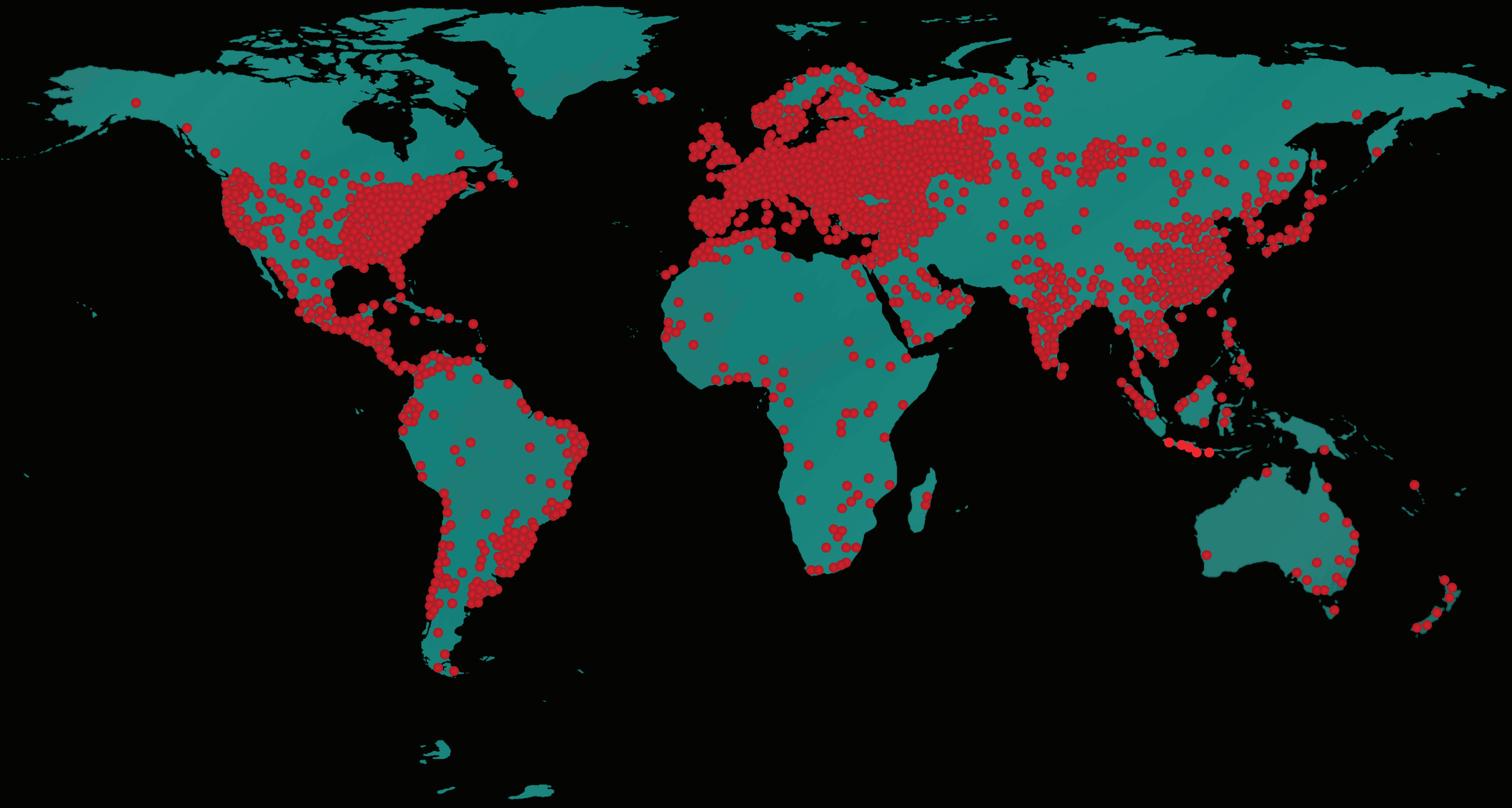
2017 Cost of Data Breach Study

Impact of Business Continuity Management

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2017



Ponemon Institute©
Research Report

2017 Cost of Data Breach Study:

Impact of Business Continuity Management

Ponemon Institute, June 2017

Part 1. Introduction

The *2017 Cost of Data Breach Study: Impact of Business Continuity Management (BCM)* [1], 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 *2017 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 decreased from $158 to $141. The total cost of a data breach decreased from $4 million to $3.62 million.[3] However, despite the decline in the overall cost, companies in this year's study are having larger breaches. The average size (number of lost or stolen records) of the data breaches in this research increased 1.8 percent.

This year's study included 419 companies in 17 industries in the following 11 countries and two regions:

- The United States
- The United Kingdom
- Germany
- Australia
- France
- Brazil
- Japan
- Italy
- India
- Canada
- South Africa
- The Middle East (including the United Arab Emirates and Saudi Arabia)
- ASEAN region (including Singapore, Indonesia, the Philippines and Malaysia)

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

- $10.9 reduction in per capita cost of data breach
- 15.6% reduction in the per capita cost of data breach
- 16.2% reduction in the total cost of data breach
- 43-day reduction in the mean time to identify a data breach
- 35-day reduction in the mean time to contain a data breach
- 28.4% decrease in the likelihood of a data breach over the next 2 years

All participating organizations experienced a data breach ranging from a low of approximately 2,600 to nearly 100,000 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 terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

A material data breach is one that involves a minimum of 1,000 lost or stolen records containing personal information about consumers or customers. This research does not include data breaches involving high-value information assets such as intellectual property, trade secrets and business confidential information.

[1] This report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2016 calendar year.
[2] The BCM teams supporting the incident response process include practitioners in the disaster recovery function.
[3] This year, a strong U.S. dollar significantly influenced the global cost analysis. The conversion from local currencies to the U.S. dollar deflated the per capita and average total cost estimates, especially for companies in the U.K., Germany, France and Italy (e.g., the Pound (£) and Euro (€)). For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost. It is important to note, that this issue only affects the global analysis because all country-level results are shown in local currencies.
[4] The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

By design, we did not recruit organizations that had data breaches involving more than 100,000 compromised records. Specifically, such data breaches as those experienced by Yahoo and Linkedin are not indicative of the data breaches most organizations incur. Thus, including them in the study would have artificially skewed the results.

The majority of companies (54 percent) in the global study have a BCM or disaster recovery (DR) function or team that is involved in enterprise risk management 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.

Why the cost of data breach fluctuates across countries

What explains the significant increases in the cost of data breach this year for organizations in the Middle East, the United States and Japan? In contrast, how did organizations in Germany, France, Australia, and the United Kingdom succeed in reducing the costs to respond to and remediate the data breach? Understanding how the cost of data breach is calculated will explain the differences among the countries in this research.

For the *2017 Cost of Data Breach Study: Global Overview*, we recruited 419 organizations in 11 countries and two regions to participate in this year's study. More than 1,900 individuals who are knowledgeable about the data breach incident in these 419 organizations were interviewed. The first data points we collected from these organizations were: (1) how many customer records were lost in the breach (i.e. the size of the breach) and (2) what percentage of their customer base did they lose following the data breach (i.e. customer churn). This information explains why the costs increase or decrease from the past year.

In the course of our interviews, we also asked questions to determine what the organization spent on activities for the discovery of and the immediate response to the data breach, such as forensics and investigations, and those conducted in the aftermath of discovery, such as the notification of victims and legal fees. A list of these activities is shown in Part 3 of this report. Other issues covered that may have an influence on the cost are the root causes of the data breach (i.e. malicious or criminal attack, insider negligence or system glitch) and the time to detect and contain the incident.

It is important to note that only events directly relevant to the data breach experience of the 419 organizations represented in this research and discussed above are used to calculate the cost. For example, new regulations, such as the General Data Protection Regulation (GDPR), ransomware and cyber attacks, such as Shamoon, may encourage organizations to increase investments in their governance practices and security-enabling technologies but do not directly affect the cost of a data breach as presented in this research.

The calculation of the components of the cost of data breach that affect the cost

The following information presents the data that is used to calculate the cost and the factors that may increase or decrease these costs. We believe such information will help organizations make better decisions about how to allocate resources to minimize the financial consequences when the inevitable data breach strikes.

