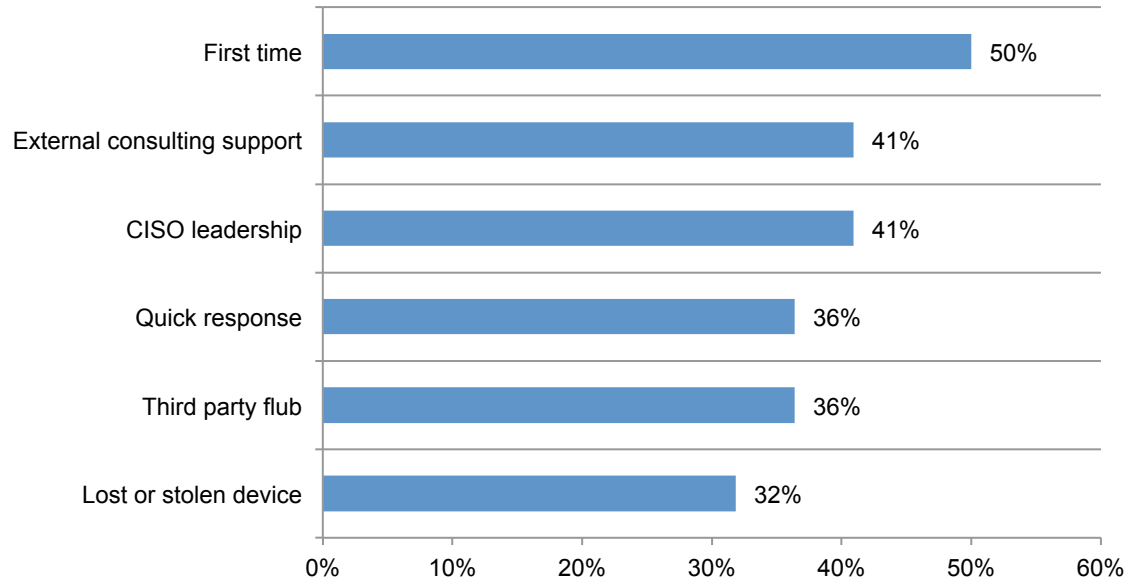


Figure 9 summarises the per capita costs for six normatively important conditions or attributes about the benchmark sample. As previously mentioned, these attributes were selected based on learned experiences from previous cost benchmark studies.

Per capita costs are above the mean for companies experiencing a major data breach involving third party mistakes ($169) or the loss or theft of a data-bearing device ($163). Per capita costs are below the mean for organisations that have engaged external consultants to assist in data breach investigation, have a CISO in-charge of data protection efforts or notify victims quickly.

Figure 9. Per capita cost for six attributes or conditions

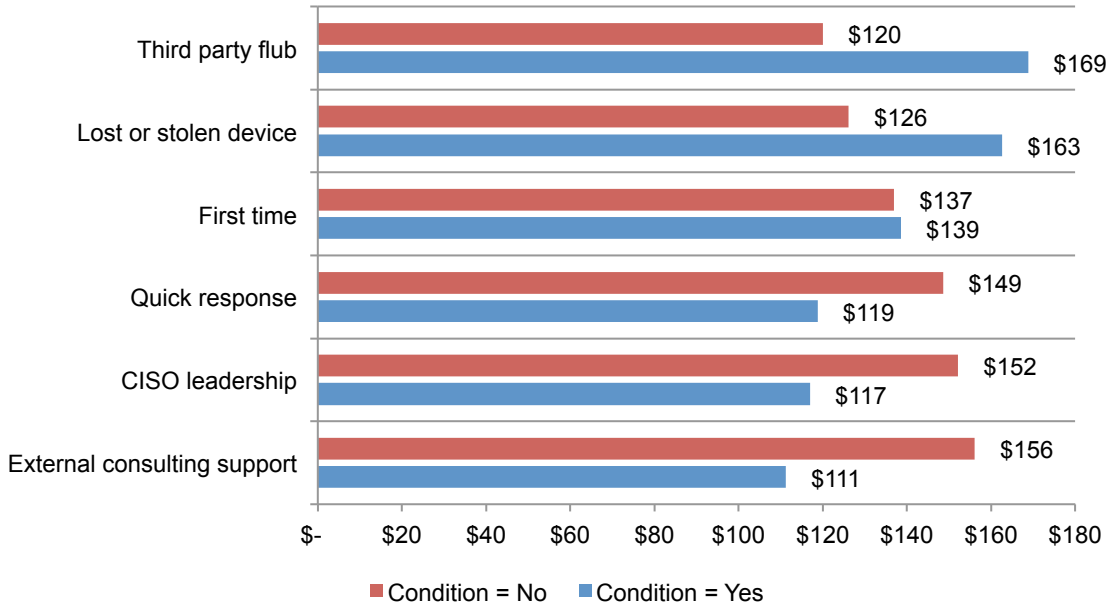
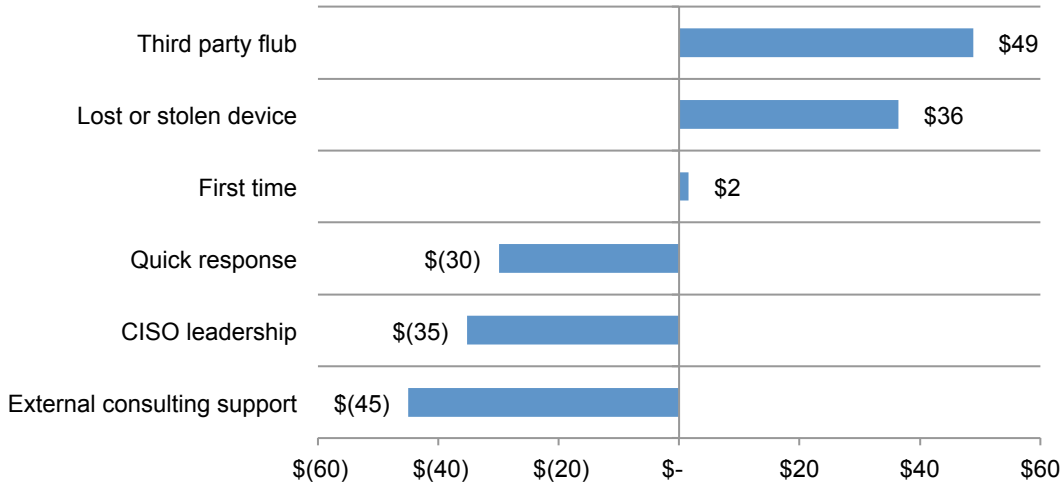


