2016 Cost of Data Breach Study:
Impact of Business Continuity Management

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2016

2016[1] Cost of Data Breach Study:
Impact of Business Continuity Management

Ponemon Institute, June 2016

Part 1. Introduction

The *2016 Cost of Data Breach Study: Impact of Business Continuity Management (BCM),* sponsored by IBM, analyzes the financial and reputational benefits of having a BCM program in advance of a data breach. According to the research, BCM programs can reduce the per capita cost of data breach, the mean time to identify and contain a data breach and the likelihood of experiencing such an incident over the next two years.[2]

The BCM research is part of the *2016 Cost of Data Breach Study: Global Study,* which quantifies the economic impact of data breaches and observes cost trends over time. In this year's global study, the average per capita cost of data breach increased from $154 to $158. The total cost of a data breach increased from $3.8 to $4 million.[3]

This year's study involved 383 companies in 16 industry sectors representing the following countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, Arabian region, Canada and, for the first time, South Africa. All participating organizations experienced a data breach ranging from a low of approximately 3,000 to nearly 101,500 compromised records[4]. We define a compromised record as one that identifies the individual whose information has been lost or stolen in a data breach.

The majority of companies (52 percent) in the global study have a BCM function or team that is involved in enterprise risk management, disaster recovery and crisis management. These experts are involved when a company has a data breach and, as a result of their involvement, the resolution of the data breach is more efficient and less costly.

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

- $9 reduction in per capita cost of data breach
- 11% reduction in the per capita cost of data breach
- 15% reduction in the total cost of data breach
- 52-day reduction in the mean time to identify a data breach
- 36-day reduction in the mean time to contain a data breach
- 29% decrease in the likelihood of a data breach over the next 2 years

The following key takeaways reveal how companies in this year's study benefited from a BCM program.

- **BCM involvement results in a substantially lower mean time to identify and mean time to contain the data breach incident.** In particular, companies without BCM involvement experienced an average of 227 days to identify the breach. In contrast, companies with BCM involvement experienced an average of 175 days to identify the breach. Similarly, those without BCM involvement experienced an average of 88 days to contain versus 52 days to contain the breach for those with BCM involvement.
- **The combined saved days in identifying and containing a material data breach varies across 16 industry sectors.** Education and retail organizations were able to reduce the time it takes to identify and contain a material data breach by 115 and 109 days respectively. Financial services reduces the time by 68 days.

---

[1]This report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of
[2]The BCM teams supporting the incident response process include practitioners in the disaster recovery function.
[3]Local currencies were converted to U.S. dollars.
[4]The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

- **BCM involvement in data breach incident response planning and execution is very significant**. Of the 383 companies in this global study, 199 companies self-reported they have BCM involvement in resolving the consequences of a data breach. The majority of these companies (65 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 $167. With BCM involvement the average cost can be as low as $149. Similarly, the total cost of data breach with or without BCM involvement is $3.71 million and $4.29 million, respectively.
- **The per day cost savings resulting from BCM involvement is substantial.** The extrapolated cost savings per day that result from efficiencies in identifying and containing the data breach incident. As can be seen, companies that involve BCM achieve an average per day savings of $6,591 through the containment phase of the data breach response.
- **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 29 percent. Whereas, if BCM is involved, this likelihood drops to 22 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, 78 percent of companies without BCM involvement had a material disruption to business operations. This decreases to 52 percent for companies involving BCM.
- **BCM involvement improves the resilience of IT operations**. Seventy-five percent of companies without BCM involvement said they had a material disruption to their IT operations. In contrast, 55 percent of those with BCM involvement said IT operations were materially disrupted.
- **BCM can protect a company's reputation following a data breach**. Fifty-one percent of companies in this study said their reputation or brand had been negatively impacted because of a data breach. However, (a much larger percentage) 60 percent of companies without BCM involvement said their organization's brand and reputation was affected.

A further analysis based on 33 interviews with individuals responsible for managing the data breach incident response process reveals the following reasons that contribute to the financial and reputational benefits of a BCM program.

- Creates an orientation toward rigorous planning and testing
- Enables an upstream and downstream communication channel under times of crisis
- Establishes a structure that reduces complexity of the incident response process
- Raises organizational acumen and awareness about crisis events as a result of compliance with BCM policies, plans and standards
- Provides leadership and expertise that support proactive management of significant risk
- Advances a culture that embraces proactive monitoring and vigilance

Part 2. Key Findings

The following table lists 12 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 South Africa to 11 years for the United States.

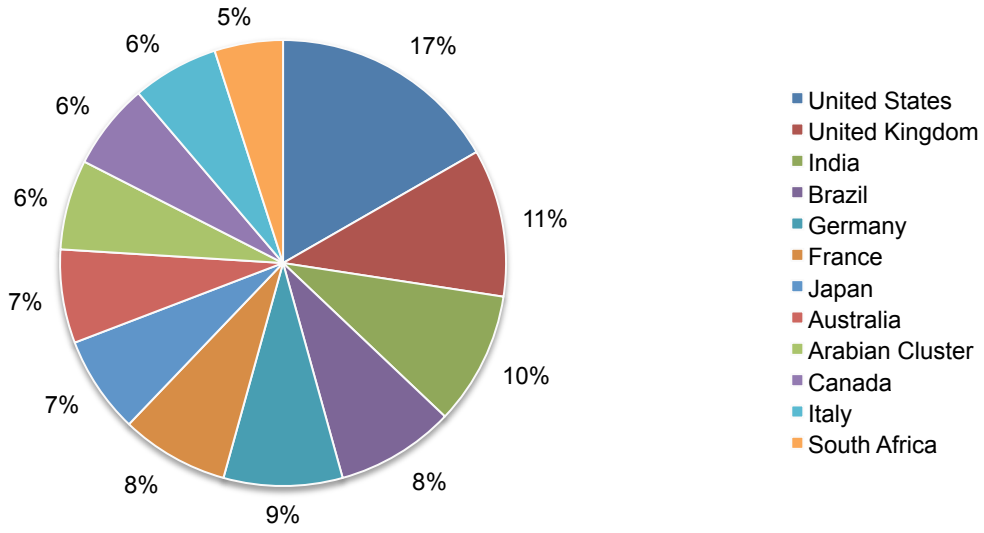
Table 1. Global Study at a Glance

Legend	Countries	Sample	Pct%	Currency	Years of study
AB	Arabian Cluster*	25	7%	AED/SAR	3
AU	Australia	26	7%	AU Dollar	7
BZ	Brazil	33	9%	Real	4
CA	Canada	24	6%	CA Dollar	2
DE	Germany	33	9%	Euro	8
FR	France	30	8%	Euro	7
ID	India	37	10%	Rupee	5
IT	Italy	24	6%	Euro	5
JP	Japan	27	7%	Yen	5
SA	South Africa	19	5%	ZAR	1
UK	United Kingdom	41	11%	GBP	9
US	United States	64	17%	US Dollar	11
	Total	383	100%		