- **The unexpected and unplanned loss of customers following a data breach (churn rate)**

Programs that preserve customer trust and loyalty in advance of the breach will help reduce the number of lost business/customers. In this year's research, more organizations worldwide lost customers as a result of their data breaches. However, as shown, having a senior-level leader such as a chief privacy officer or chief information security officer who will be able to direct initiatives that improve customers' trust in how the organization safeguards their personal information will reduce churn and the cost of the breach. Organizations that offer data breach victims breach identity protection in the aftermath of the breach are also more successful in reducing churn.

- **The size of the breach or the number of records lost or stolen**

It makes sense that the more records lost, the higher the cost of data breach. Therefore, data classification schema and retention programs are critical to having visibility into the sensitive and confidential information that is vulnerable to a breach and reducing the volume of such information.

- **The time it takes identify and contain a data breach**

The faster the data breach can be identified and contained, the lower the costs. In this year's study, organizations were able to reduce the days to identify the data breach from an average of approximately 201 in 2016 to 191 days and the average days to contain the data breach from 70 to 66 days. We attribute these improvements to investments in such enabling security technologies as security analytics, SIEM, enterprise wide encryption and threat intelligence sharing platforms.

In contrast, security complexity and the deployment of disruptive technologies can affect the time to detect and contain a data breach. Although some complexity in an IT security architecture is expected to deal with the many threats facing organizations, too much complexity can impact the ability to respond to data breaches. Disruptive technologies, access to cloud-based applications and data as well as the use of mobile devices (including BYOD and mobile apps) increase the complexity of dealing with IT security risks and data breaches. As shown in the research, cloud migration at the time of the data breach and mobile platforms were shown to increase the cost.

- **The detection and escalation of the data breach incident**

Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. Investments in governance, risk management and compliance (GRC) programs that establish an internal framework for satisfying governance requirements, evaluating risk across the enterprise and tracking compliance with governance requirements can improve an organization's ability to detect and escalate a data breach.

- **Post data breach costs, including the cost to notify victims**

These costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The United States had the highest notification costs.

The purchase of cyber and data breach insurance can help manage the financial consequences of the incident. As shown in this year's study, insurance protection and business continuity management reduced the cost of data breach following the discovery of the incident. In contrast, the rush to notify victims without understanding the scope of the breach, compliance failures and the engagement of consultants all increase post data breach costs. Expenditures to resolve lawsuits also increase post data breach costs.

BCM provides the following nine important benefits:

1. **Significantly reduces the time to identify and contain the data breach incident.** On average, companies with BCM involvement saved 43 days in the identification of the incident and 35 days in the containment of the data breach (totaling 78 days saved).

2. **BCM is recognized as a valuable addition to data breach incident response planning**. Of the 419 companies in this global study, 226 companies self-reported they have BCM involvement in resolving the consequences of a data breach. Of these companies, 95 percent of these companies rate their involvement as very significant (65 percent) or significant (30 percent).

3. **Significantly reduces the cost of data breach.** The average cost per lost or stolen record can be as high as $152. With BCM involvement the average cost can be as low as $130. Similarly, the average total cost of data breach with BCM involvement was $3.35 million and without BCM was $3.94 million, respectively.

4. **Results in substantial per day cost savings.** Companies that involve BCM or the disaster recovery (DR) team in the response to data breach achieve an average per day savings of $5,064 – or total incremental cost savings of $394,922 – through the containment phase of the data breach response.

5. **Reduces the likelihood of having recurring data breaches.** If BCM is not involved in data breach planning and execution, the likelihood of having a data breach sometime over the next 2 years is 31.8 percent. Whereas, if BCM is involved this likelihood drops to 23.9 percent.

6. **Minimizes disruptions to business operations when a data breach occurs**. According to the findings, 76 percent of companies without BCM involvement had a material disruption to business operations. This decreases to 55 percent for companies involving BCM in advance of the data breach.

7. **Improves the resilience of IT operations**. Seventy-two percent of companies without BCM involvement said they had a material disruption to their IT operations. In contrast, 56 percent of those with BCM involvement said IT operations were materially disrupted.

8. **Diminishes the negative impact on the company's reputation following a material data breach**. Specifically, 52 percent of companies with BCM involvement said their reputation or brand had been negatively impacted because of a data breach. However, 62 percent of companies without BCM involvement said their organization's brand and reputation was negatively affected.

9. **BCM involvement reduces the average per day cost of a data breach.** In this year's study, the average data breach cost per day for companies in the BCM group is $4,222. In contrast, non-BCM companies have a much higher average per day cost of $6,050. The overall average cost per day for all 419 companies is $5,064.

10. **DR automation and orchestration reduces the per day cost of a data breach.** BCM companies that have a manually operated DR process experienced an estimated average cost of $5,015 per day. In contrast, BCM companies deploying an automated DR process that provides resiliency orchestration experienced a much lower average cost per day of $3,360. This represents a net difference of 39.5 percent (or a cost savings of $1,655 per day).

Part 2. Key Findings

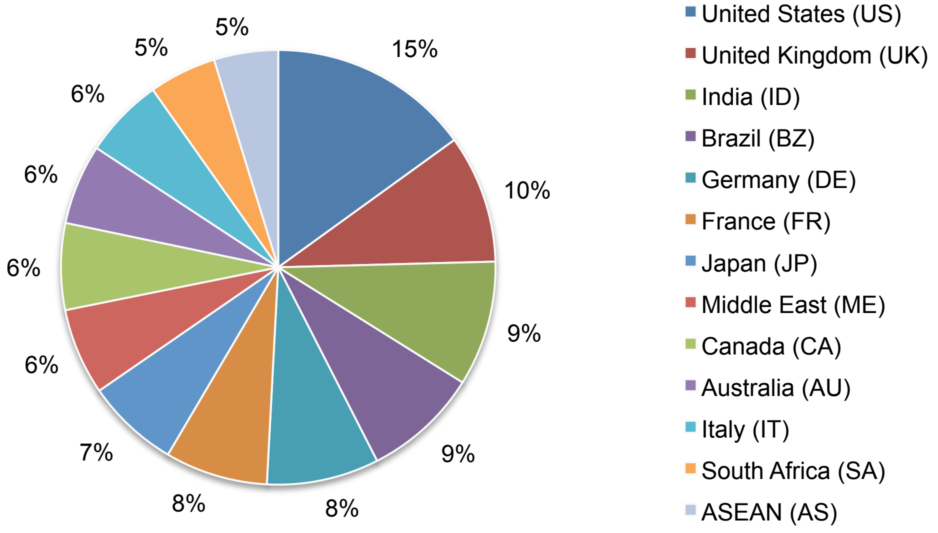
The following table lists 11 countries and two regions, legend, sample sizes and currencies used in this global study. It also shows the number of years of annual reporting for each country ranging from one year for ASEAN companies to 12 years for the United States.

Legend	Countries	Sample	Pct%	Currency	Years of study
US	United States	63	15%	US Dollar	12
UK	United Kingdom	40	10%	GBP	10
ID	India	39	9%	Rupee	6
BZ	Brazil	36	9%	Real	5
DE	Germany	35	8%	Euro	9
FR	France	32	8%	Euro	8
JP	Japan	29	7%	Yen	6
ME	Middle East*	27	6%	AED/SAR	4
CA	Canada	27	6%	CA Dollar	3
AU	Australia	25	6%	AU Dollar	8
IT	Italy	25	6%	Euro	6
SA	South Africa	21	5%	ZAR	2
AS	ASEAN#	20	5%	SGD	1
	Total	419	100%		

*ME is a combined sample of companies located in Saudi Arabia and the United Arab Emirates
#ASEAN includes Singapore, Indonesia, Philippines and Malaysia