Figure 10 summarises the per capita cost differences for six normatively important conditions or attributes about the benchmark sample. In this analysis, a negative difference means that the attribute or condition moderates or lessens data breach costs. A positive difference has the opposite meaning.

Figure 10. Per capita cost differences for six attributes or conditions



As shown above, organisations engaging an external consultant enjoy a per capita cost saving of $45. In addition, organisations employing a CISO with enterprise-wide responsibility for data protection experience a $35 cost saving per compromised record. Finally, organisations that quickly notify experience a $30 average saving. The remaining three conditions have positive differences, thus suggesting an unfavorable impact on per capita cost.

The average number of records lost or stolen among organisations has not changed significantly. Figure 11 shows, in ascending order, the number of lost or stolen records involved in data breach incidents included in studies conducted over the past three years. According to the figure, the number of compromised records has remained relatively constant since 2009. The benchmark samples do not contain data breach incidents involving millions of compromised records. In our experience, these so-called "mega breaches" are rare events and including them would skew results. The largest data breach incident in this year's study involved 65,521 records.

Figure 11. Ascending frequency of compromised records over three years

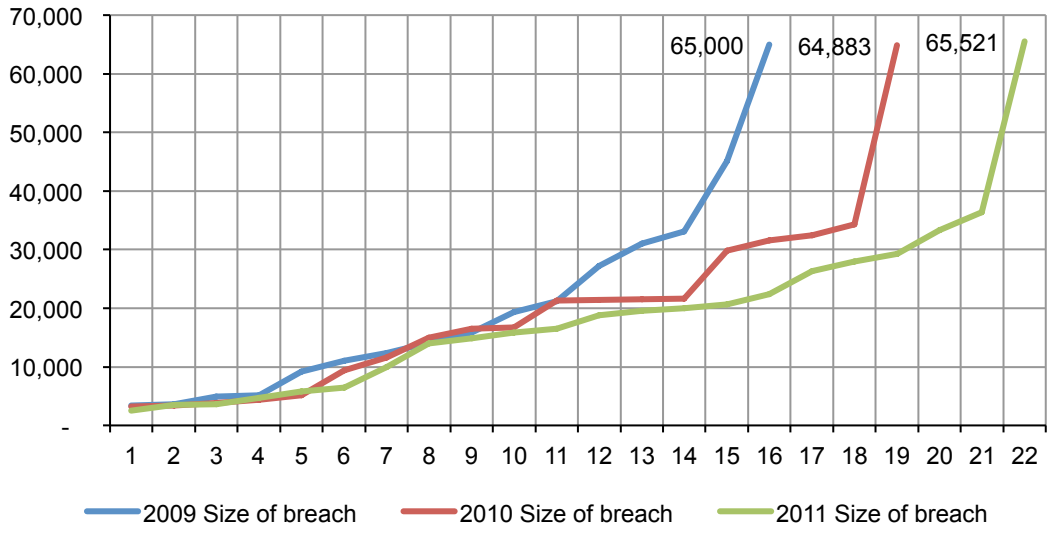
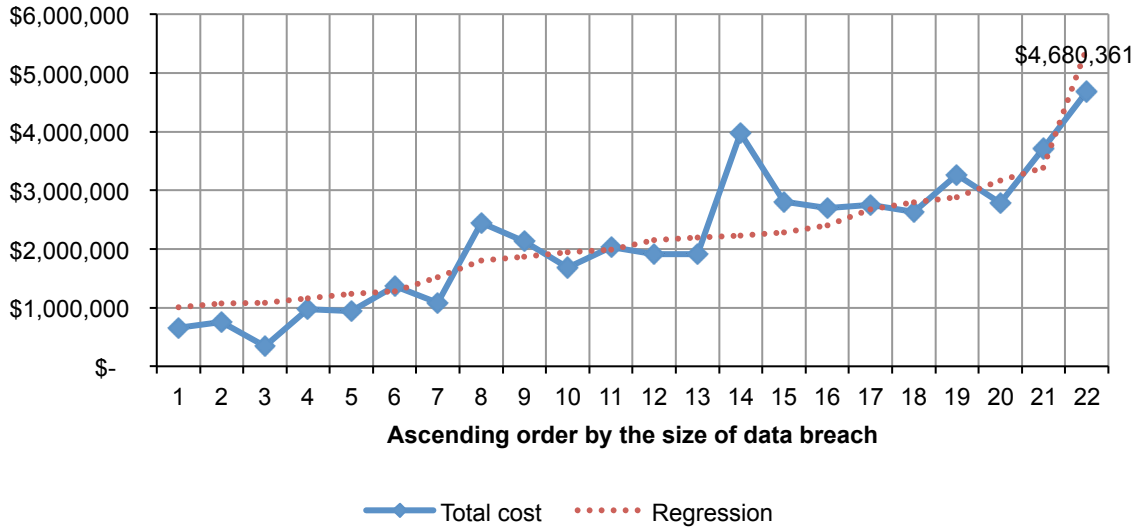


