



2015 Cost of Data Breach Study: Impact of Business Continuity Management

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



2015¹ Cost of Data Breach Study: Impact of Business Continuity Management Ponemon Institute, June 2015

Part 1. Introduction

The *2015 Cost of Data Breach Study: Global Study*, sponsored by IBM, quantifies the economic impact of data breaches and observes cost trends over time. We believe a better understanding of the cost, the root causes and factors that influence the cost will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the consequences of an attack.

The average per capita cost of data breach differs widely among the countries. Many of these cost differences can be attributed to the types of attacks and threats organizations face as well as the data protection regulations and laws in their respective countries. In this year's global study, the average per capita cost of data breach increased from \$145 to \$154. The total cost of a data breach increased from \$3.5 to \$3.8 million.²

This year's study involved 350 companies in 16 industry sectors representing the following countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Arabian region and, for the first time, Canada. All participating organizations experienced a data breach ranging from a low of approximately 3,000 to nearly 100,000 compromised records³. We define a compromised record as one that identifies the individual whose information has been lost or stolen in a data breach.

An important takeaway from this annual research is a better understanding of the factors that can minimize the financial consequences of a data breach. This special report analyzes the positive impact a business continuity management (BCM) program can have on the financial and reputational consequences of a data breach.⁴

Many companies have a BCM function or team that is involved in enterprise risk management, disaster recovery and crisis management. About 50 percent of companies in this study are now involving BCM experts when they have a data breach. As a result of having these experts and BCM processes in place the resolution of the data breach is more efficient and less costly.

The Impact of Business Continuity Management Programs on the Cost of a Data Breach

- 9% reduction in the per capita cost of data breach
- 27% reduction in the mean time to identify a data breach
- 41% reduction in the mean time to contain a data breach
- 28% decrease in the likelihood of a data breach over the next 2 years

Key takeaways about the importance of BCM in reducing the consequences of a data breach:

- **The cost of data breach is linearly related to the mean time it takes to identify and the mean time to contain the data breach incident.** Our findings suggest that BCM involvement results in a substantially lower mean time to identify and mean time to contain

¹This 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.

²Local currencies were converted to U.S. dollars.

³The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

⁴The BCM teams supporting the incident response process include practitioners in the disaster recovery function.

the data breach incident. Specially, companies without BCM involvement experienced an average of 234 days to identify the breach. In contrast, companies with BCM involvement experienced an average of 178 days to identify the breach. Similarly, those without BCM involvement experienced an average of 83 days to contain versus 55 days to contain the breach for those with BCM involvement.

- **BCM involvement in data breach incident response planning and execution is very significant.** Of the 350 companies in this global study, 174 companies self-reported they have BCM involvement in resolving the consequences of a data breach. The majority of these companies (63 percent) rate their involvement as very significant.
- **The cost of data breach is more expensive if BCM is not part of the data breach incident response planning and execution.** The average cost per lost or stolen record can be as high as \$161. With BCM involvement the average cost can be as low as \$147.
- **The likelihood of having a future data breach is higher for companies that do not involve BCM as part of its incident response planning.** The findings reveal that if BCM is not involved in data breach planning, the likelihood of having a data breach sometime over the next 2 years is 27.9 percent. Whereas, if BCM is involved, this likelihood drops to 21.1 percent.
- **Germany and Japan have the highest percentage of companies that engage their company's BCM teams to aid in the planning and execution of data breach incident response.** The countries with the lowest BCM involvement are Brazil and the Arabian region. With the exception of Italy, all countries increased the level of BCM involvement in the data breach incident management process.
- **BCM minimizes disruptions to business operations when a data breach occurs.** According to the findings, 80 percent of companies without BCM involvement had a material disruption to business operations. This decreases to 55 percent for companies involving BCM.
- **BCM involvement improves the resilience of IT operations.** Seventy-four percent of companies without BCM involvement said they had a material disruption to their IT operations. This decreases to 52 percent of those with BCM involvement said IT operations were materially disrupted.
- **BCM can protect a company's reputation following a data breach.** Less than half of companies in this research with BCM involvement (45 percent) said their reputation or brand was negatively impacted because of a data breach. However, 55 percent of companies without BCM involvement said their organization's brand and reputation was affected.

Part 2. Key Findings

The following table lists 11 countries, legend, sample sizes and currencies used in this global study. It also shows the number of years of annual reporting for each country ranging from one year for Canada to 10 years for the United States.

