Ponemon INSTITUTE

2018 Cost of Data Breach Study: **Impact of Business Continuity Management**

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC

October 2018

IBM

Part 1. Introduction

The 2018 Cost of Data Breach Study: Impact of Business Continuity Management (BCM)[1] sponsored by IBM, analyses 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 (MTTI) and the mean time to contain (MTTC) a data breach and the likelihood of experiencing such an incident over the next two years.[2]

The purpose of the study is to demonstrate the economic value of BCM when dealing with data breach incidents. The BCM study has been conducted over four consecutive years and during this period the research has consistently shown the following trends when companies have incorporated BCM into their data breach response:

- Decreases the time to identify the data breach
- Decreases the time to contain the data breach
- Decreases the likelihood of a future breach

The cost of data breach research has been conducted for 13 consecutive years. Two new countries were added to this year's study: South Korea and Turkey. This year's study included 477 companies in 17 industries in the following 13 countries and two regions:

- ASEAN
- Australia
- Brazil
- Canada
- France
- Germany
- India
- Italy
- Japan
- The Middle East
- South Africa
- South Korea
- Turkey
- The United Kingdom
- The United States

The Impact of BCM Programs on the Cost of Data Breach

- **USD9.3** reduction in per capita cost of data breach
- **6.5 percent** reduction in the per capita cost of data breach
- **44** day reduction in the mean time to identify a data breach
- **38** day reduction in the mean time to contain a data breach
- **31** day reduction in the mean time to recover (MTTR) from a data breach
- **32 percent** decrease in the likelihood of a data breach over the next two years
- **31.5** percentage cost per day differential between companies that involve BCM and those that do not

[1]This report is dated in the year of publication rather than by the fieldwork completion date. Please note that the majority of data breach incidents studied in this report happened in the 2017 calendar year.

[2]The BCM teams supporting the incident response process include practitioners in the disaster recovery function.

Companies in the ASEAN sample include those located in Singapore, Indonesia, the Philippines and Malaysia. The Middle East region combines companies in Saudi Arabia and the United Arab Emirates.

All participating organisations experienced a data breach ranging from a low of approximately 2,500 to nearly 100,000 compromised records[3]. 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. By design, we did not recruit organisations that had data breaches involving more than 100,000 compromised records. Specifically, such data breaches as those experienced by Equifax, Facebook and others are not indicative of the data breaches most organisations experience. Thus, including them in the study would have skewed our results.

A total of 262 companies (55 percent) in our global sample have a BCM or disaster recovery (DR) function or team that is somewhat involved in enterprise risk 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.

For the 2018 Cost of Data Breach Study: Global Overview, we recruited 477 organisations in 13 countries and two regions to participate in this year's study. A total of 2,634 individuals who are knowledgeable about the data breach incident in these 477 organisations were interviewed. The first data points we collected from these organisations 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 organisation 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 477 organisations represented in this research and discussed above are used to calculate the cost. For example, new regulations and/or targeted cyber attacks may encourage organisations 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 organisations make better decisions about how to allocate resources to minimise the financial consequences when the inevitable data breach strikes.

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

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

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 organisations 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 organisation safeguards their personal information, will reduce churn and the cost of the breach. Organisations that offer data breach victims identity protection 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 to 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, organisations experienced an increase in the number of days to identify the data breach from an average of approximately 191 in 2017 to 197 days. The average days to contain the data breach increased from 66 to 69 days. We attribute the increase in days to the growth in the use of IoT devices, extensive use of mobile platforms, increased migration to the cloud and compliance failures.

> 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 /organisation and tracking compliance with governance requirements can improve an organisation'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 due to numerous regulations requiring disclosure to data breach victims and regulators.

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 an average of USD4 per record. 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.

What's new in this year's Cost of Data Breach research?

The Cost of Data Breach research now includes a framework for measuring the cost of mega breaches, which are breaches involving one million or more compromised records. We also added a special analysis of the cost to recover from a data breach. This analysis was conducted on a subset of the overall sample.[4]

[4]The MTTR was estimated from a subsample of 56 companies that experienced a data breach in both the FY2017 and FY2016 timeframe. This variable contains costs up to one year after data breach containment.

BCM provides the following 10 important benefits:

1. **Significantly reduces the time to identify and contain the data breach incident because of a more structured and disciplined approach to responding to adverse events**. Lessons learned from a BCM program can be applied to the management of a data breach response. On average, companies with BCM involvement saved 44 days in the identification of the incident and 38 days in the containment of the data breach (totaling 82 days saved).

2. **BCM is recognised as a valuable addition to data breach incident response planning**. Of the 477 companies in this global study, 262 companies self-reported they have BCM involvement in resolving the consequences of a data breach. Of these companies, 98 percent of these companies rate their involvement as very significant (68 percent) or significant (30 percent).