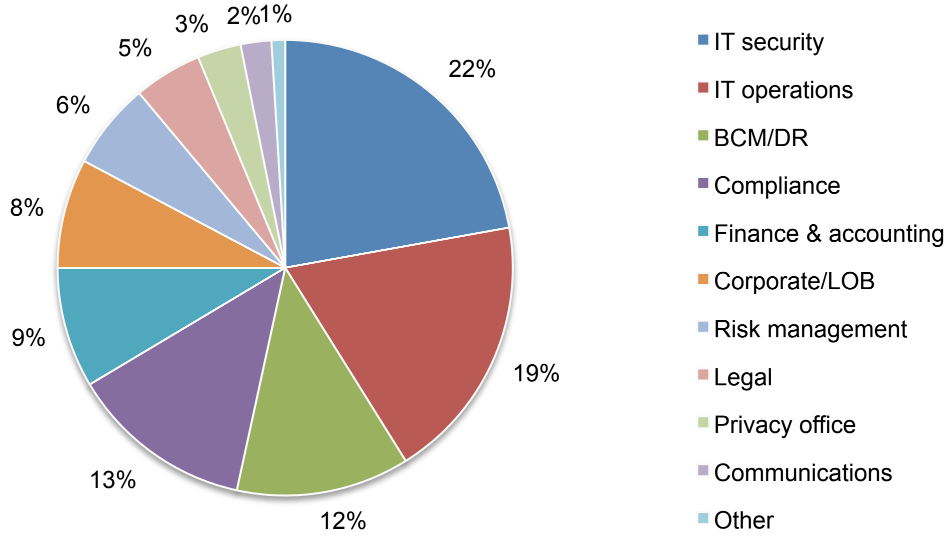
The following chart shows the distribution of 419 participating organizations within 11 countries and two regional samples. As can be seen, the US represents the largest segment with 63 organizations and ASEAN represents the smallest sample with 20 organizations.

Pie Chart 1. Percentage frequency of benchmark samples by country
Consolidated view (n=419)



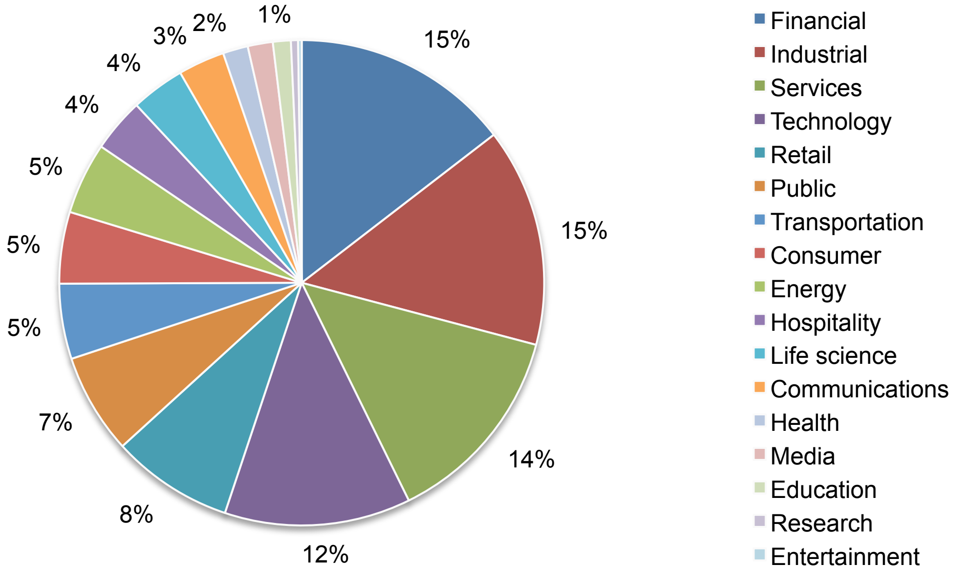
Pie Chart 2 shows the distribution of 2,065 individuals who participated in interviews, representing 419 organizations within 11 countries and two regional samples. Twenty-two percent of interviewees are located in IT security (e.g., SecOps), followed by 19 percent who are located in IT operations.

Pie Chart 2. Percentage frequency of interviewees who participated in the study by functional location
Consolidated view (n=2.065)



The following chart provides the industry distribution of 419 companies that participated in this year's study. Pie Chart 3 shows the percentage distribution across 17 industry sectors. The largest segments include financial services, industrial and services.

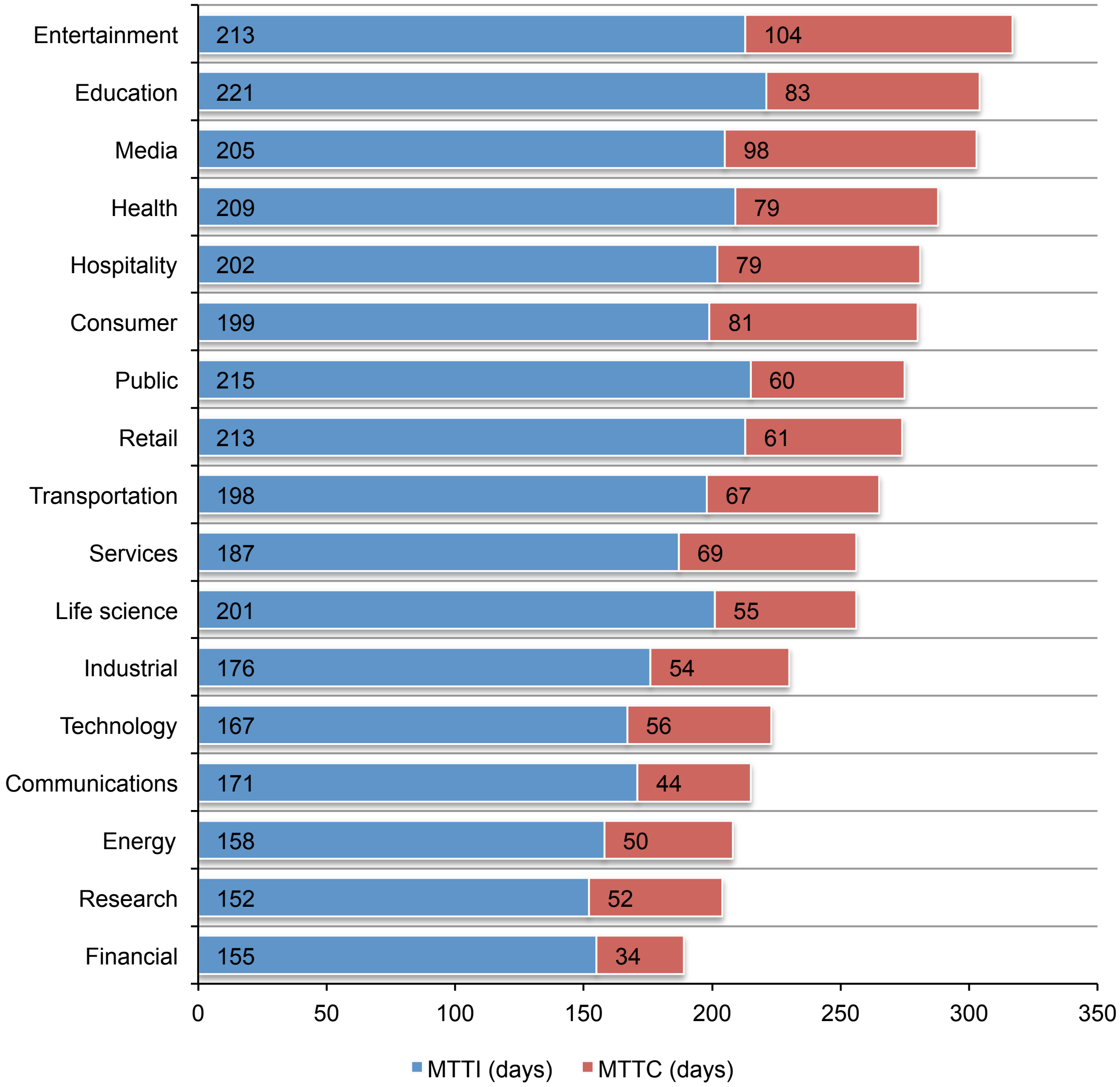
Pie Chart 3. Percentage frequency of benchmark samples by industry
Consolidated view (n=419)



The faster the data breach can be identified and contained, the lower the costs. MTTI and MTTC metrics are used to determine the effectiveness of an organization's incident response and containment processes. The MTTI metric helps organizations to understand the time it takes to detect that an incident has occurred and the MTTC metric measures the time it takes to contain it.