Figure 12 shows the relationship between the total cost of data breach and the size of the incident for 22 benchmarked companies in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year's study, the cost ranged from $342,849 to $4,680,361.

Figure 12. Total cost of data breach by size of lost or stolen records
Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope.



Fewer customers are leaving organisations following a data breach. Figure 13 shows the abnormal churn rates for each one of the 22 organisations included in this research. As shown, the churn rate distribution is varied, with a range of 0 (no abnormal churn) to 7.8 percent. It is important to note that the average abnormal churn decreased slightly from 3.5 percent in the 2010 study to 3.4 percent this year.

Figure 13. Distribution of abnormal churn rates for 22 benchmark companies

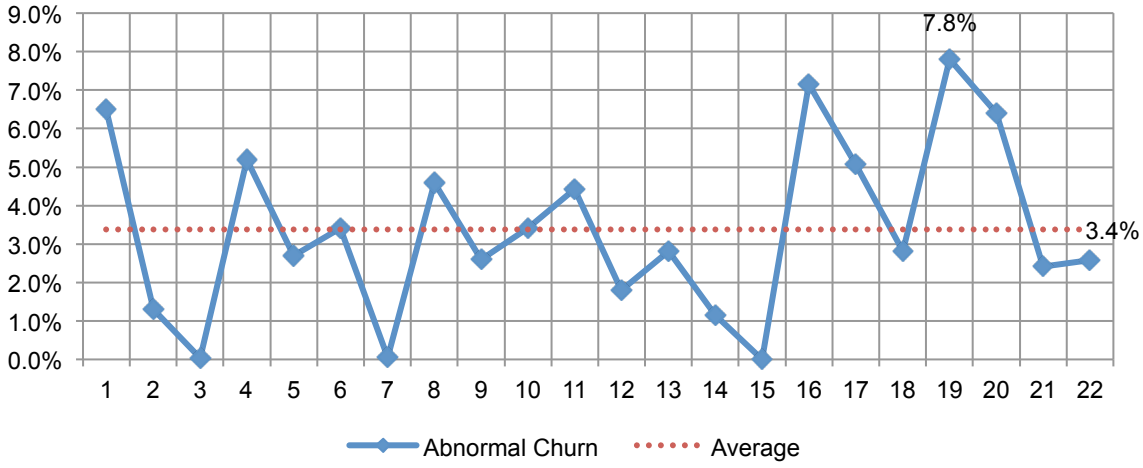
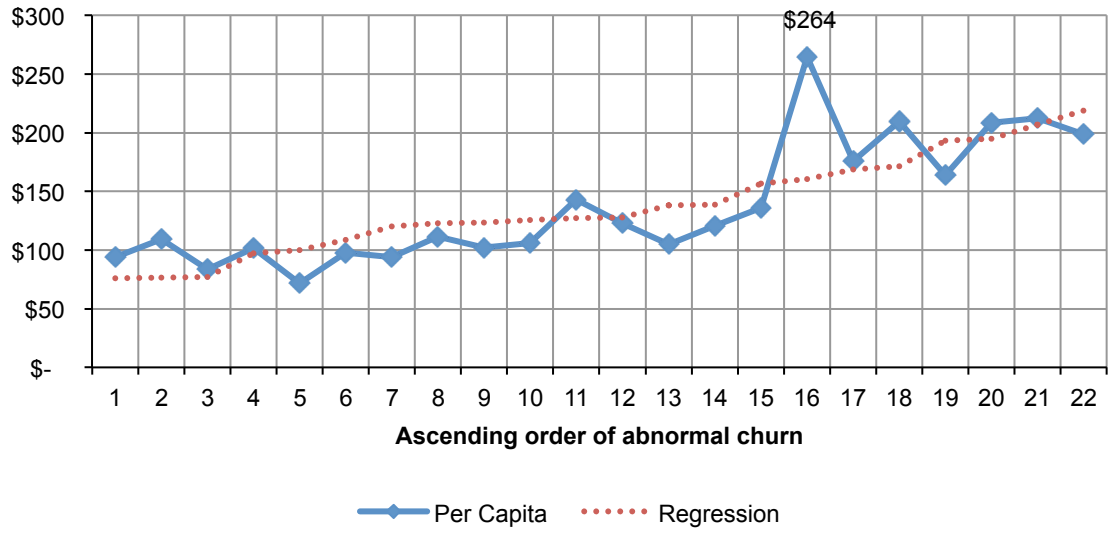