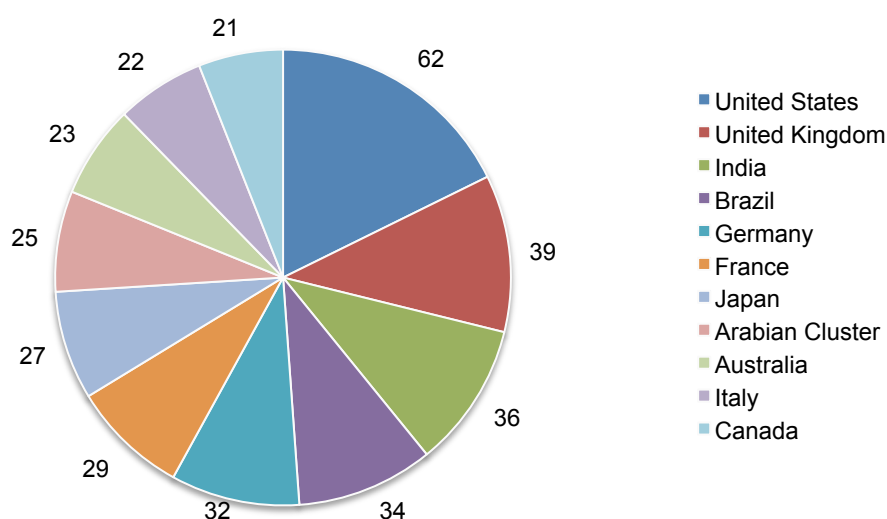
Table 1. Global Study at a Glance					
Legend	Countries	Sample	Pct%	Currency	Years of study
AB	Arabian Cluster*	25	7%	AED/SAR	2
AU	Australia	23	7%	AU Dollar	6
BZ	Brazil	34	10%	Real	3
CA	Canada	21	6%	CA Dollar	1
DE	Germany	32	9%	Euro	7
FR	France	29	8%	Euro	6
ID	India	36	10%	Rupee	4
IT	Italy	22	6%	Euro	4
JP	Japan	27	8%	Yen	4
UK	United Kingdom	39	11%	GBP	8
US	United States	62	18%	US Dollar	10
	Total	350	100%		

*AB is a combined sample of companies located in Saudi Arabia and the United Arab Emirates

The following chart shows the distribution of 350 participating organizations within 11 countries. As can be seen, the US represents the largest segment with 62 organizations and Canada the smallest sample with 21 organizations.

Pie Chart 1. Frequency of benchmark samples by country

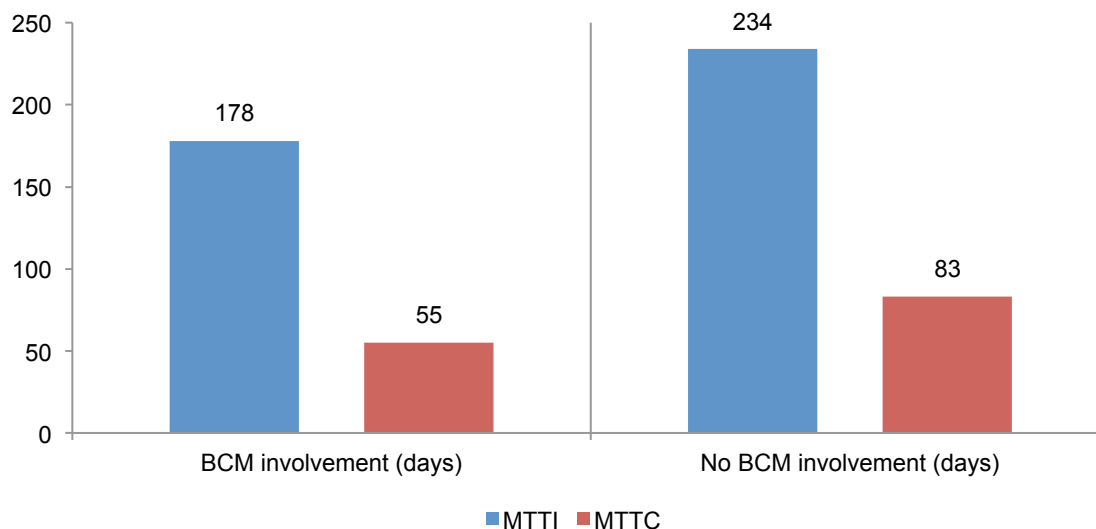
Consolidated view (n = 350)



The cost of data breach is linearly related to the mean time it takes to identify and the mean time to contain the data breach incident. In this year's study, we showed that the mean time to identify (MTTI) and mean time to contain (MTTC) the data breach were linearly related to data breach costs. Figure 1 shows another interesting interrelationship. That is, both days to identify and days to contain the data breach incident are substantially lower for organizations that involved BCM. The percentage difference in the MTTI and MTTC is 27 percent and 41 percent, respectively.

Figure 1. MTTI and MTTC for organizations that involve or fail to involve BCM in the incident response process