Figure 1 shows the MTTI and MTTC across 17 industry sectors. As can be seen, the MTTI and MTTC vary across industries. In this year's study, for our consolidated sample of 419 companies, the MTTI averaged 191 days. The MTTC averaged 66 days with a range of 10 to 164 days. Companies in the education industry had the longest MTTI at 221 days. Companies in the entertainment industry had the longest MTTC at 104 days. In contrast, companies in the research sector had the shortest MTTI at 152 days, and financial service companies had the shortest MTTC at 34 days.

Figure 1. Average days to identify and contain a data breach by industry
Consolidated view (n=419)



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 2 shows the days to identify the data breach are lower for organizations that involved BCM; namely, a time saving of 43 days in FY 2017, 52 days in FY 2016 and 56 days in FY 2015. In percentage terms over the past year, MTTI decreased by 3 percent for companies in the BCM group and decreased 6 percent for the non-BCM group.

Figure 2. MTTI for organizations that involve or fail to involve BCM in the incident response process
MTTI differences (FY 2017=43 days, FY 2016=52 days, FY 2015=56 days)
Consolidated view (FY 2017=419, FY 2016=383, FY 2015=350)

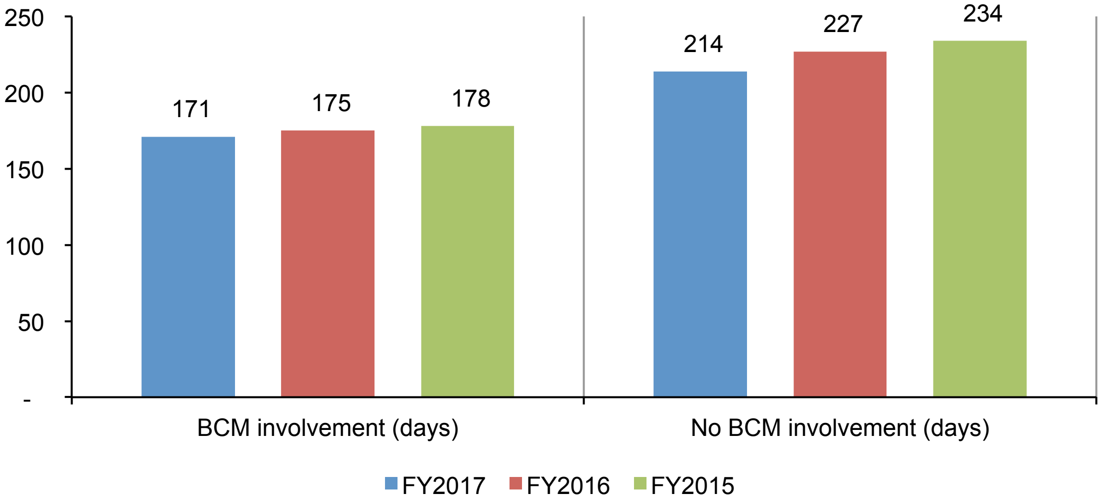


Figure 3 shows a similar relationship. That is, days to contain the data breach incident were substantially lower for organizations that involved BCM, or a time saving of 35 days (85-50 days) in FY 2017, 36 days in FY 2016 (88-52 days) and 28 days in FY 2015 (83-50 days). In percentage terms over the past year, MTTC decreased by 4 percent for companies in the BCM group and 3 percent for the non-BCM group.

Figure 3. MTTC for organizations that involve or fail to involve BCM in the incident response process
MTTC differences (FY 2017=35 days, FY 2016=36 days, FY 2015=28 days)
Consolidated view (FY 2017=419, FY 2016=383, FY 2015=350)

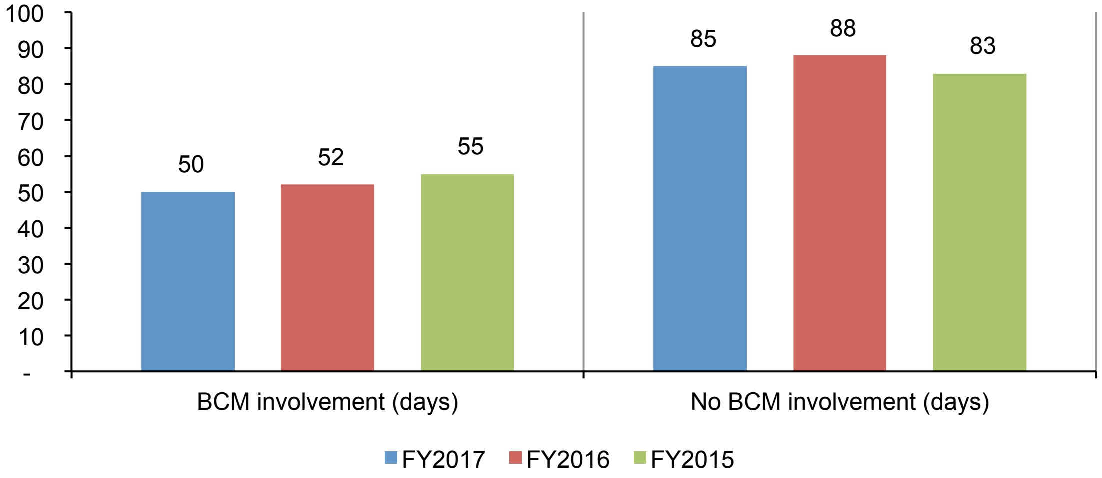
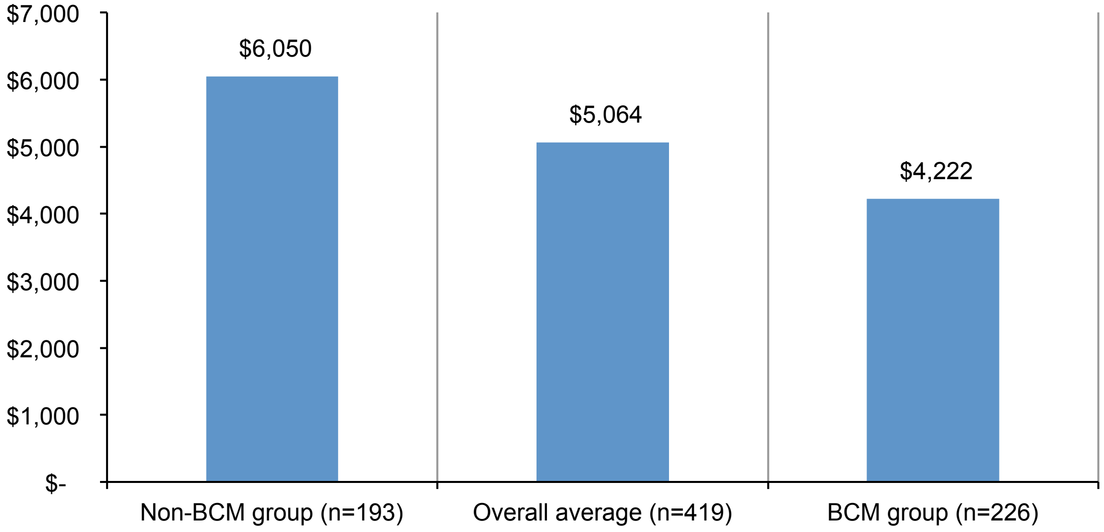


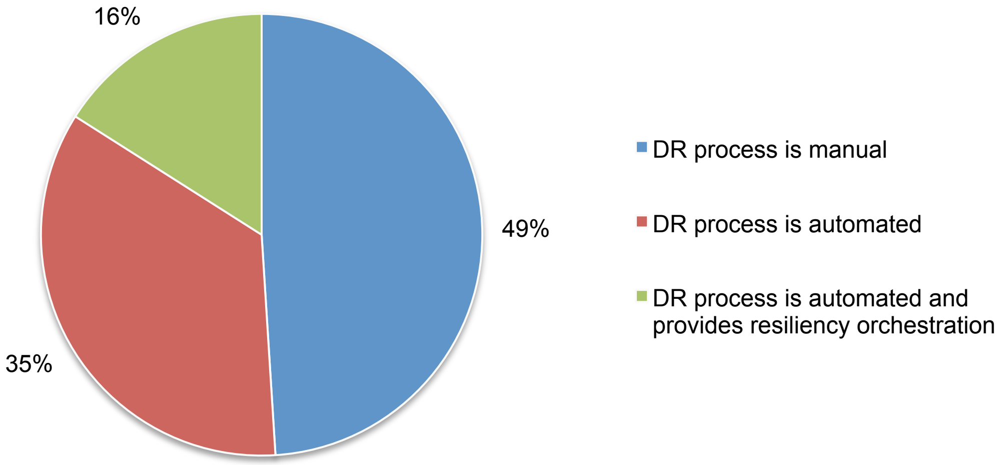
Figure 4 provides the extrapolated cost per day that result from MTTI and MTTC inefficiencies. As can be seen, 193 companies that do not involve BCM achieved an average cost per day savings of $6,050, and the average cost per day for all 419 companies is $5,064. In contrast, the average cost per day for the BCM group is much lower at $4,222.