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

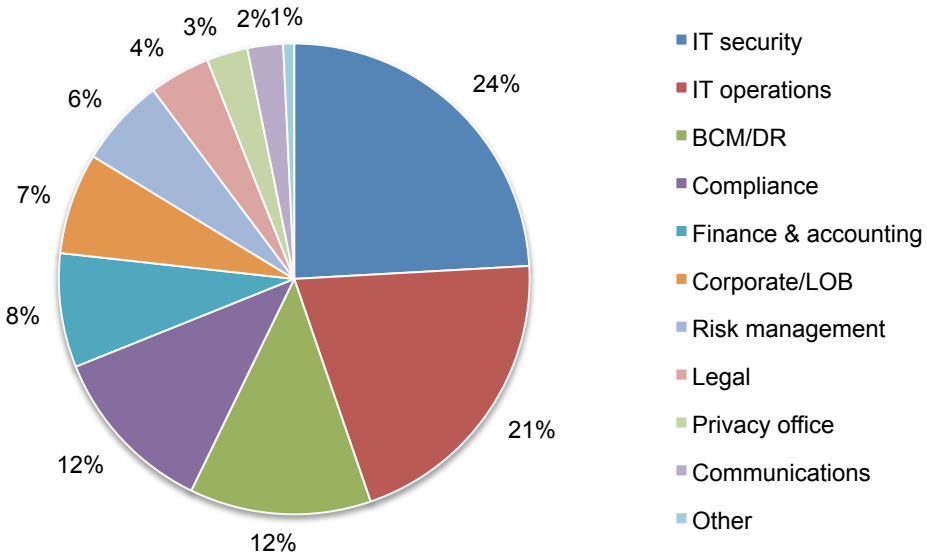
The following chart shows the distribution of 383 participating organizations within 12 countries. As can be seen, the US represents the largest segment with 64 organizations and South Africa represents the smallest sample with 19 organizations.

Pie Chart 1. Percentage frequency of benchmark samples by country
Consolidated view (n=383)



Pie Chart 2 shows the distribution of 1,596 individuals who participated in interviews, representing 383 organizations within 12 countries. Twenty-four percent of interviewees are located in IT security (e.g., SecOps), followed by 21 percent who are located in IT operations.

Pie Chart 2. Percentage frequency of interviewees who participated in the study by functional location
Consolidated view (n=1,596)



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) the data breach is positively correlated to data breach costs. Figure 1 shows the days to identify the data breach are lower for organizations that involved BCM; namely, a time savings of 52 days in FY 2016 and 56 days in FY 2015.

Figure 1. MTTI for organizations that involve or fail to involve BCM in the incident response process
MTTI differences (FY 2016=52 days, FY 2015=56 days)
MTTI percentage differences (FY 2016=26%, FY 2015=27%)
Consolidated view (FY 2016=383, FY 2015=350)

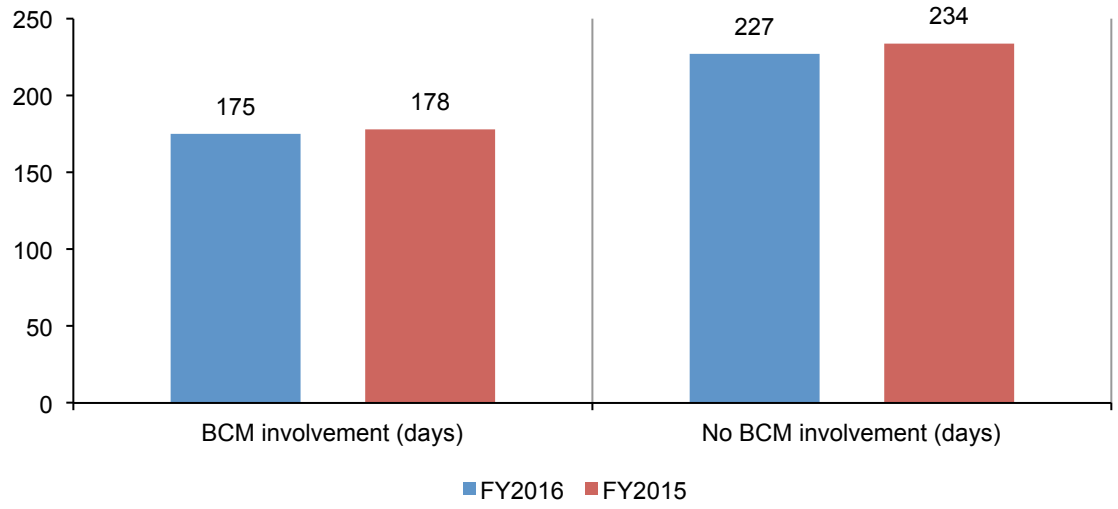
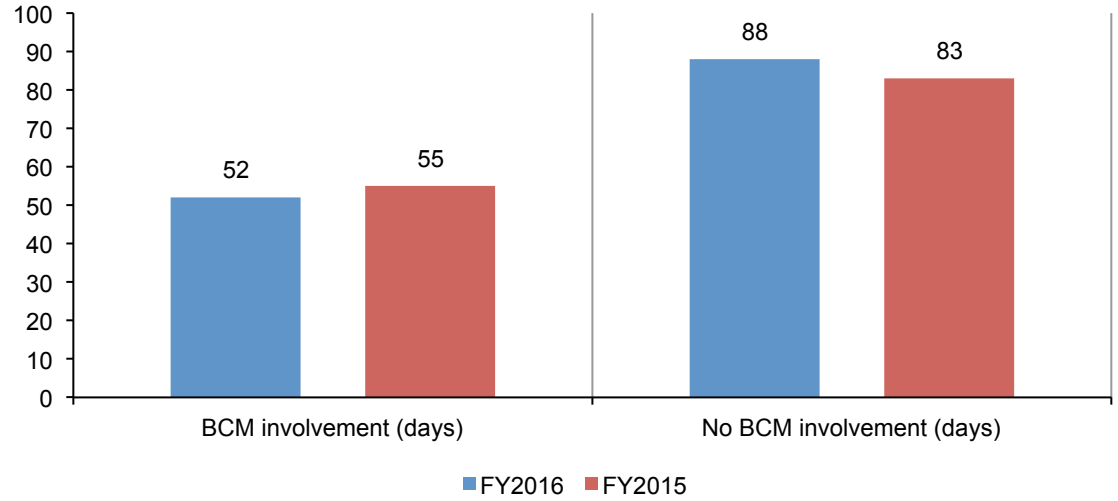


Figure 2 shows a similar relationship. That is, days to contain the data breach incident are substantially lower for organizations that involved BCM, or a time savings of 36 days in FY 2016 and 28 days in FY 2015.