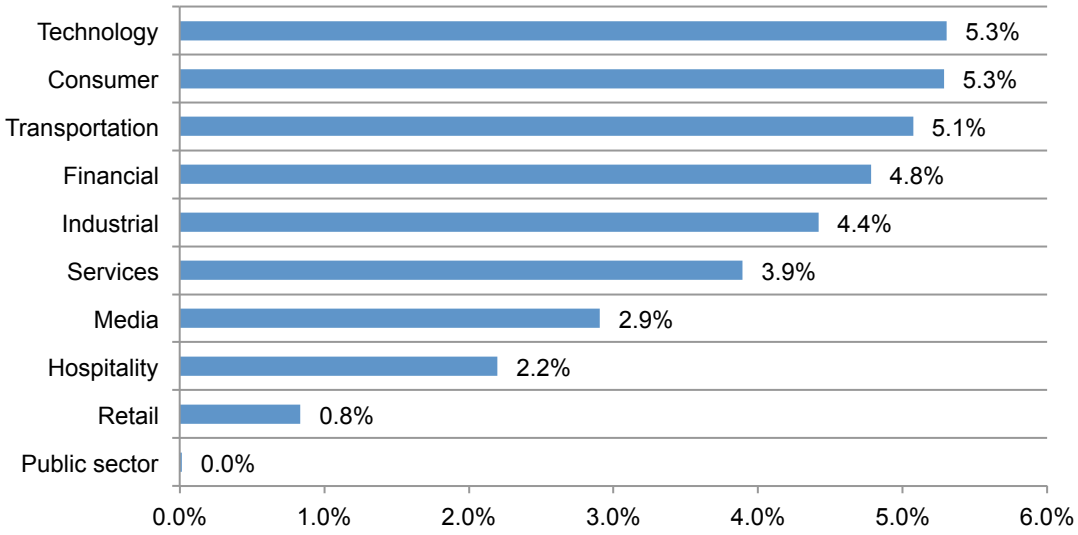
Figure 14 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 14. Distribution of per capita costs in ascending value of abnormal churn rates
Regression = Intercept + {Abnormal Churn} x β, where β denotes the slope.



Certain industries are more vulnerable to churn. Figure 15 reports the abnormal churn rate of benchmarked organisations for the 2011 study. While small sample size prevents us from generalizing the affect of industry on data breach cost, our 2011 industry results are consistent with prior years – wherein technology and consumer companies tend to experience relatively high abnormal churn and retail companies tend to experience a relatively low abnormal churn.[4] In this year's study, public service (government) organisations realise the lowest churn rates.

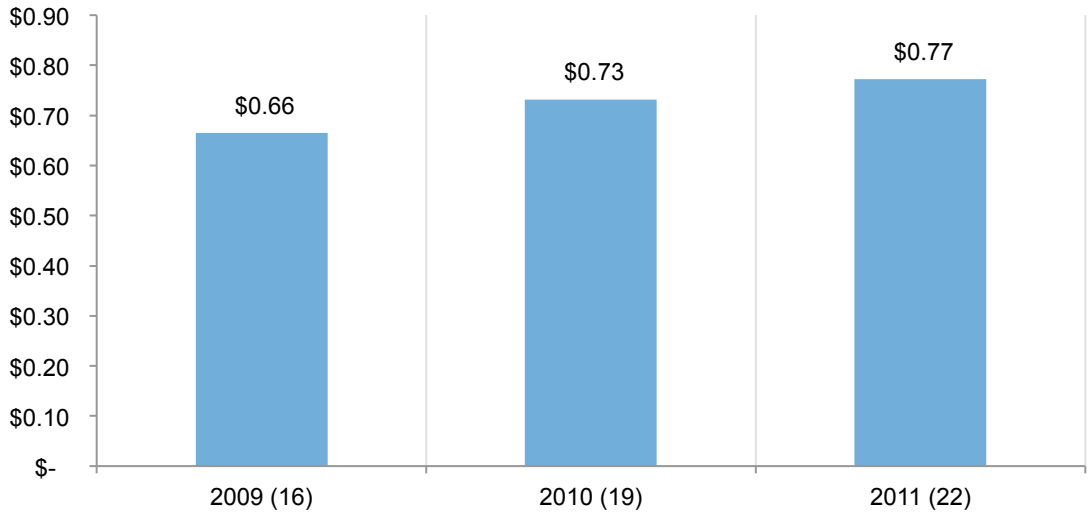
Figure 15. Abnormal churn rates by industry classification of benchmarked companies



[4]Public sector organisations utilise a different churn framework given that customers of government organisations typically do not have an alternative choice.