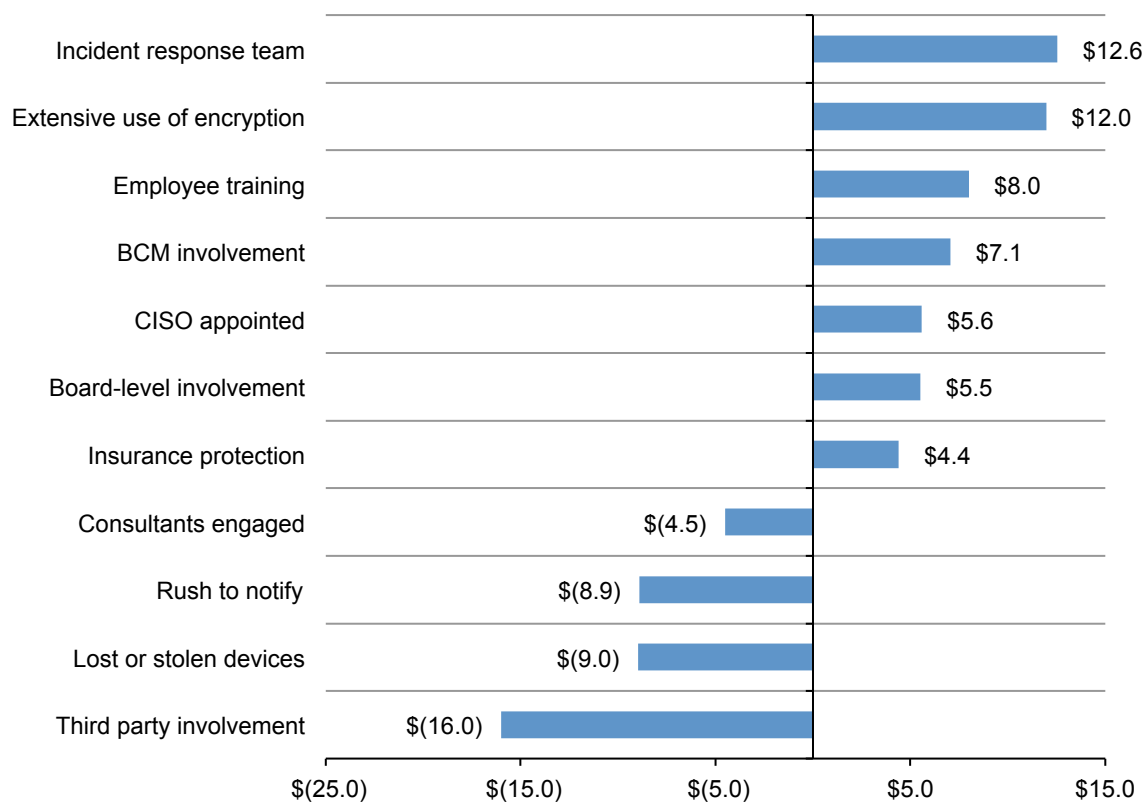
Percentage difference for MTTI = 27%; percentage difference for MTTC = 41%
Consolidated view (FY 2015 = 350, FY 2014 = 315)



Factors that influence the cost of data breach. In the context of this analysis, positive numbers are incremental cost savings and negative numbers are incremental cost increases defined for each one of 11 factors. As shown in Figure 2, the existence of a strong incident response team results in the greatest decrease in the per capita cost of data breach. Business continuity management decreases the cost of data breach by an average of \$7.1 per compromised record.

Figure 2. Impact of 11 factors on the per capita cost of data breach

Measured in US\$ consolidated view (n = 350)



BCM's contribution to incident response planning. Figure 3 provides a summary of BCM involvement in the data breach incident response planning and execution. Of the 350 companies in this global study, 174 or 50 percent had BCM involvement. The remaining 176 companies did not involve their BCM team or only involved BCM on an ad hoc basis. Last year's analysis showed 45 percent of companies involved BCM in the data breach incident response.

Figure 3. How does BCM contribute to the data breach incident response process?

Consolidated view (FY 2015 = 350, FY 2014 = 315)