Figure 2. MTTC for organizations that involve or fail to involve BCM in the incident response process
MTTC differences (FY 2016=36 days, FY 2015=28 days)
MTTC percentage differences (FY 2016=40%, FY 2015=41%)
Consolidated view (FY 2016=383, FY 2015=350)



The following chart provides the industry distribution of 383 companies that participated in this year's study. Pie Chart 3 shows the distribution of 16 industry sectors.

Pie Chart 3. Percentage frequency of benchmark samples by industry
Consolidated view (n=383)

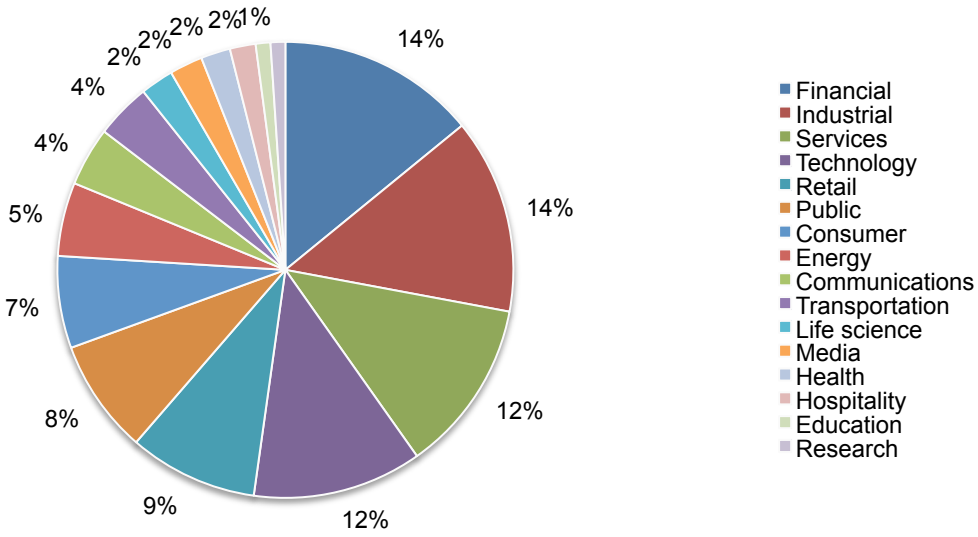


Figure 3 shows the combined saved days in identifying and containing a material data breach for 16 industry sectors. Education and retail achieve the highest day savings at 115 and 109 days respectively. At 68 days, financial services has the lowest savings.

Figure 3. MTTI and MTTC combined saved days resulting from BMC involvement
Average day savings (FY 2016=88 days)
Consolidated view (n=199)

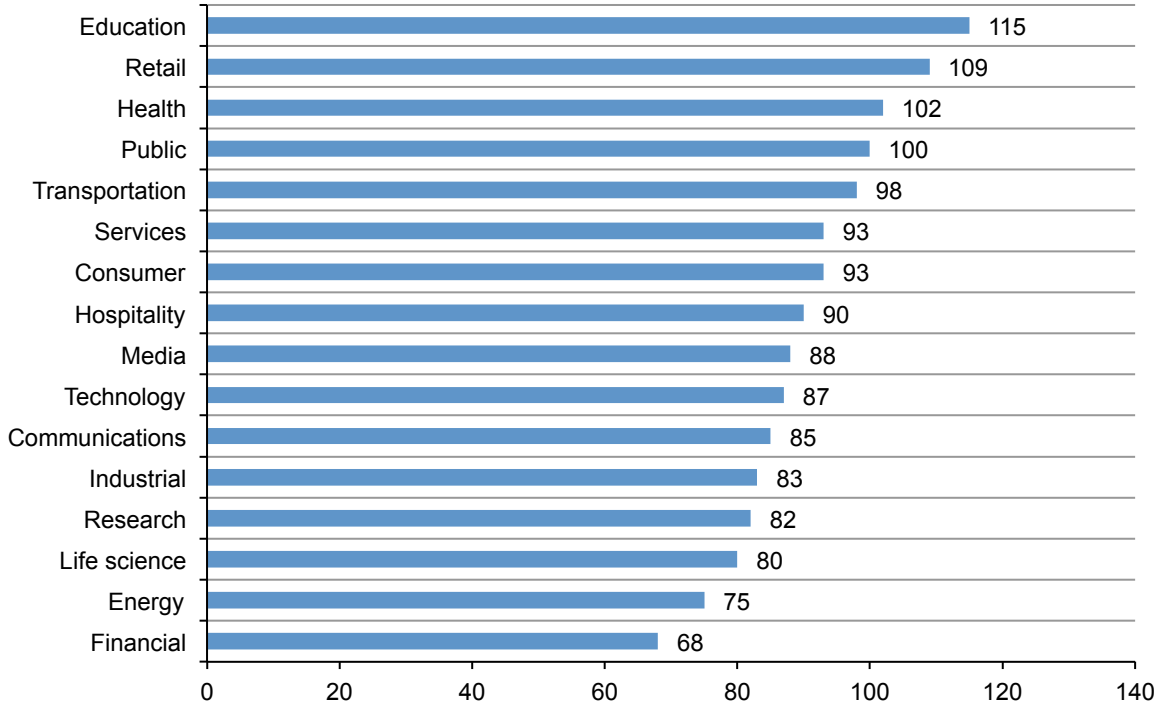


Figure 4 provides the extrapolated cost savings per day that result from MTTI and MTTC efficiencies. As can be seen, companies that involve BCM achieve an average per day savings of $6,591 over 88 days. Last year's extrapolated savings were $5,952 over 84 days.