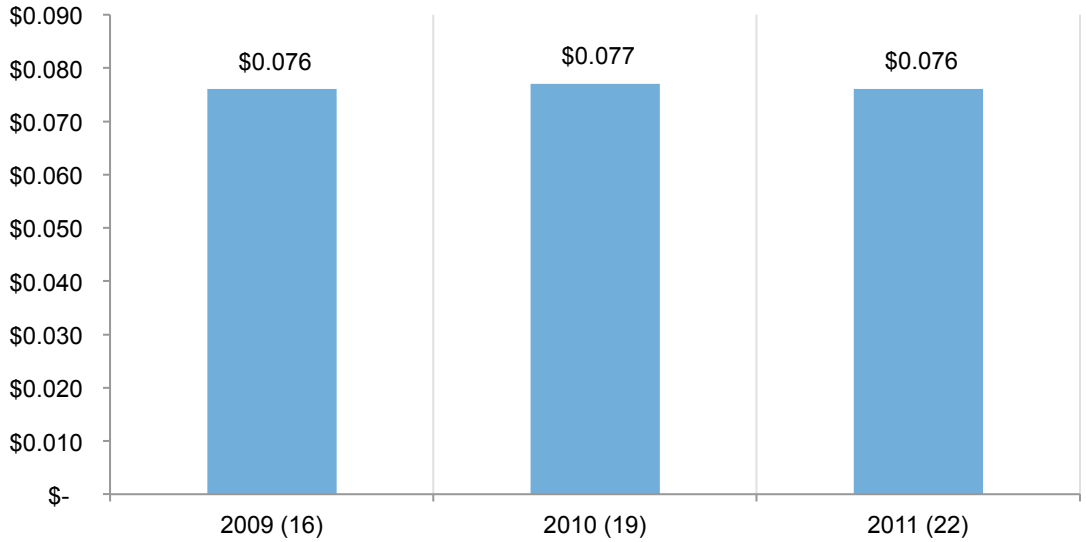
Detection and escalation costs increase. Figure 16 shows the distribution of costs associated with detection and escalation of the data breach event. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. As noted, average detection and escalation costs increased from $730,000 in 2010 to $770,000 in the present study.

Figure 16. Average detection and escalation costs over three years
$000,000 omitted



Notification costs decreased slightly. Figure 17 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 is $76,000, which is similar to notification costs in 2009. This represents only a slight decrease from $77,000 in 2010.

Figure 17. Average notification costs over three years
$000,000 omitted

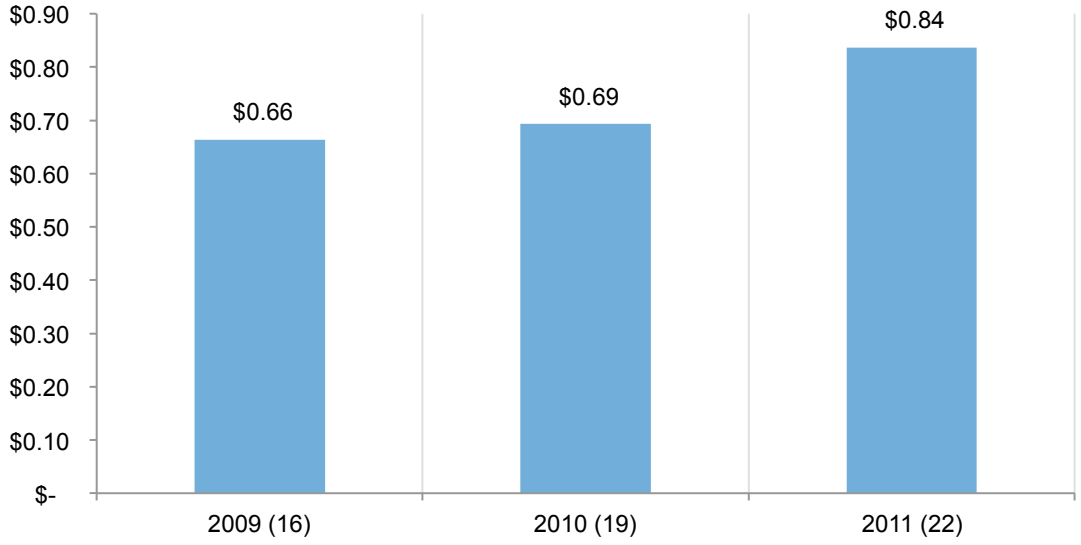


Post data breach costs have decreased steadily since 2009. Figure 18 shows the distribution of costs associated with ex-post (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost decreased from $500,000 in 2010 to a three-year low of $470,000 in this year's study.