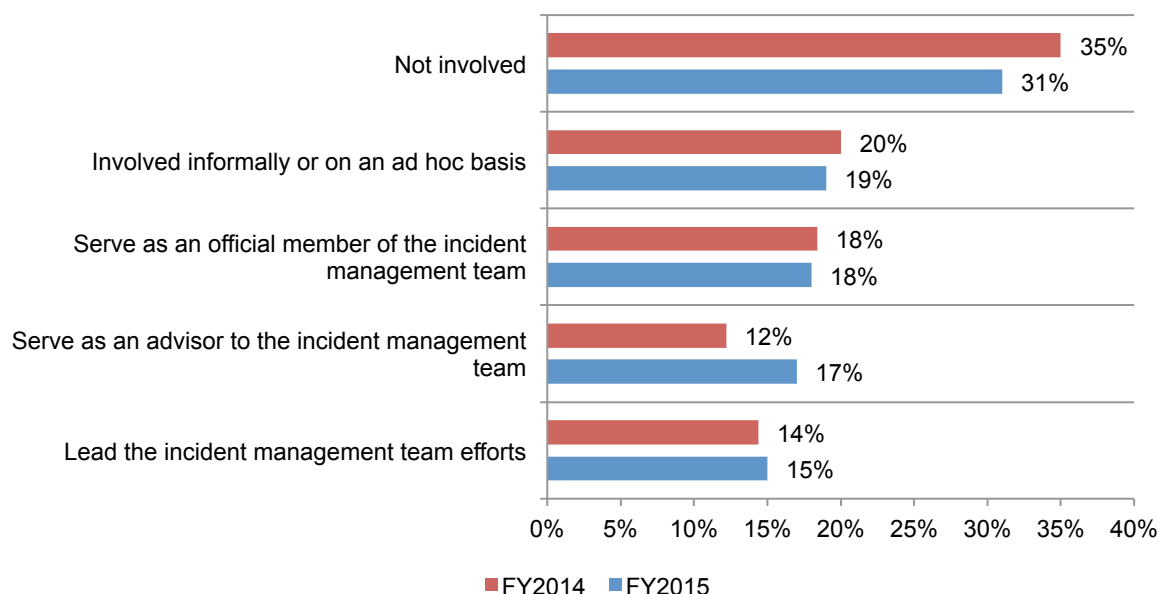
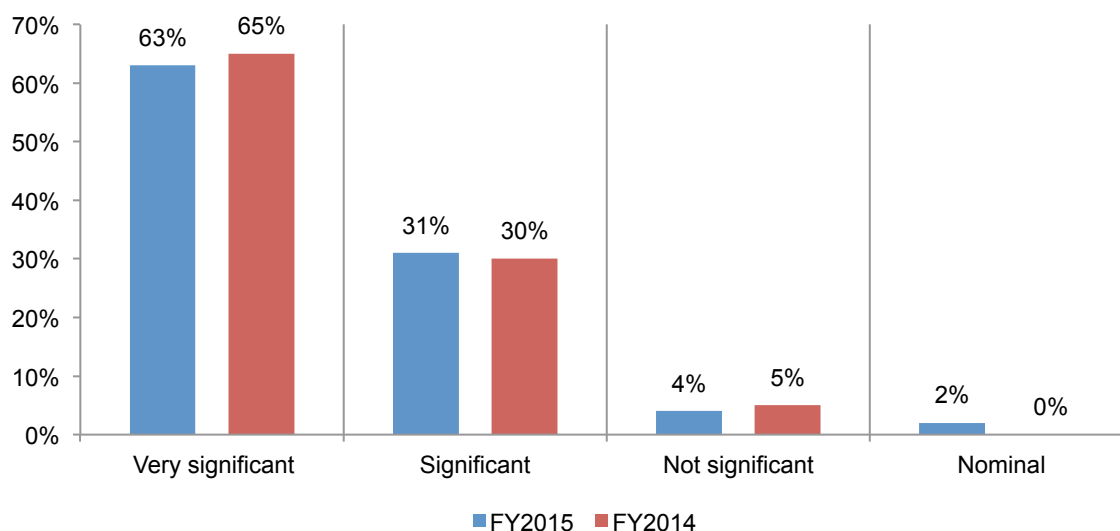


Figure 4 shows the level of BCM involvement in incident response planning and execution. For this year's study, 63 percent of companies rate this involvement as very significant. Another 31 percent rate BCM involvement as significant. Last year's study showed 65 and 30 percent rating BCM involvement as very significant or significant, respectively.

Figure 4. What best describes BCM's contribution to the incident response process?

Consolidated view (FY 2015 = 350, FY 2014 = 315)



BCM reduces the per capita cost of data breach. Figure 5 reports the average per capita cost of data breach for companies that involve the BCM team in incident response planning and execution, and those that do not over two years. Those companies involving BCM experience a lower per capita cost than those that do not involve BCM. The percentage difference in the per capita cost of data breach between companies that do and do not involve BCM is 9 percent this year. Last year's percentage difference was 13 percent.

Figure 5. Per capita cost of data breach for companies with or without BCM involvement

Percentage difference in FY 2015 = 9%; percentage difference in FY 2014 = 13%

Consolidated view (FY 2015 = 350, FY 2014 = 315)