Figure 4. Cost savings per day as a result of BCM involvement
Total cost savings in U.S. millions resulting from BCM involvement (FY 2016=$.580, FY 2015=$.500)
MTTI and MTTC combined day savings (FY 2016=88 days, FY 2015=84 days)
Consolidated view (FY 2016=383, FY 2015=350)

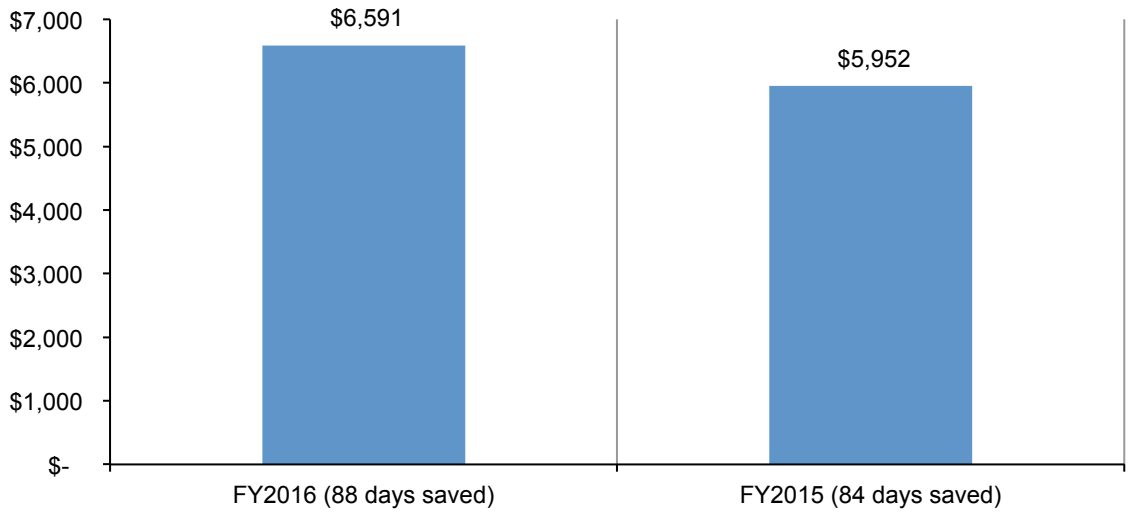


Table 2 illustrates the potential cost savings by industry segment. As shown, the potential for the most cost savings is in education. While, the least is in financial services.

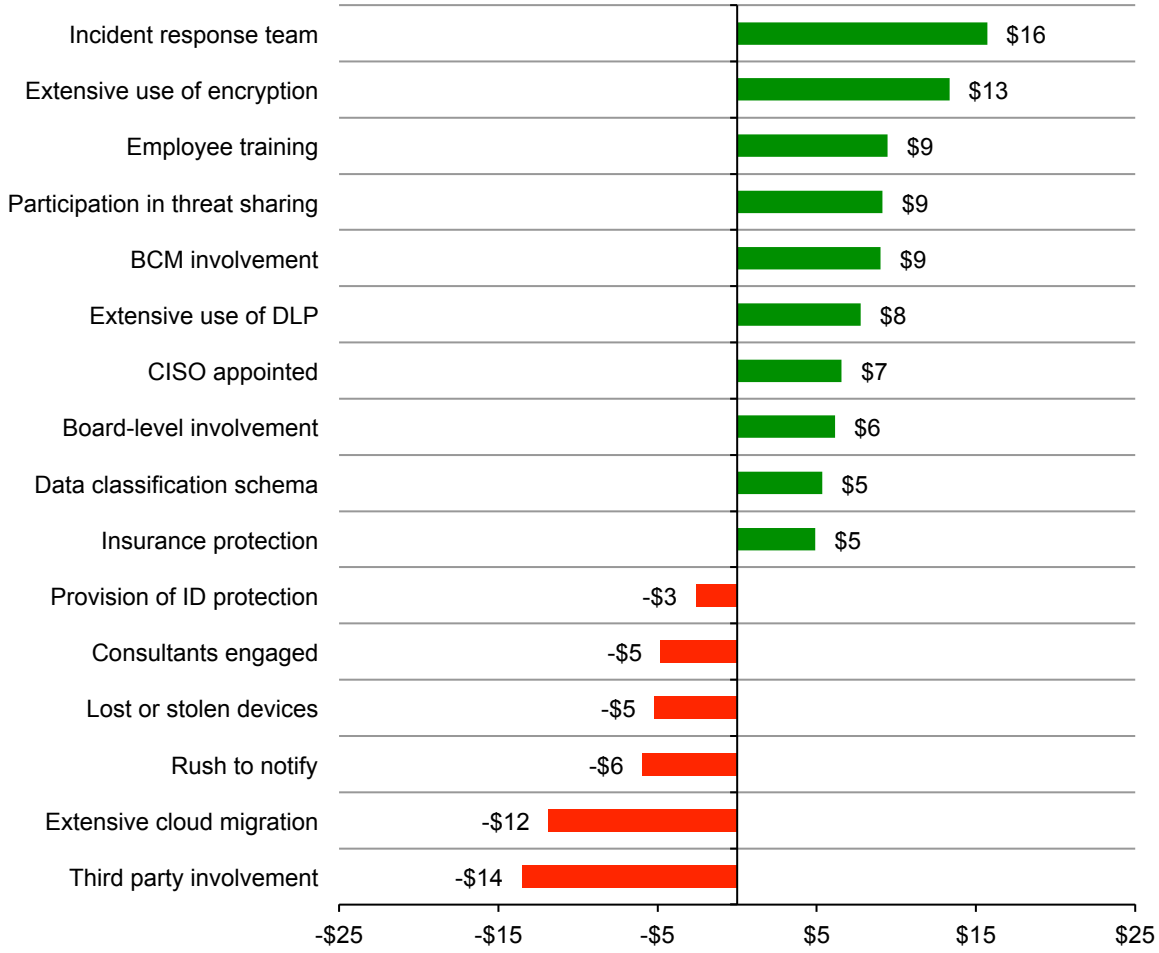
Table 2: Estimated cost savings by industry	Days saved	Total cost savings*
Education	115	$757,965
Retail	109	$718,419
Health	102	$672,282
Public	100	$659,100
Transportation	98	$645,918
Consumer	93	$612,963
Services	93	$612,963
Hospitality	90	$593,190
Media	88	$580,008
Technology	87	$573,417
Communications	85	$560,235
Industrial	83	$547,053
Research	82	$540,462
Life science	80	$527,280
Energy	75	$494,325
Financial	68	$448,188

*Cost savings in FY2016 is simply days saved X $6,591 for each industry.