Figure 4. Cost per day for BCM and non-BCM companies
Consolidated view (Overall n=419; BCM group=226; non-BCM group=193)
Measured in US$



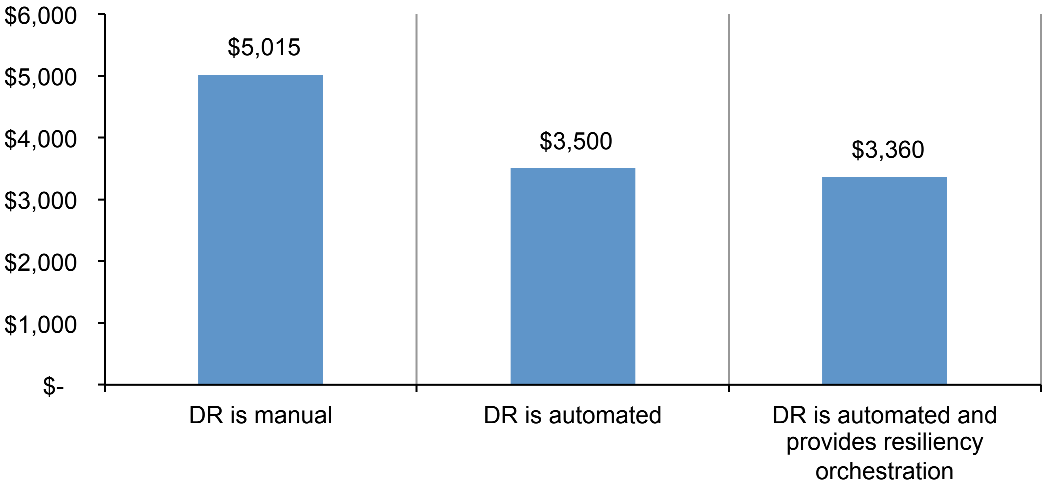
Manual vs. automated disaster recovery (DR) processes. As shown in Pie Chart 4, nearly half (49 percent) of our sample of benchmarked companies deploys manual DR procedures. Another 35 percent said their company was deploying a DR process that is primarily automated. Only 16 percent of companies' DR process are automated and provides resiliency orchestration.

Pie Chart 4. Percentage frequency by the type of DR process deployed by benchmarked companies
Consolidated view (BCM Group=256)



DR automation and orchestration reduces the per day cost of a data breach. Figure 5 shows the cost impact of DR processes. The overall average data breach cost per day for BCM companies is estimated at $4,222. BCM companies that have a manually operated DR process experienced an estimated average cost of $5,015 per day. In contrast, companies with an automated DR process that provides resiliency orchestration experienced a much lower average cost per day of $3,360. This represents a net difference of 39.5 percent (or a cost savings of $1,655 per day).

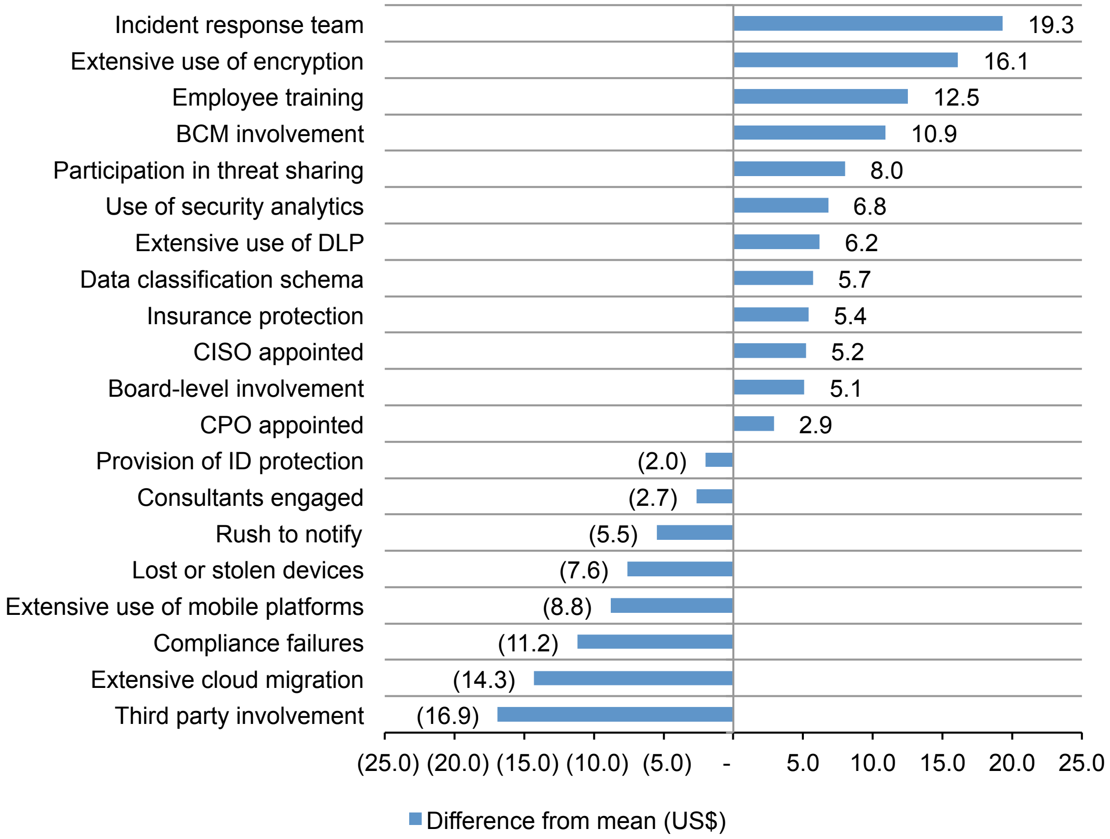
Figure 5. The impact of DR process on cost per day
Consolidated view (BCM Group=226)
Measured in US$



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 20 factors. The extensive use of DLP is particularly important in preventing data exfiltration from insiders and can reduce the average cost of data breach by $6.2. However, the rush to notify can increase costs (an average of $5.5) when organizations have not determined the extent of the breach and make mistakes in notifying regulators and potential victims of the incident. Further, if the breach occurs during an extensive cloud migration there is additional complexity in understanding the types of data lost or stolen.

As shown in Figure 6, the existence of a strong incident response team resulted in the greatest reduction in the per capita cost of data breach. Business continuity management decreased the cost of data breach by an average of $10.9 per compromised record.

Figure 6. Impact of 20 factors on the per capita cost of data breach
Measured in US$ consolidated view (n=419)



BCM's contribution to incident response planning. Figure 7 provides a summary of BCM involvement in the data breach incident response planning and execution. Of the 419 companies in this global study, 226 or 54 percent had BCM involvement. The remaining 193 companies did not involve their BCM team or only involved BCM on an ad hoc basis. Last year's analysis showed 52 percent of companies involved BCM in the data breach incident response.