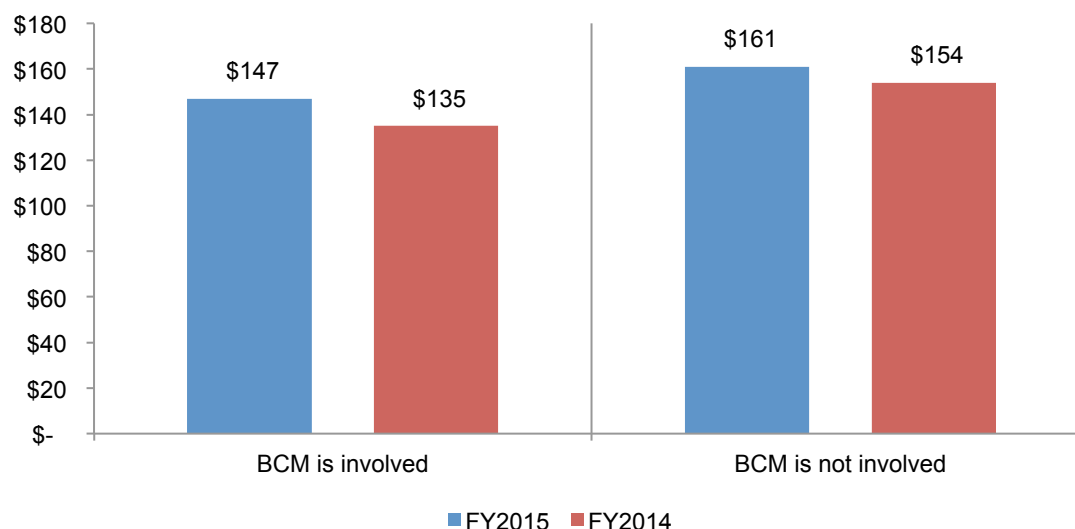


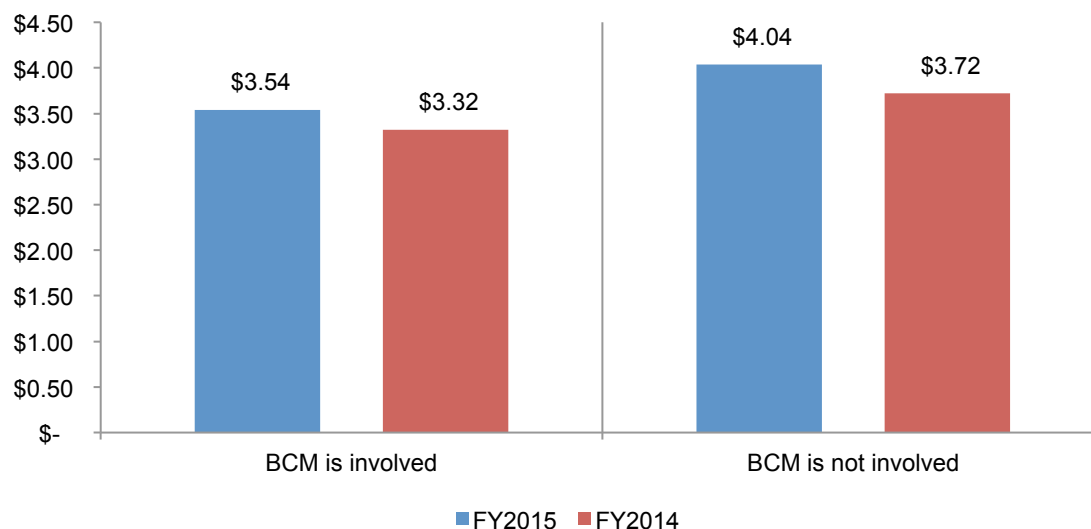
Figure 6 reports the total cost of data breach for companies that involve the BCM team in incident response planning and execution, and those that do not over two years. Similar to the above, those companies involving BCM experience a lower total cost than those that do not involve BCM. The percentage difference in the total cost between companies that do and do not involve BCM is 13 percent. Last year, this percentage difference was 11 percent.

Figure 6. Per capita cost of data breach for companies with or without BCM involvement

Percentage difference in FY 2015 = 13%; percentage difference in FY 2014 = 11%

Consolidated view (FY 2015 = 350, FY 2014 = 315)

(\$millions)

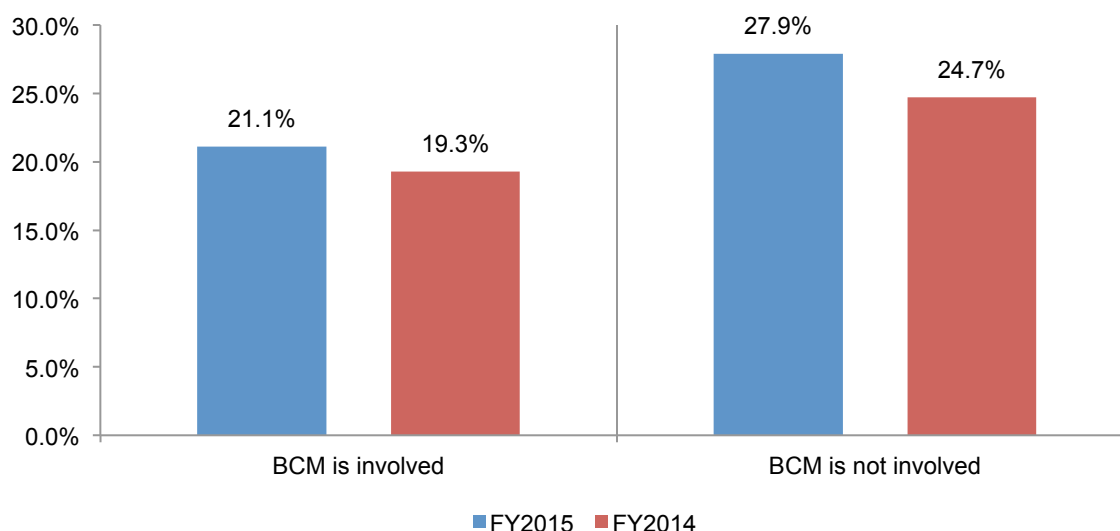


BCM reduces the likelihood of a data breach. Figure 7 reports the average likelihood of data breach involving a minimum of 10,000 or more records over the next 24 months for companies that involve the BCM team and those that do not.