Factors that influence the cost of data breach. In the context of this analysis, positive numbers (highlighted in green) are incremental cost savings and negative numbers (highlighted in red) are incremental cost increases defined for each one of the 16 factors.

As shown in Figure 4, the existence of a strong incident response team results in the greatest reduction in the per capita cost of data breach. Business continuity management decreases the cost of data breach by an average of $9 per compromised record.

Figure 4. Impact of 16 factors on the per capita cost of data breach
Measured in US$ consolidated view (n=383)



BCM's contribution to incident response planning. Figure 5 provides a summary of BCM involvement in the data breach incident response planning and execution. Of the 383 companies in this global study, 199 or 52 percent had BCM involvement. The remaining 184 companies did not involve their BCM team or only involved BCM on an ad hoc basis. Last year's analysis showed 50 percent of companies involved BCM in the data breach incident response.

Figure 5. How does BCM contribute to the data breach incident response process?
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)

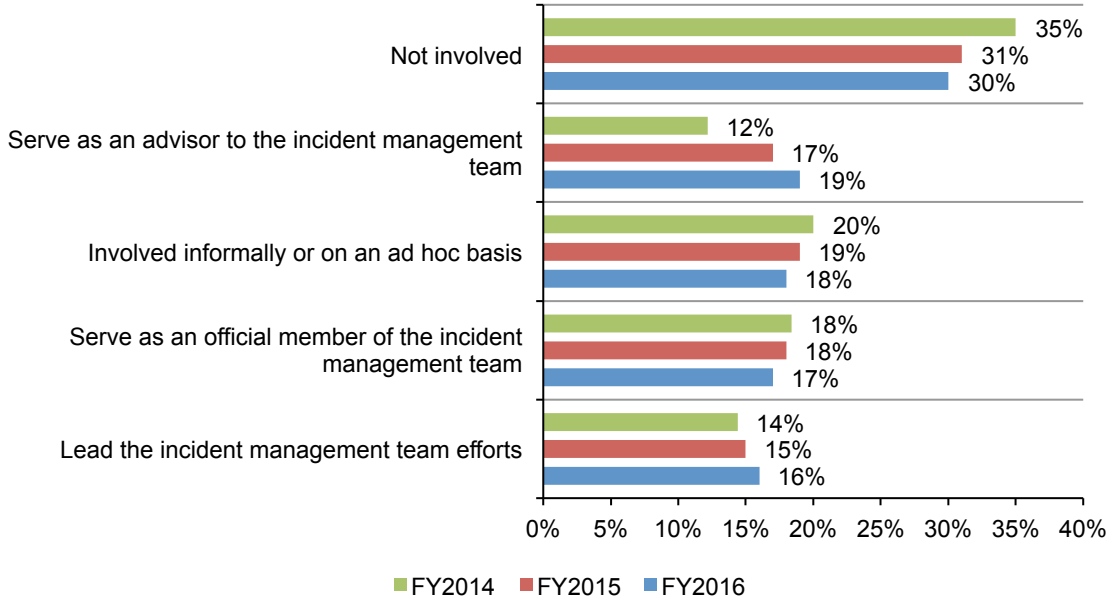
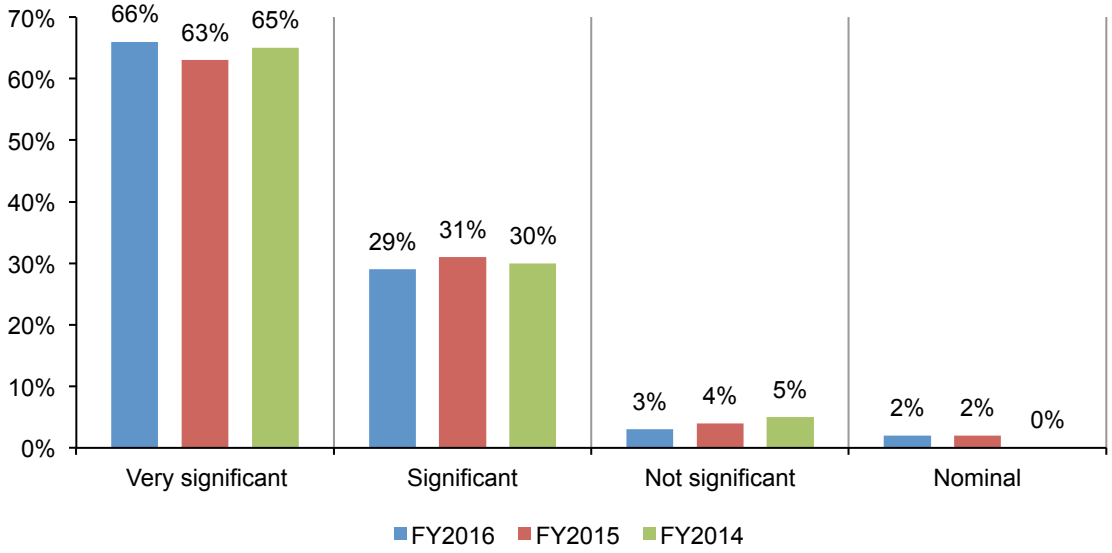


Figure 6 shows the level of BCM involvement in incident response planning and execution. For this year's study, 66 percent of companies rate this involvement as very significant. Another 29 percent rate BCM involvement as significant. Last year's study showed that 63 and 31 percent rated BCM involvement as very significant or significant, respectively.

Figure 6. What best describes BCM's contribution to the incident response process?
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)



BCM reduces the per capita cost of data breach. Figure 7 reports the average per capita cost of data breach over three years for companies that involve the BCM team in incident response planning and execution, and those that do not. Those companies involving BCM experience a lower per capita cost than those that do not involve BCM. In this year's study, the difference in the per capita cost of data breach between companies that do and do not involve BCM is ± $9 – or a percentage difference of 11 percent.