Figure 18. Average ex-post response costs over three years
$000,000 omitted

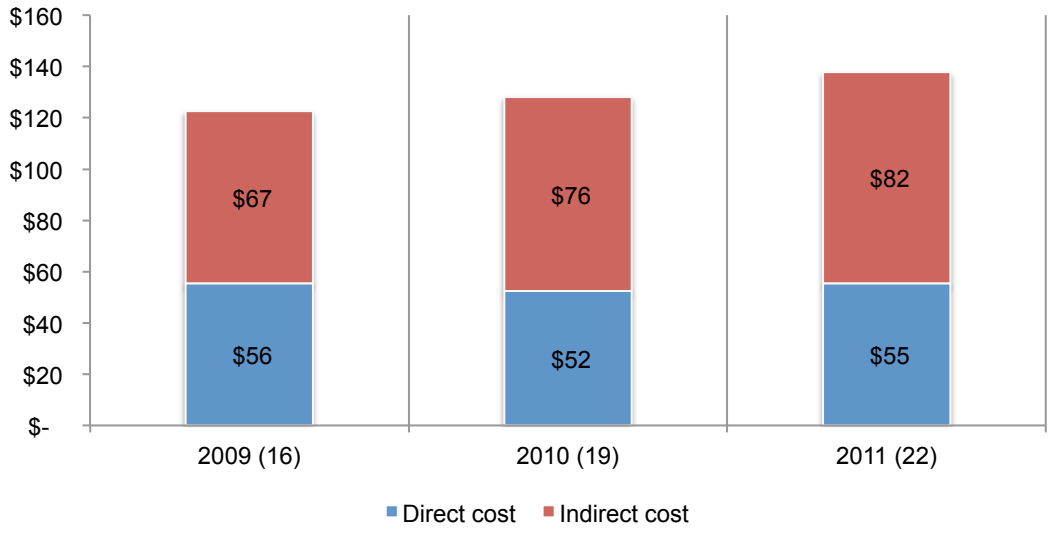
Lost business costs increased sharply. Figure 19 reports lost business costs associated with data breach incidents over three years, which again shows an increasing trend. The cost category typically includes the turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs increased from $690,000 in 2010 to $840,000 in 2011.

Figure 19. Average lost business costs over three years
$000,000 omitted



Indirect and direct costs increased significantly. Figure 20 reports the direct and indirect cost components of data breach on a per capita basis. In essence, the cost of data breach per compromised record increased by $10 – from $128 in 2010 to $138 in 2011. Approximately 40 percent are direct costs and indirect costs represent 60 percent of total per capita cost, which is approximately the same as in the 2010 study.

Figure 20. Direct and indirect per capita data breach cost over three years



We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process. [5] Figure 21 reports the SES Index for 22 organisations. The SES range of possible scores is +2 (most favorable) to -2 (least favorable). Compiled results for the present benchmark sample vary from a high of +1.53 to a low of -1.26, with a mean value at +0.33.

Figure 21. Distribution of Security Effectiveness Scores for 22 benchmark companies

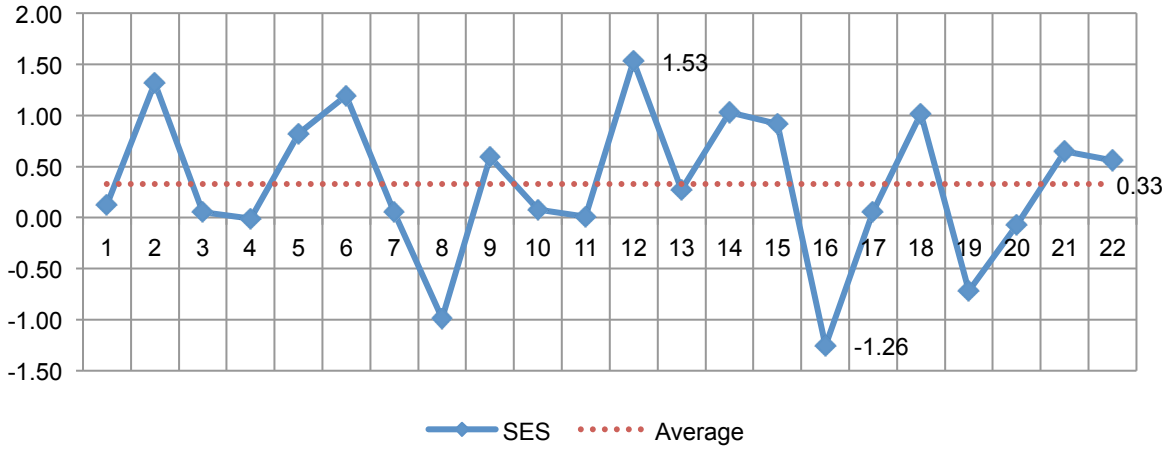
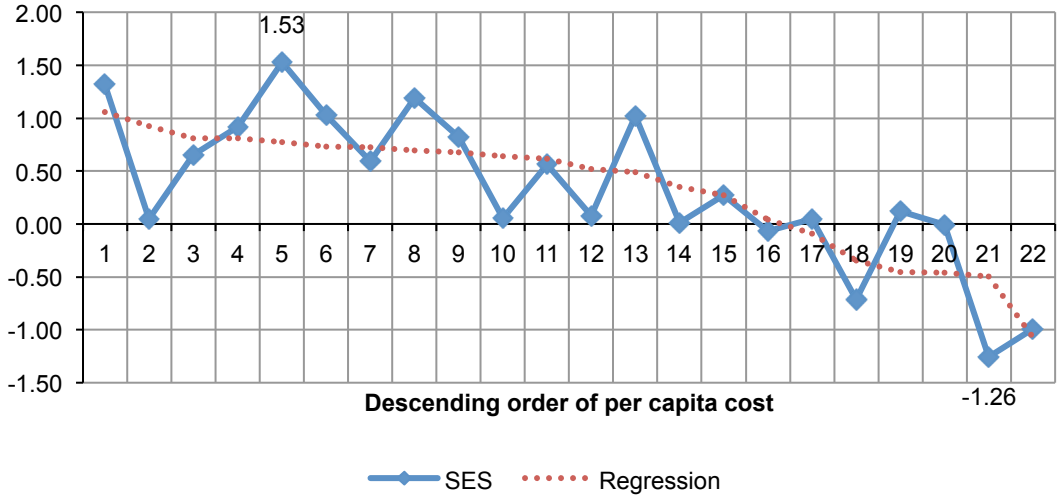


Figure 22 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is downward sloping, suggesting that the security effectiveness score (SES) for each organisation is inversely related to their per capita data breach cost. In other words, a strong security posture appears to moderate data breach costs.