Clearly, organizations that involve BCM experience a lower likelihood of incurrence than those that do not involve BCM. This pattern holds true for both the 2014 and 2015 results. Specifically, the percentage difference in the likelihood of a future data breach between companies that do and do not involve BCM is 28 percent this year. Last year's percentage difference was 25 percent.

Figure 7. Likelihood of a material data breach for companies with or without BCM involvement

Percentage difference in FY 2015 = 28%; percentage difference in FY 2014 = 25%
Consolidated view (FY 2015 = 350, FY 2014 = 315)



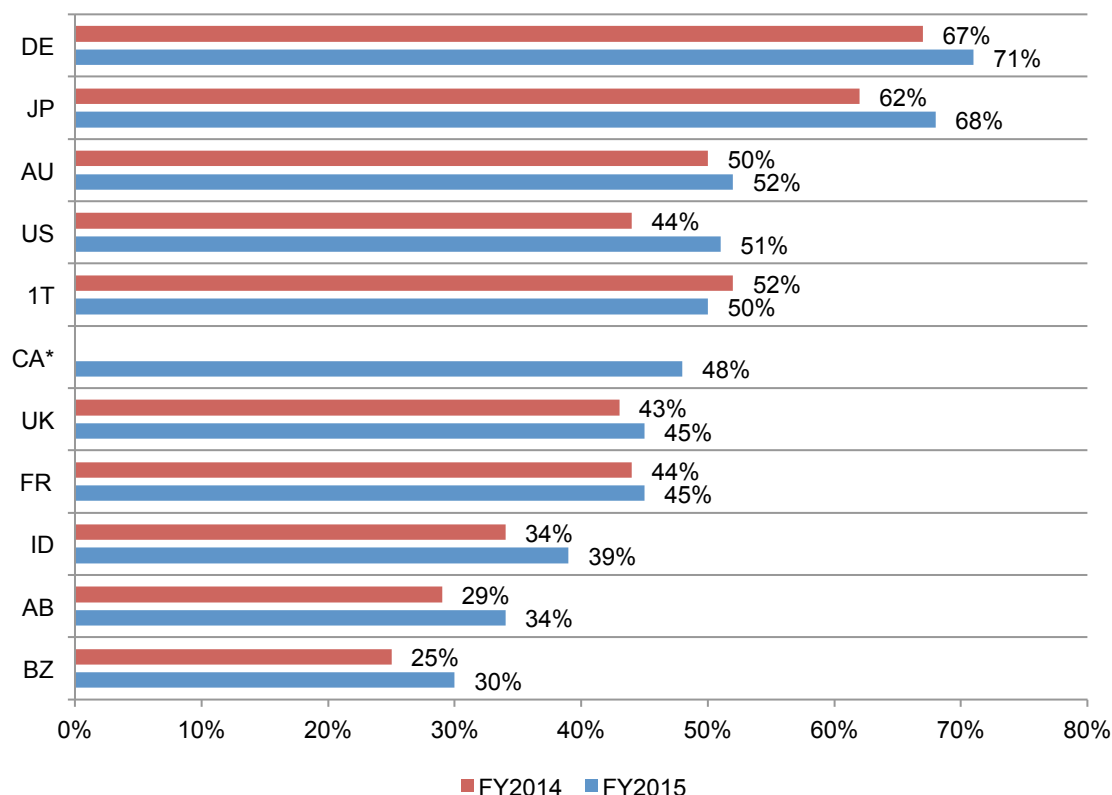
Germany and Japan are most likely to involve BCMs when dealing with data breaches.

Figure 8 shows the percentage of BCM team involvement in incident planning and execution for 11 country samples. Similar to last year, Germany (DE) has the highest rate of BCM involvement with 71 percent of German companies reporting they have a BCM team. In contrast, only 30 percent of Brazilian (BZ) companies have BCM involvement. It is interesting to note that with one exception (Italy), all countries experienced a net increase in BCM involvement over the past year.

Figure 8. BCM participation rate by country sample

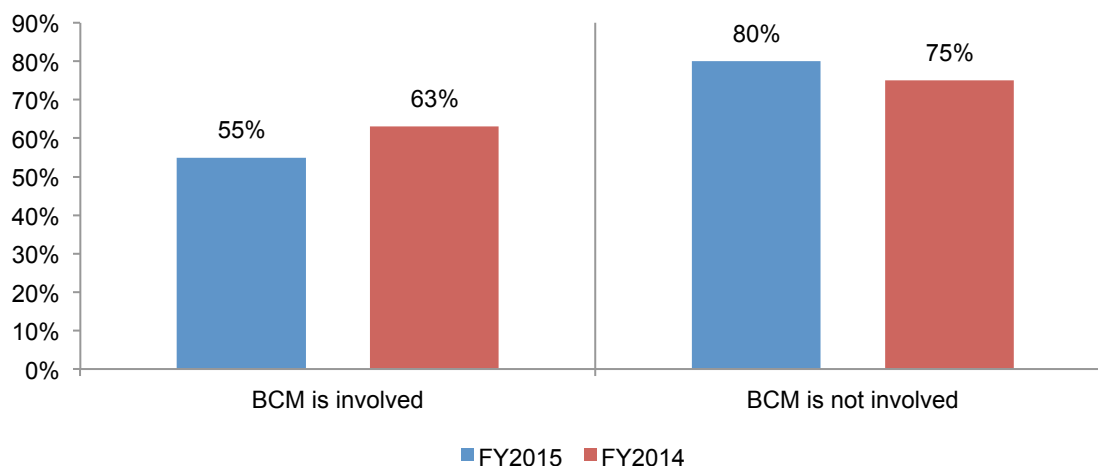
*Historical data is not available

(FY 2015 = 350, FY 2014 = 315)