Figure 7. How does BCM contribute to the data breach incident response process?
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)

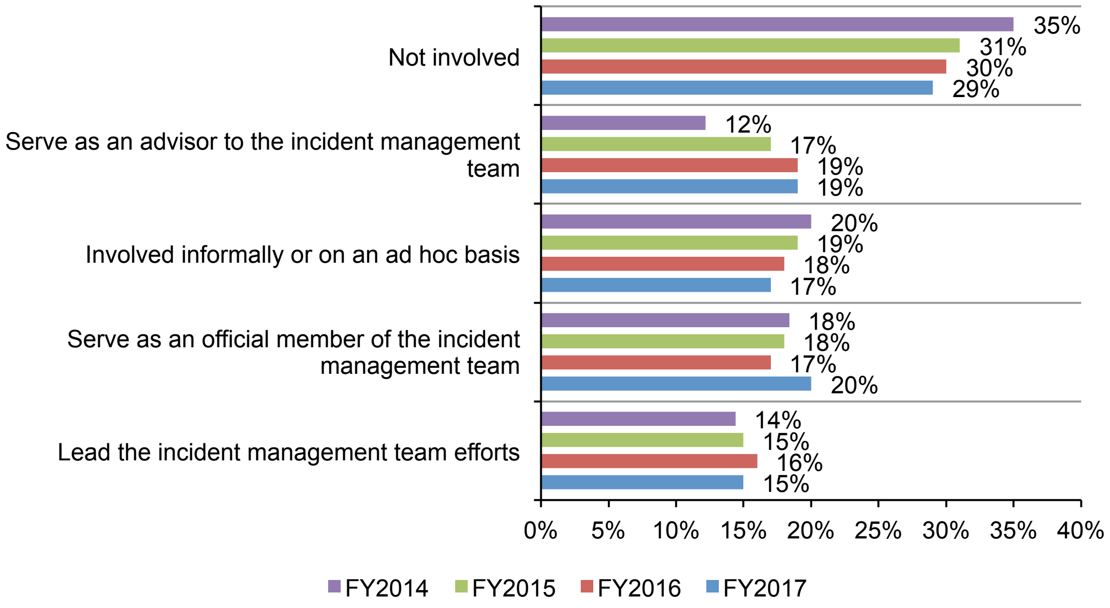
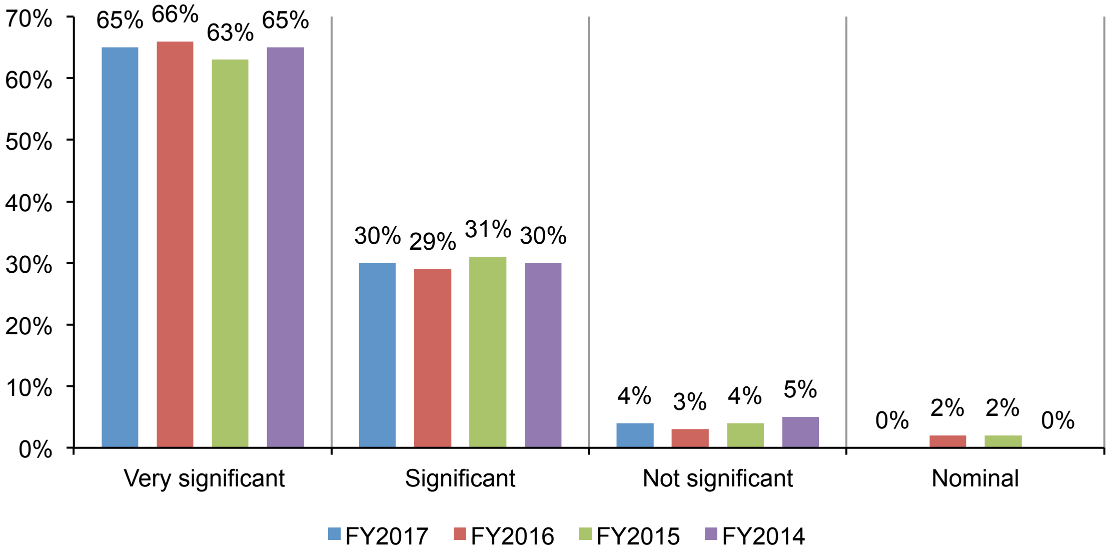


Figure 8 shows the level of BCM involvement in incident response planning and execution. For this year's study, 65 percent of companies rate this involvement as very significant. Another 30 percent rate BCM involvement as significant. Last year's study showed that 66 and 29 percent rated BCM involvement as very significant or significant, respectively.

Figure 8. What best describes BCM's contribution to the incident response process?
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)



BCM reduces the per capita cost of data breach. Figure 9 reports the average per capita cost of data breach over three years for companies that involved the BCM team in incident response planning and execution, and those that did not. Those companies involving BCM experienced a lower per capita cost than those that did not involve BCM. In this year's study, the difference in the per capita cost of data breach between companies that did and did not involve BCM is ± $10.9. In percentage terms over the past year, per capita cost decreased by 14 percent for companies in the BCM group and 9 percent for the non-BCM group.

Figure 9. Per capita cost of data breach for companies with or without BCM involvement
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)

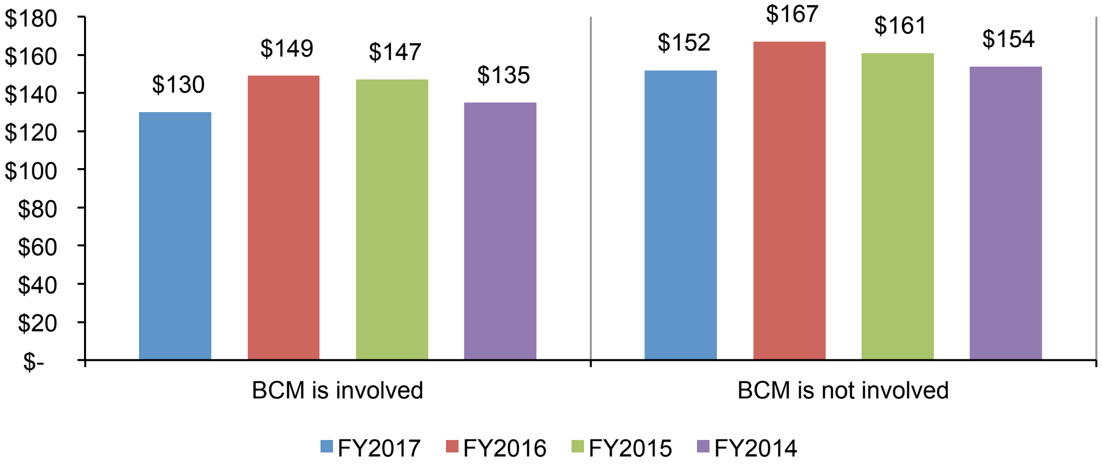
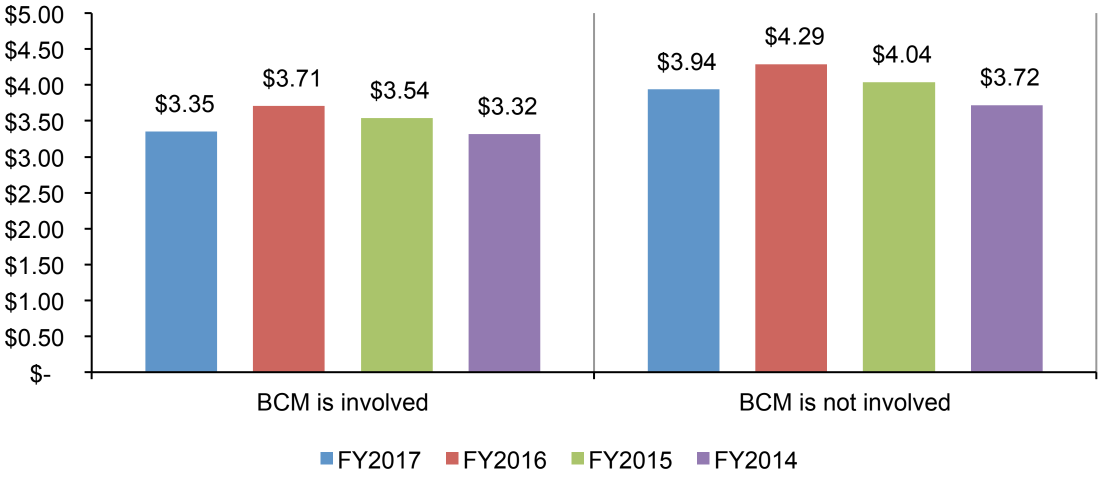


Figure 10 reports the total cost of data breach over three years for companies that involved the BCM team in incident response planning and execution and those that did not. Similar to the above, those companies involving BCM experienced a lower total cost of data breach than those that did not involve BCM. In this year's study, the difference in the total cost between companies that did and did not involve BCM is more than $590,000. In percentage terms over the past year, per capita cost decreased by 10 percent for companies in the BCM group and 9 percent for the non-BCM group.