Figure 7. Per capita cost of data breach for companies with or without BCM involvement
Percentage difference (FY 2016=11%, FY 2015=9%, FY 2014=13%)
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)

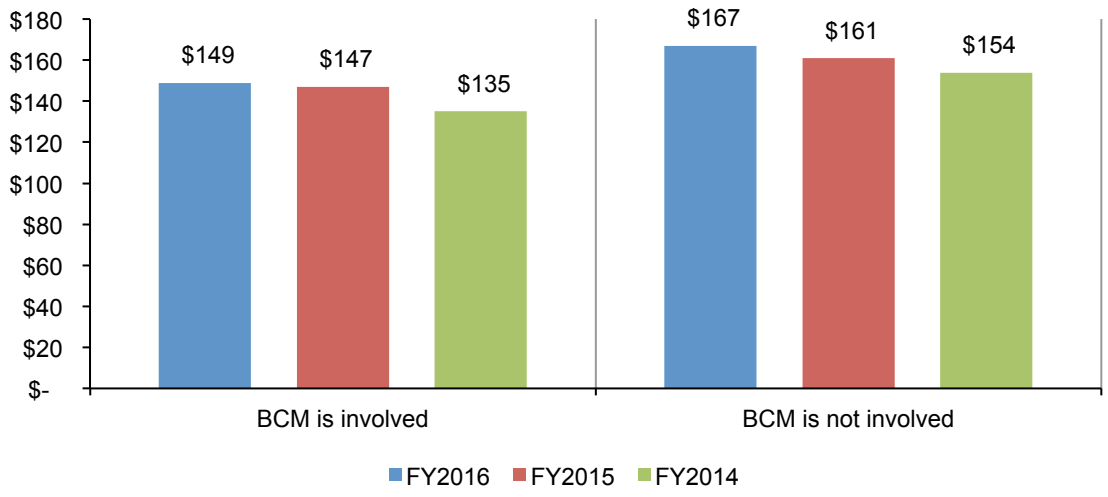
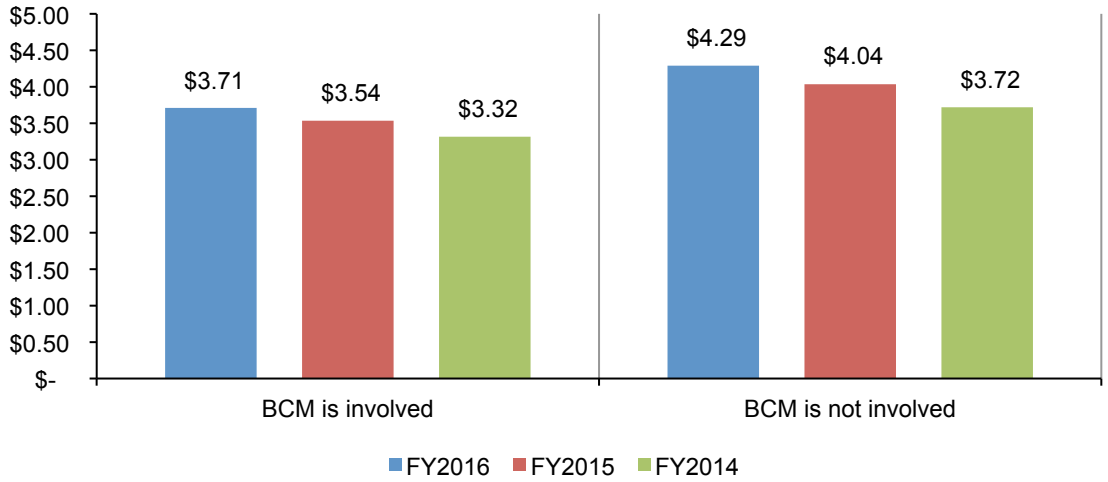


Figure 8 reports the total cost of data breach over three years for companies that involve the BCM team in incident response planning and execution and those that do not. Similar to the above, those companies involving BCM experience a lower total cost of data breach than those that do not involve BCM. In this year's study, the difference in the total cost between companies that do and do not involve BCM is more than $580,000 – or a percentage difference of 15 percent.

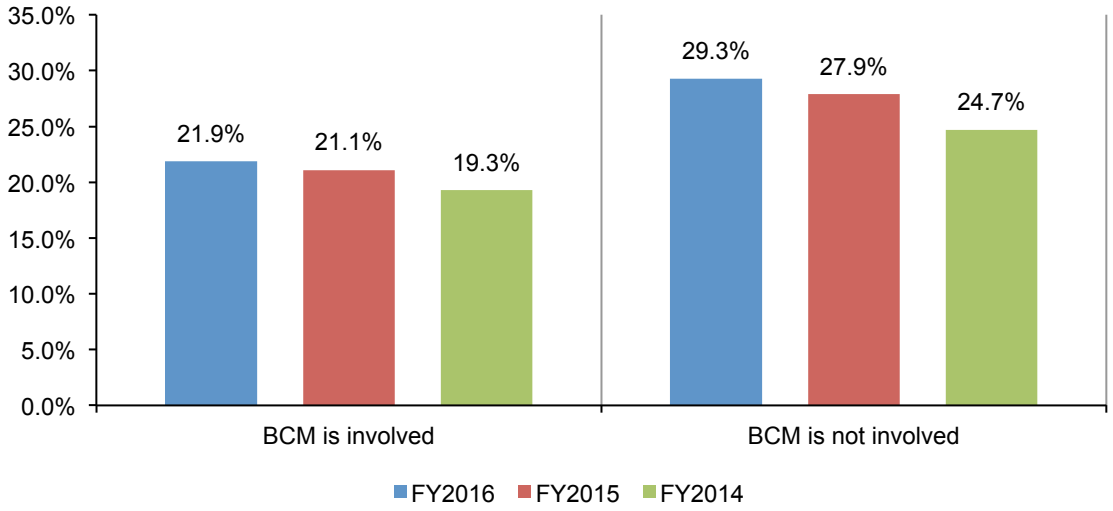
Figure 8. Total cost of data breach for companies with or without BCM involvement
Percentage difference (FY 2016=15%, FY 2015=13%, FY 2014=11%)
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)
($millions)



BCM reduces the likelihood of a data breach. Figure 9 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.