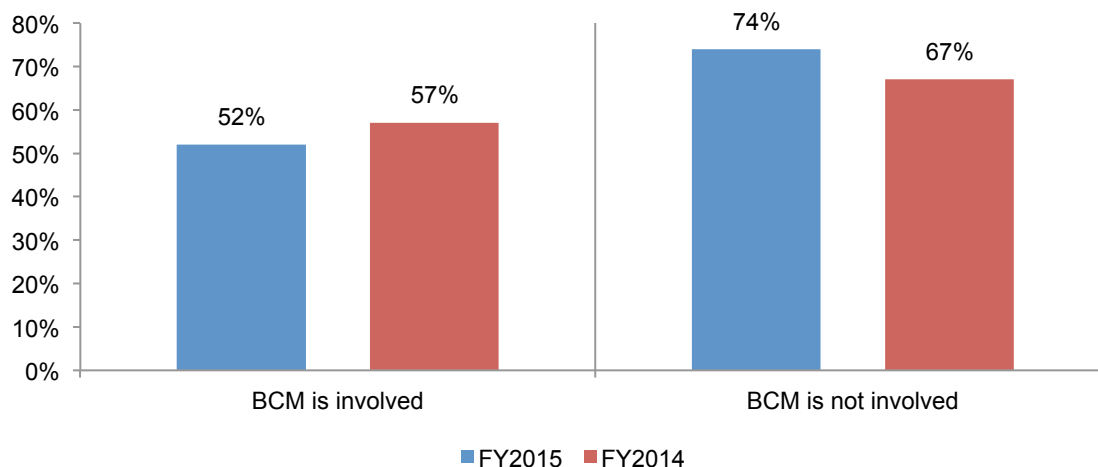
BCM minimizes disruptions to business operations when a data breach occurs. Figure 9 reveals differences between companies with or without BCM involvement with respect to material disruption to business processes. As reported for FY 2015, 80 percent of companies without BCM involvement said the data breach incident caused a material disruption to business process. However, 55 percent of companies with BCM involvement had a material disruption. A similar pattern holds true for FY 2014 results.

Figure 9. Did the data breach incident cause a material disruption to business processes?
Consolidated view (FY 2015 = 350, FY 2014 = 315)



BCM involvement improves the resilience of IT operations. Similar to the above, Figure 10 shows differences between companies with or without BCM involvement with respect to material disruption to IT operations. As reported for FY 2015, 74 percent of companies without BCM involvement said the data breach incident caused a material disruption to IT operations. In contrast, 52 percent of companies with BCM involvement said the incident caused a material disruption. A similar pattern holds true for FY 2014 results.

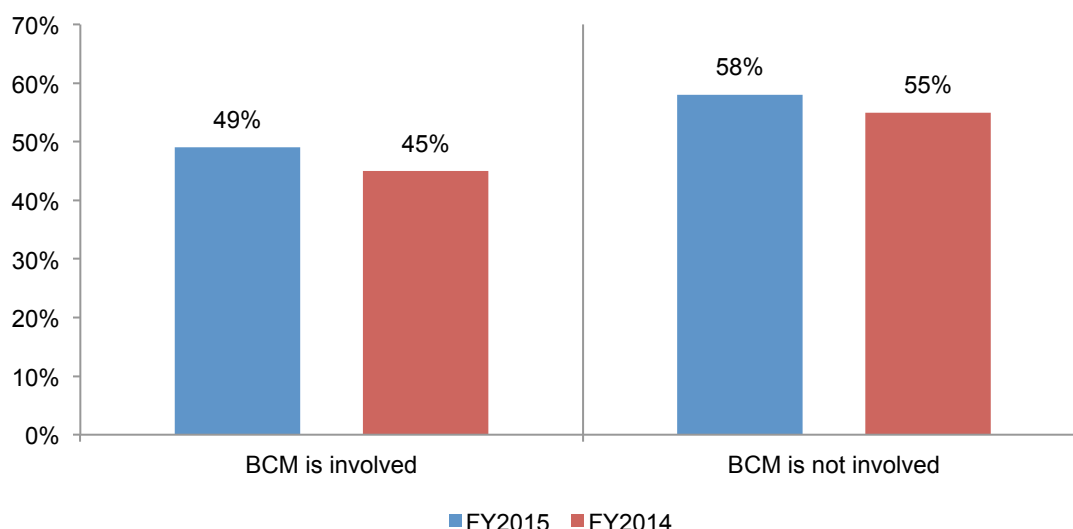
Figure 10. Did the data breach incident cause a material disruption to IT operations?
Consolidated view (FY 2015 = 350, FY 2014 = 315)



BCM can protect a company's reputation following a data breach. Figure 10 also shows differences between companies that engage BCM versus those that do not. In the current year's study, 55 percent of companies that do not involve BCM said the data breach had a material negative impact on reputation and brand. In contrast, 45 percent of companies that involve BCM said the incident had a negative impact on the organization's reputation or brand. A similar pattern holds true for FY 2014 results.