Figure 22. Security Effectiveness Score (SES) in descending value of per capita cost
Regression = Intercept + {Per Capita Cost} x β, where β denotes the slope.



[5] The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organisations. 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.

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 implemented by companies after the data breach. The top preventive measures or steps taken after the data breach includes: additional manual controls (47 percent), the expanded use of encryption (46 percent), training and awareness programs (44 percent) and the strengthening of perimeter controls (33 percent).

Table 1. Preventive measures and controls implemented after the data breach	2009	2010	2011
Additional manual procedures and controls	56%	55%	47%
Training and awareness programs	52%	46%	44%
Expanded use of encryption	40%	43%	46%
Strengthening of perimeter controls	27%	30%	33%
Other system control practices	24%	21%	25%
Identity and access management solutions	23%	19%	23%
Data loss prevention (DLP) solutions	15%	16%	15%
Security certification or audit	13%	12%	10%
Security event management systems	11%	15%	18%
Endpoint security solutions	10%	16%	19%

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

Table 2 provides the percentage changes for 11 cost categories over three years. As can be seen, most cost categories appear to be relatively stable over time. The two highest cost categories pertain to investigation and forensics and lost customer business.

Table 2. Cost changes over three years	FY 2009	FY 2010	FY 2011
Investigations & forensics	26%	27%	28%
Audit and consulting services	11%	10%	9%
Outbound contact costs	10%	12%	12%
Inbound contact costs	9%	8%	7%
Public relations/communications	3%	3%	2%
Legal services - defense	4%	3%	5%
Legal services - compliance	6%	5%	4%
Free or discounted services	1%	1%	1%
Identity protection services	0%	0%	0%
Lost customer business	22%	22%	22%
Customer acquisition cost	8%	9%	10%

Part 3. Concluding observations and description about participating companies

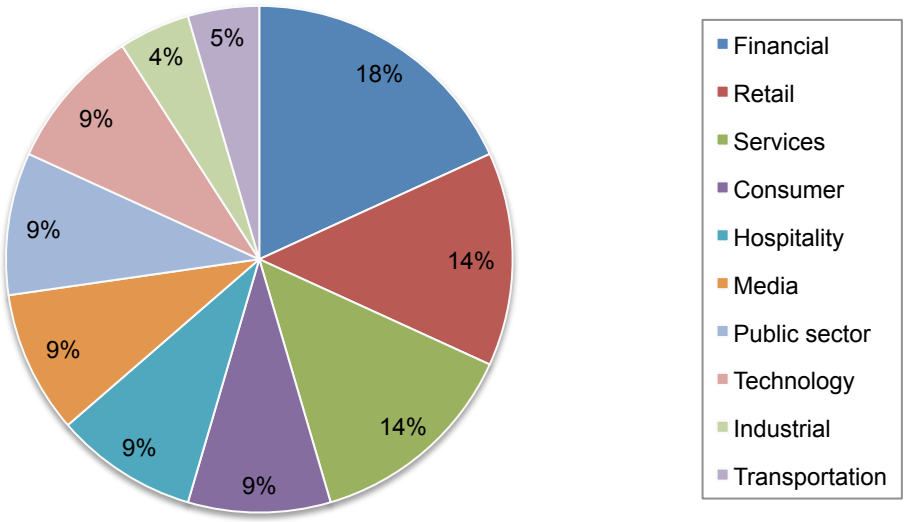
Companies participating in our annual study continue to report an increase in both the average total cost and per capita cost of data breach. The most profitable investments as evidenced by the lower cost of a data breach are the engagement of external consultants, appointment of a CISO with enterprise-wide responsibility and notification of data breach victims within 30 days.

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

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 23 shows the distribution of benchmark organisations by their primary industry classification. In this year's study, 10 industries are represented. Financial services, public sector (government), retail and hospitality represent the four largest segments.

Figure 23. 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 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.
- Ex-post 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-post 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.[6]
- 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.[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).

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

[6]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.

[7]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.[8]

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.