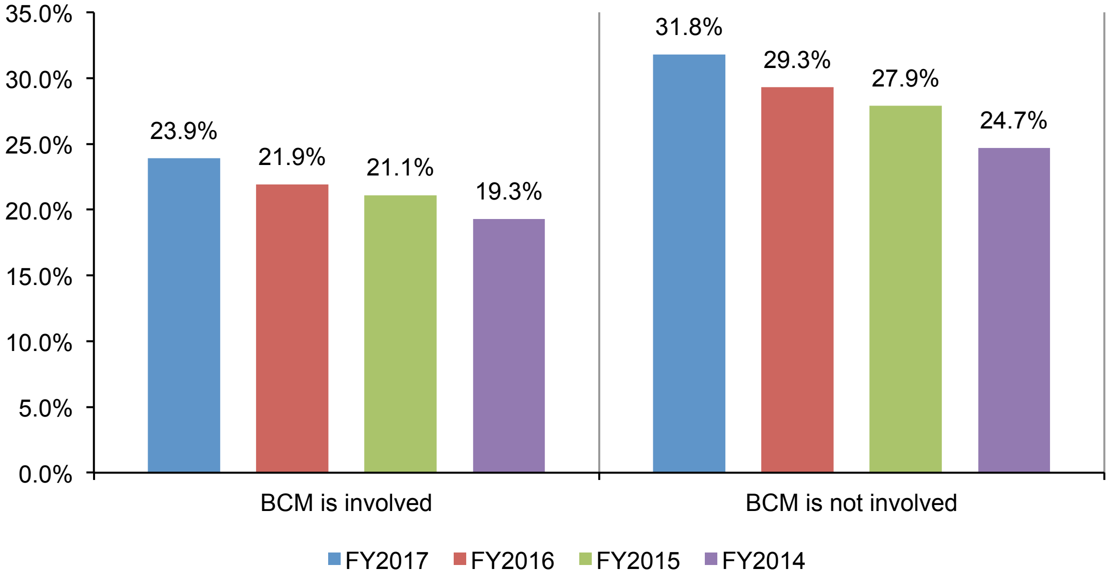
Figure 10. Total cost of data breach for companies with or without BCM involvement
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)
US$ millions



BCM reduces the likelihood of a data breach. Figure 11 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.

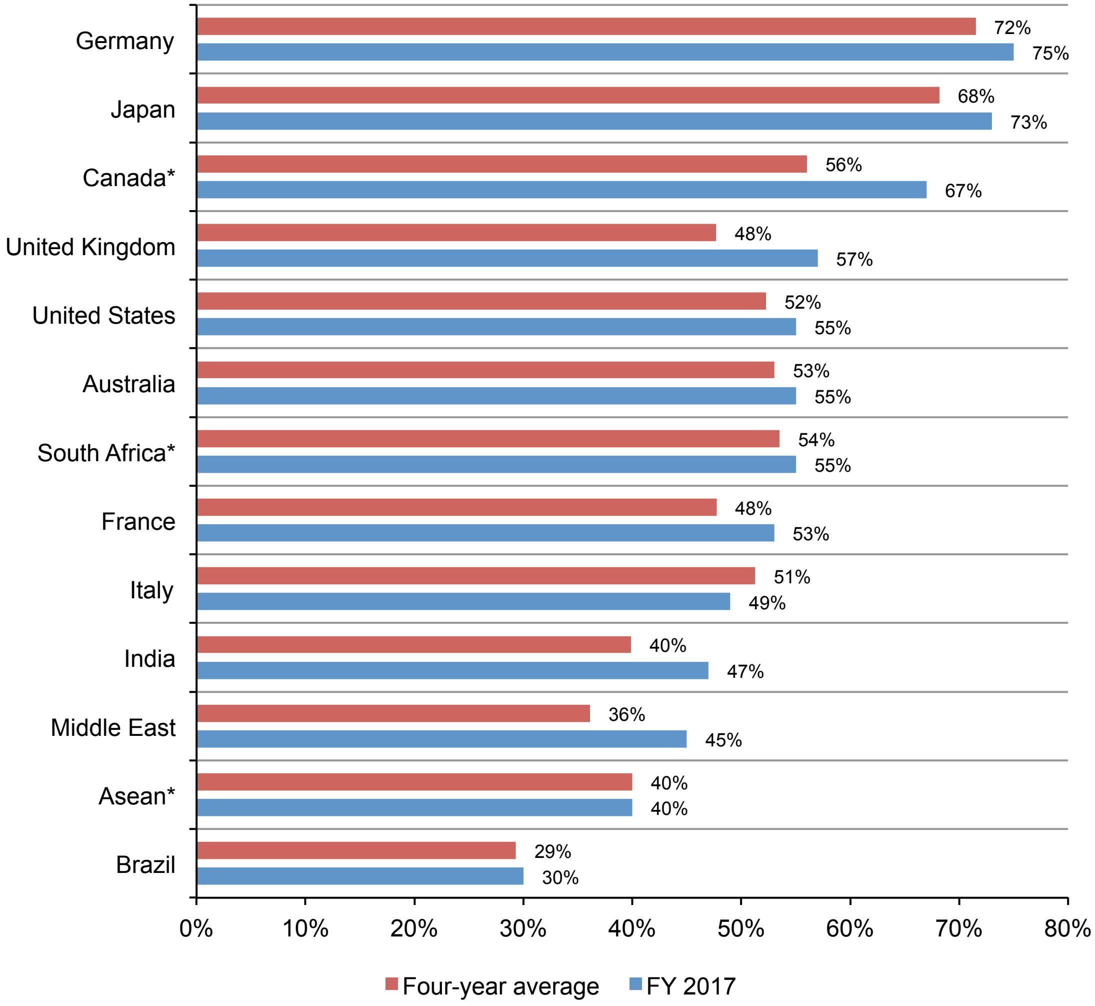
Over the past four years, we found that organizations that involved the BCM team experienced a lower likelihood of incurrence than those that did not involve BCM. In this years study, the difference in the likelihood of a future data breach between companies that did and did not involve BCM is 7.9 percent. In percentage terms over the past year, the probability of data breach increased by 8.7 percent for companies in the BCM group and 8.2 percent for the non-BCM group.

Figure 11. Likelihood of a material data breach for companies with or without BCM involvement over the next 24 months
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)



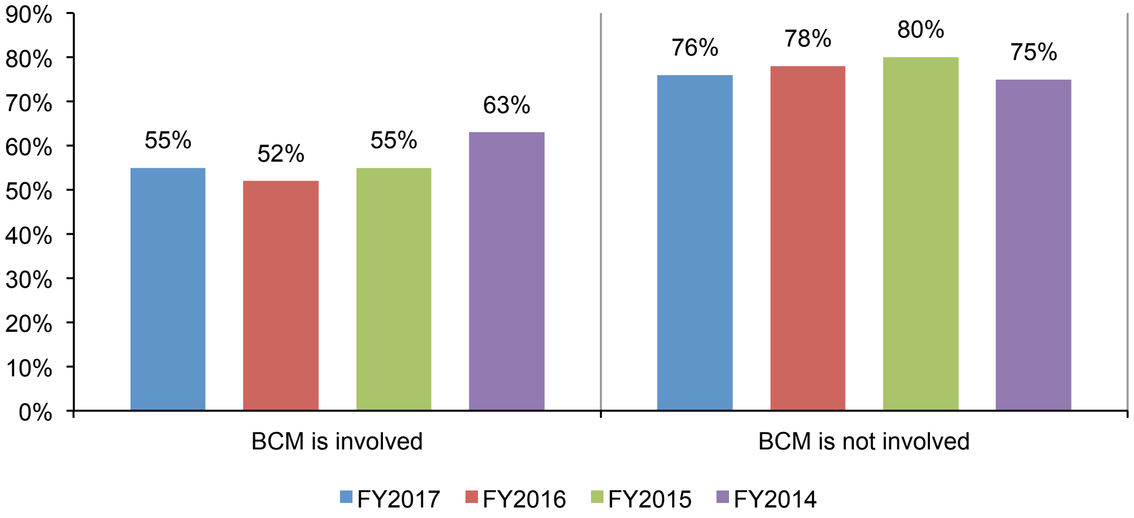
Germany and Japan are most likely to involve BCMs when dealing with data breaches. Figure 12 shows the percentage of BCM team involvement in incident planning and execution for country and regional samples. Similar to the last three years, Germany had the highest rate of BCM involvement with 75 percent of German companies reporting they had a BCM or DR team in place. In contrast, only 30 percent of Brazilian companies had BCM involvement.