Figure 10. Did the data breach have a material negative impact on the organization's reputation?

Consolidated view (FY 2015 = 350, FY 2014 = 315)



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:

- Detection or discovery: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.
- Escalation: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- Notification: Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.
- Post data breach: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms. Post data breach activities also include credit report monitoring or the reissuing of a new account (or credit card).

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

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

- Turnover of existing customers: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.⁵
- 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.⁶ 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).

⁵In 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.

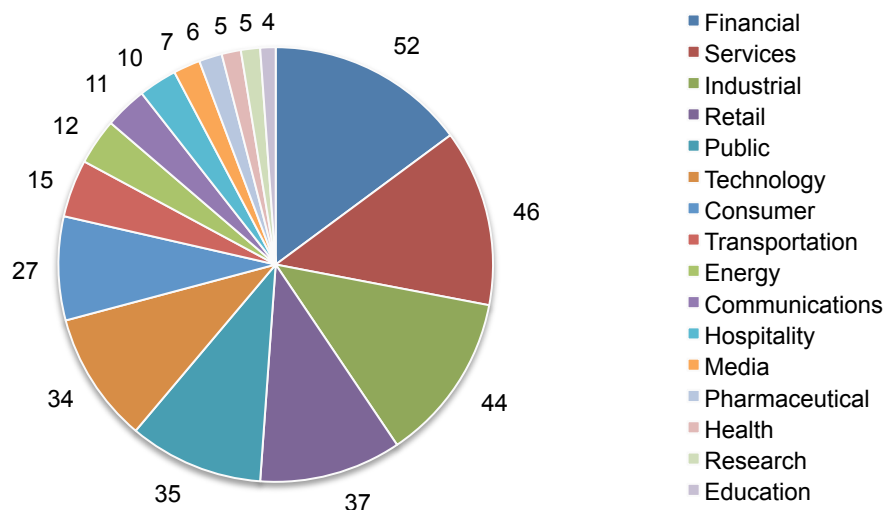
⁶In this study, we consider citizen, patient and student information as customer data.

Part 4. Organizational characteristics and benchmark methods

Pie Chart 2 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 16 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Pie Chart 2. Distribution of the benchmark sample by industry segment

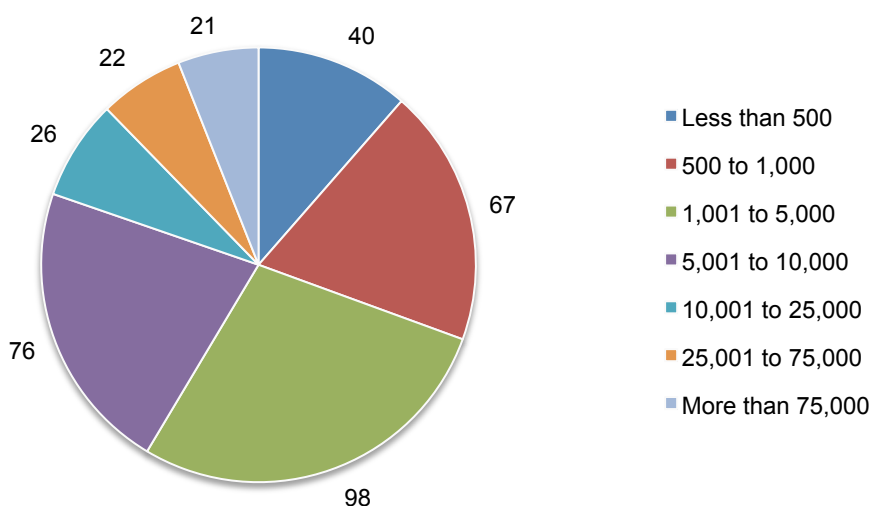
Consolidated view (n = 350)



Pie Chart 3 shows the distribution of benchmark organizations by total headcount. The largest segments include companies with more than 1,000 employees.

Pie Chart 3. Global headcount of participating companies

Consolidated view (n = 350)



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	<hr style="border: none; border-top: 1px solid black; margin: 0;"/>	UL
----	---	----

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

To keep the benchmarking process to a manageable size, we carefully limited items to only those cost activity centers that we considered crucial to data breach cost measurement. Based upon discussions with learned experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was re-examined carefully for consistency and completeness.

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

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

Part 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 global 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. In this global study, 350 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 reports are available at www.ibm.com/security/data-breach

Ponemon Institute
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.