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

LL	_____|_____	UL

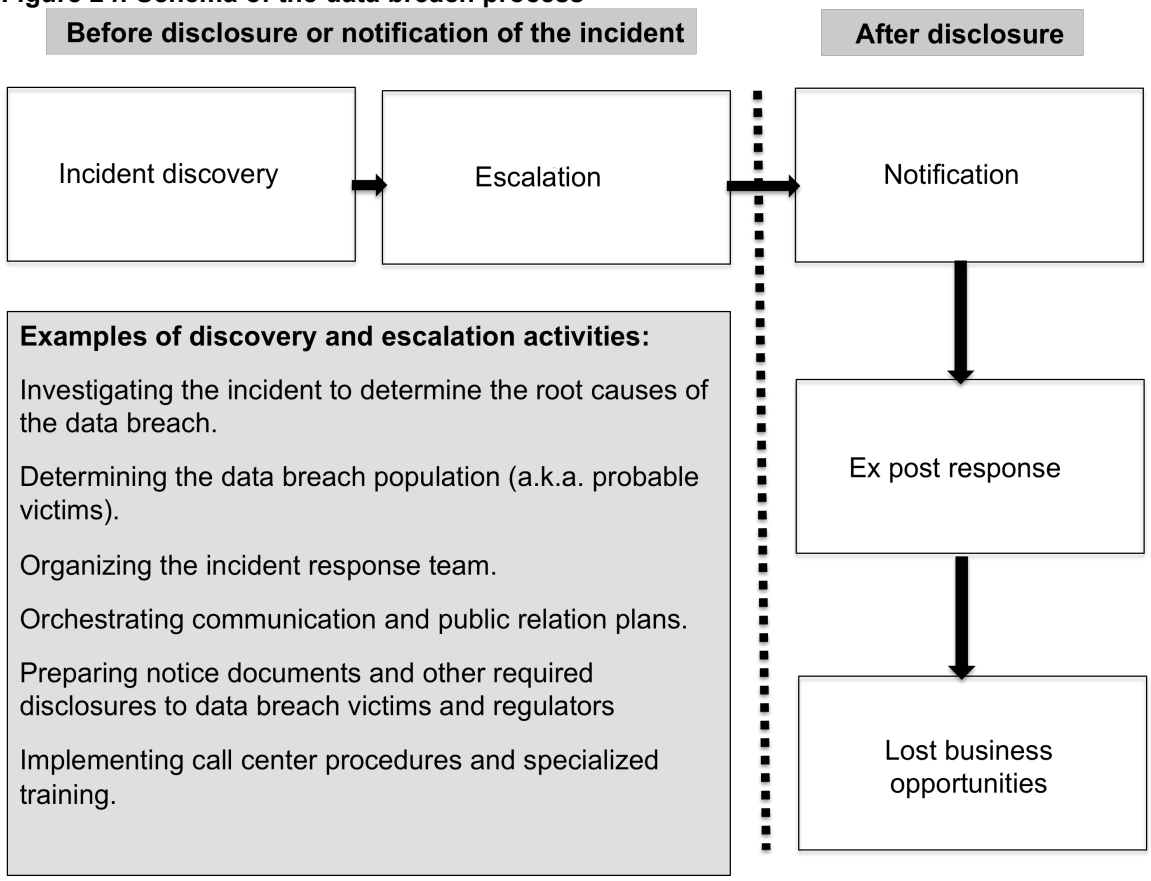
The numerical value obtained from the number line rather than a point estimate for each presented cost category preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

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.

[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.

Figure 24 illustrates the activity-based costing schema used in our benchmark study. The cost centers we examine sequentially are: incident discovery, escalation, notification, ex-post response and lost business.

Figure 24: Schema of the data breach process



Within each cost center, 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 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.

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-two 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.

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

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.

Appendix 1: Cost for 22 Data Breach Case Studies

Cases	Size of breach	Detection & escalation	Notification	Ex-post response	Lost business	Abnormal Churn
1	4,692	$181,260	$24,347	$184,986	$588,340	6.5%
2	65,521	$1,260,085	$32,592	$355,673	$3,032,011	1.3%
3	9,932	$577,434	$95,655	$391,689	$21,629	0.0%
4	6,500	$731,013	$151,183	$425,169	$54,010	5.2%
5	15,846	$690,217	$16,890	$780,933	$192,210	2.7%
6	26,311	$945,193	$103,083	$319,814	$1,385,496	3.4%
7	33,361	$956,788	$81,990	$298,085	$1,447,431	0.0%
8	2,500	$294,456	$29,882	$253,631	$83,002	4.6%
9	36,386	$525,918	$62,062	$2,259,294	$863,898	2.6%
10	22,440	$987,194	$112,673	$326,614	$1,275,577	3.4%
11	20,664	$1,040,418	$94,369	$281,913	$1,388,607	4.4%
12	19,528	$753,967	$88,178	$448,460	$615,690	1.8%
13	14,885	$842,598	$89,694	$517,770	$676,782	2.8%
14	18,825	$756,543	$69,343	$440,639	$642,517	1.2%
15	3,641	$261,120	$27,936	$9,181	$44,612	0.0%
16	3,541	$628,701	$106,098	$8,375	$8,695	7.2%
17	13,935	$1,123,979	$225,618	$711,878	$389,858	5.1%
18	16,485	$881,914	$11,465	$394,257	$739,767	2.8%
19	20,000	$1,081,026	$40,195	$848,760	$2,001,044	7.8%
20	5,774	$146,175	$100,930	$647,371	$49,868	6.4%
21	28,016	$1,007,606	$82,949	$524,778	$1,016,629	2.4%
22	29,245	$1,324,499	$27,653	$17,950	$1,891,539	2.6%