Figure 12. BCM participation rate by country sample versus four-year average
Consolidated view (FY 2017=419, FY 2016=383 FY 2015=350, FY 2014=315)
*Historical data are not available for all years



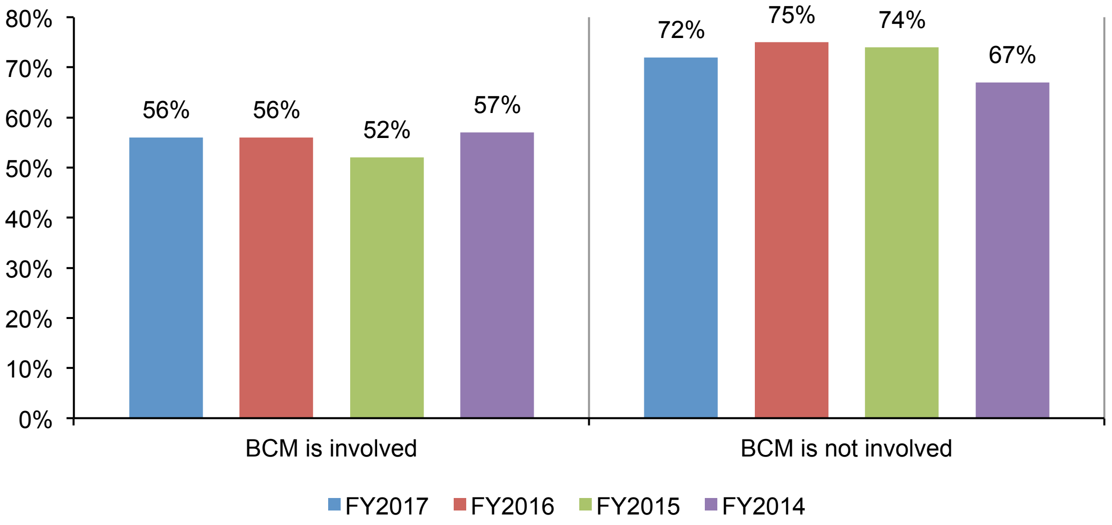
BCM minimizes disruptions to business operations when a data breach occurs. Figure 13 reveals differences between companies with or without BCM involvement with respect to material disruption to business processes. As reported for FY 2017, 76 percent of companies without BCM involvement said the data breach incident caused a material disruption to their business process. However, 55 percent of companies with BCM involvement said they had a material disruption. A consistent pattern holds true for all four years.

Figure 13. Did the data breach cause a material disruption to business processes?
Consolidated view (FY 2017=419, FY 2016=383, FY 2015=350, FY 2014=315)



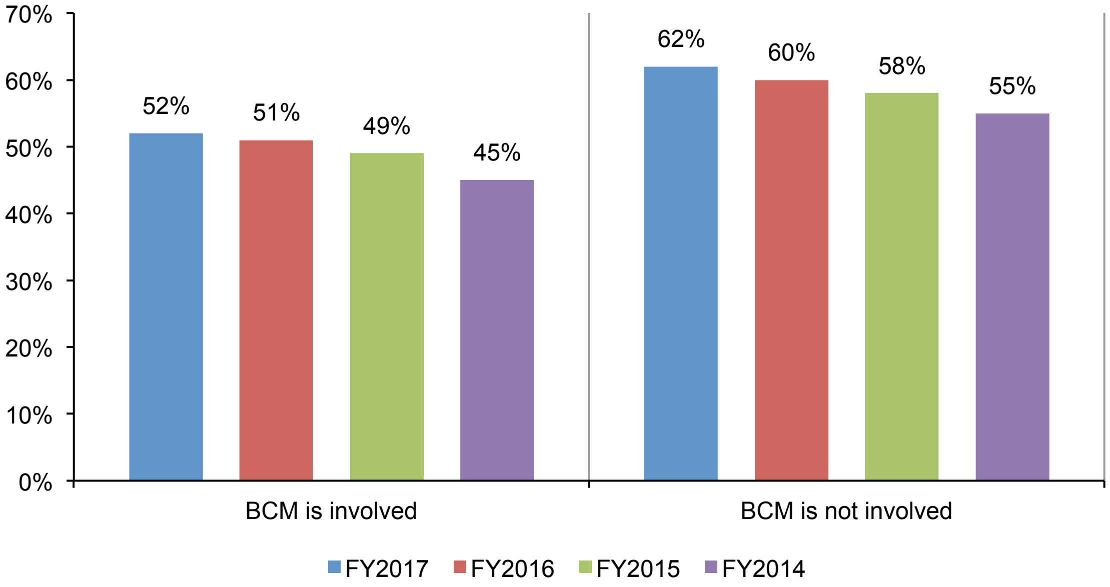
BCM involvement improves the resilience of IT operations. Similar to the above, Figure 14 shows differences between companies with or without BCM involvement with respect to material disruption to IT operations. As reported for FY 2017, 72 percent of companies without BCM involvement said the data breach incident caused a material disruption to IT operations. In contrast, 56 percent of companies with BCM involvement said the incident caused a material disruption. A consistent pattern holds true for the past four years.

Figure 14. Did the data breach incident cause a material disruption to IT operations?
Consolidated view (FY 2017=419, FY 2016=383, FY 2015=350, FY 2014=315)



BCM can protect a company's reputation following a data breach. Figure 15 shows differences between companies that engage BCM versus those that do not. In the current year's study, 62 percent of companies that did not involve BCM said the data breach had a material negative impact on the organization's reputation, brand or marketplace image. In contrast, 52 percent of companies that involved BCM said the incident had a negative impact on the organization's reputation or brand. A consistent pattern holds true for all four years.

Figure 15. Did the data breach have a material negative impact on reputation?
Consolidated view (FY 2017=419, 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).

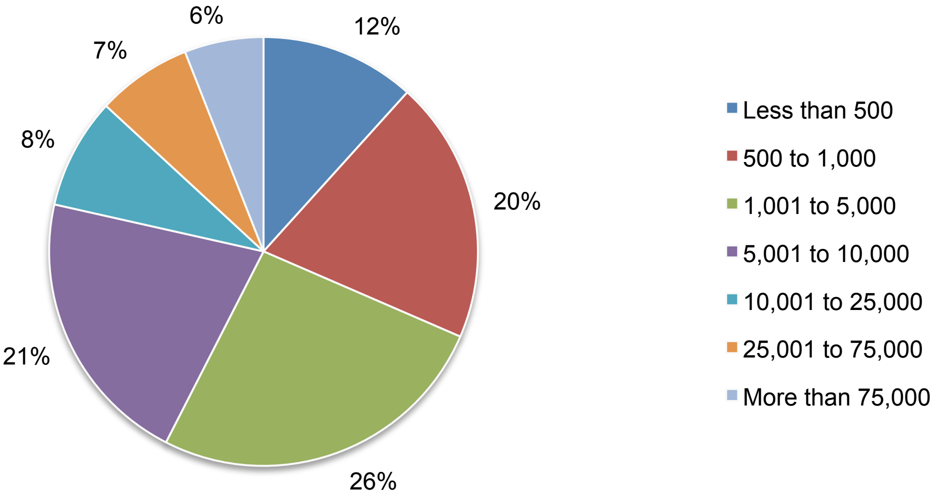
[5] In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organization, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector 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 5 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 5. Global headcount of participating companies
Consolidated view (n=419)



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, 419 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. The research process requires individuals to use categorical or aggregated response variables to disclose demographic information about the company and the individual respondent.

- 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.

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.