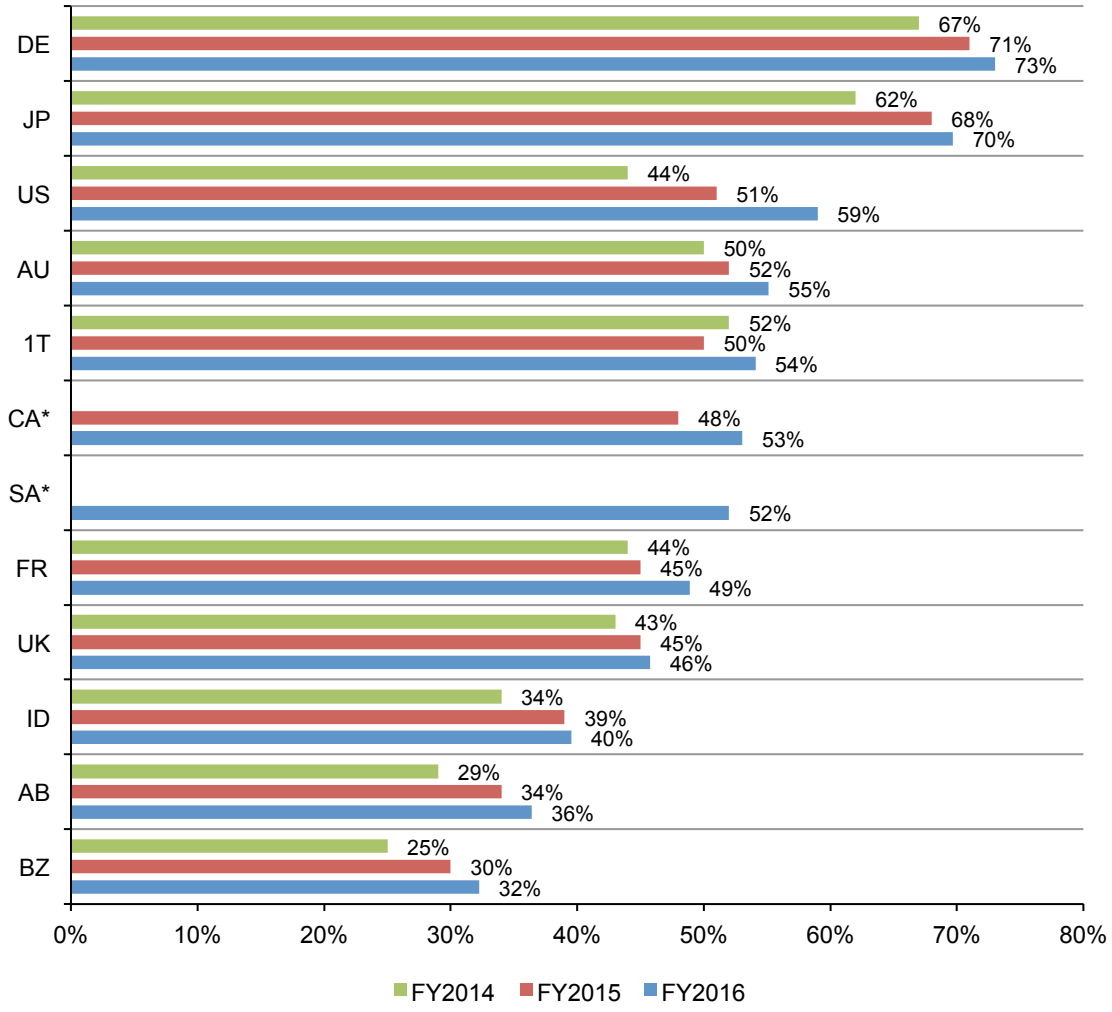
Over the past three years, we found that organizations that involve the BCM team experience a lower likelihood of incurrence than those that do not involve BCM. In this years study, the difference in the likelihood of a future data breach between companies that do and do not involve BCM is 29 percent.

Figure 9. Likelihood of a material data breach for companies with or without BCM involvement
Percentage difference (FY 2016=29%, FY 2015=28%, FY 2014=25%)
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)



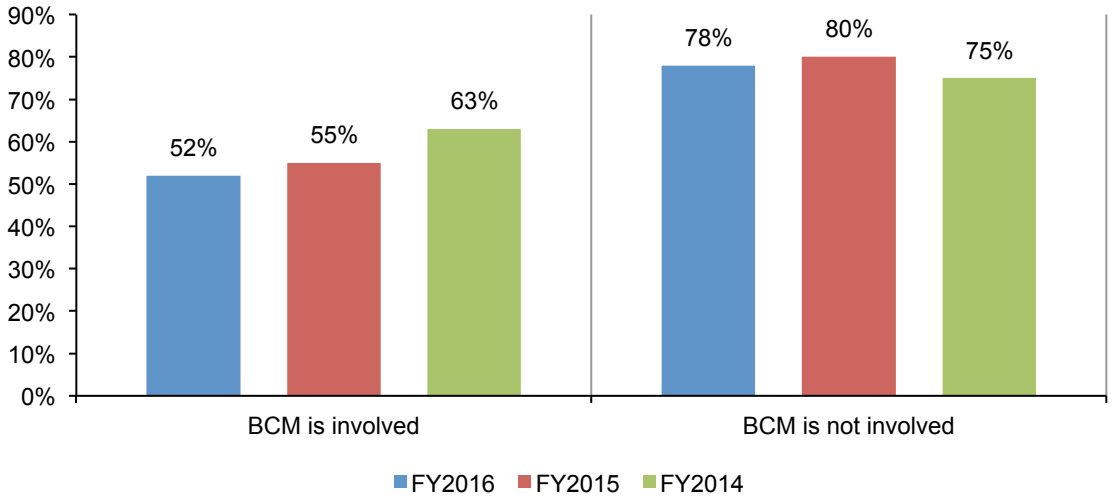
Germany and Japan are most likely to involve BCMs when dealing with data breaches. Figure 9 shows the percentage of BCM team involvement in incident planning and execution for 12 country samples. Similar to the last three years, Germany (DE) has the highest rate of BCM involvement with 73 percent of German companies reporting they have a BCM team. In contrast, only 32 percent of Brazilian (BZ) companies have BCM involvement. It is interesting to note that all countries experienced a net increase in BCM involvement over the past year.

Figure 10. BCM participation rate by country sample
*Historical data is not available
Consolidated view (FY 2016=383 FY 2015=350, FY 2014=315)



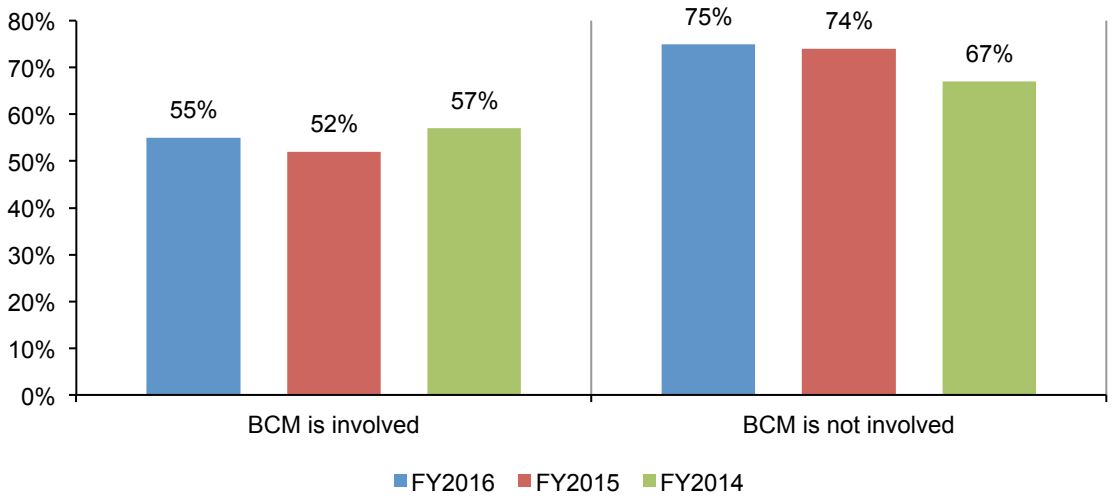
BCM minimizes disruptions to business operations when a data breach occurs. Figure 11 reveals differences between companies with or without BCM involvement with respect to material disruption to business processes. As reported for FY 2016, 78 percent of companies without BCM involvement said the data breach incident caused a material disruption to their business process. However, 52 percent of companies with BCM involvement said they had a material disruption. A similar pattern holds true for all three years.

Figure 11. Did the data breach cause a material disruption to business processes?
Consolidated view (FY 2016=383, FY 2015=350, FY 2014=315)



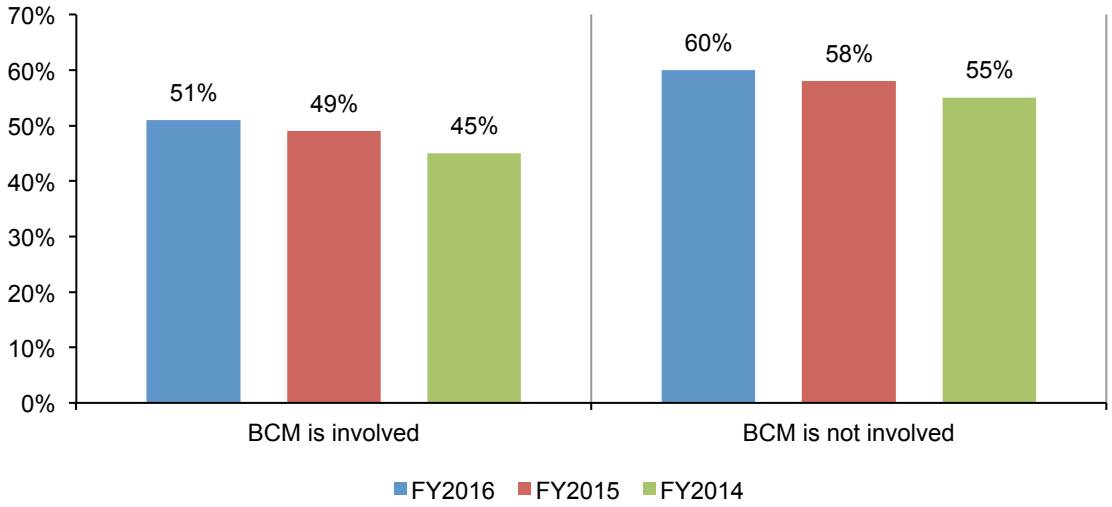
BCM involvement improves the resilience of IT operations. Similar to the above, Figure 12 shows differences between companies with or without BCM involvement with respect to material disruption to IT operations. As reported for FY 2016, 75 percent of companies without BCM involvement said the data breach incident caused a material disruption to IT operations. In contrast, 55 percent of companies with BCM involvement said the incident caused a material disruption. A similar pattern holds true for the past two years.

Figure 12. Did the data breach incident cause a material disruption to IT operations?
Consolidated view (FY 2016=383, FY 2015=350, FY 2014=315)



BCM can protect a company's reputation following a data breach. Figure 13 shows differences between companies that engage BCM versus those that do not. In the current year's study, 60 percent of companies that do not involve BCM said the data breach had a material negative impact on the organization's reputation, brand or marketplace image. In contrast, 51 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 2015 and FY 2014.

Figure 13. Did the data breach have a material negative impact on reputation?
Consolidated view (FY 2016=383, 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. These arise as a result of the 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).

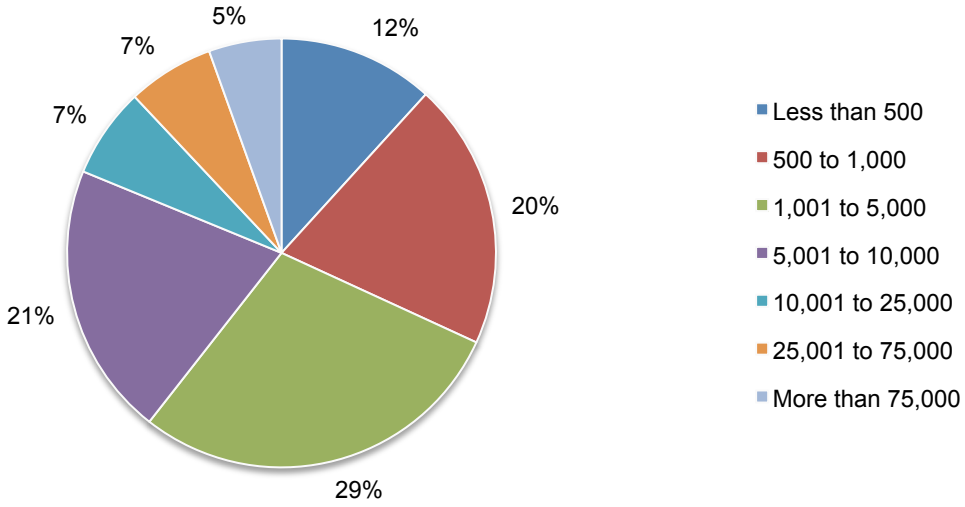
[5]In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector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

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

Part 4. Organizational characteristics and benchmark methods

Pie Chart 3 shows the distribution of all participating benchmarked organizations by total headcount. The largest segments include companies with more than 1,000 full-time equivalent employees.

Pie Chart 4. Global headcount of participating companies
Consolidated view (n=383)



Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number line format.

How to use the number line: The number line provided under each data breach cost category is one way to obtain your best estimate for the sum of cash outlays, labor and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

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

LL	_____|_____	UL

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

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

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

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

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 the 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 costs.

- 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. t 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.