3. **Significantly reduces the cost of a data breach**. Without BCM involvement, the average cost of a data breach was USD157 per record. With BCM involvement the average cost was USD139. Similarly, the average total cost of data breach without BCM involvement was USD4.24 million and with BCM was USD3.55 million.

4. **BCM saves costs per day**. Companies that involve BCM or the DR team in the response to data breach achieve an average per day savings of USD5,703[5] – or total incremental cost savings of USD467,657[6] – through containment 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 two years is 32.3 percent. Whereas, if BCM is involved this likelihood drops to 23.4 percent, a decrease of 32 percent in the likelihood of a breach recurring.

6. **Minimises 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 56 percent for companies involving BCM in advance of the data breach.

7. **Improves the resilience of IT operations**. Sixty-nine percent of companies without BCM involvement said they had a material disruption to their IT operations. In contrast, 58 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, 50 percent of companies with BCM involvement said their reputation or brand had been negatively impacted because of a data breach. However, 65 percent of companies without BCM involvement said their organisation'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 USD4,881. In contrast, non-BCM companies had a much higher average per day cost of USD6,705. The overall average cost per day for all 477 companies is USD5,703.

10. **DR automation and orchestration[7] reduces the per day cost of a data breach**. BCM companies that have a manually operated DR process experienced an estimated average cost of USD6,546 per day. In contrast, BCM companies deploying an automated DR process that provides resiliency orchestration experienced a much lower average cost per day of USD3,100. This represents a cost savings of USD3,446 per day.

[5]Based on a weighted average
[6]Calculation is 82 days x USD5,703 per diem.
[7]Automation is the process of codifying a set of manual DR steps via the creation of scripts that drive singular actions at component levels. Orchestration is the creation of an intelligent DR workflow comprised of individual automated actions with an awareness of the entire process.

Part 2. Key Findings

Table 1 lists 13 countries and two regions, a legend, the sample sizes and the local currencies used in this global study. It also shows the number of years of annual reporting for each country, ranging from one year for Turkish and South Korean companies to 13 years for the United States.

Table 1. Global study at a glance

Legend	Country	Sample	Pct%	Currency	Years of study
US	United States	65	14%	US Dollar	13
ID	India	43	9%	Rupee	7
UK	United Kingdom	42	9%	GBP	11
BZ	Brazil	37	8%	Real	6
DE	Germany	35	7%	Euro	10
JP	Japan	32	7%	Yen	7
FR	France	31	6%	Euro	9
CA	Canada	28	6%	CA Dollar	4
ME	Middle East*	28	6%	AED/SAR	5
IT	Italy	26	5%	Euro	7
SK	South Korea	25	5%	Won	1
AU	Australia	24	5%	AU Dollar	9
TY	Turkey	21	4%	TRY	1
AS	ASEAN#	20	4%	SGD	2
SA	South Africa	20	4%	ZAR	3
	Total	**477**	**100%**		

*ME is a cluster sample of companies located in Saudi Arabia and the United Arab Emirates

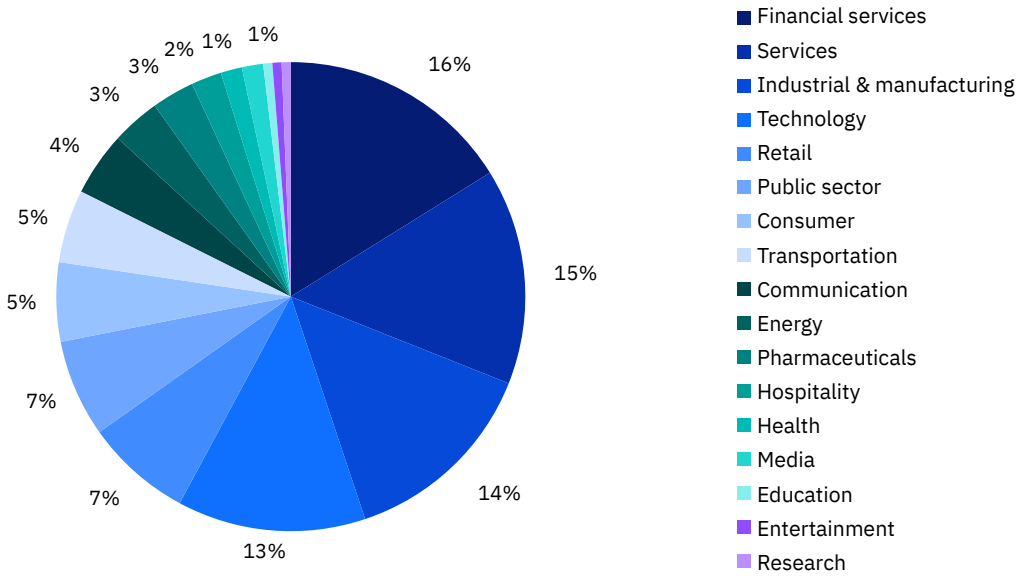
#ASEAN is a cluster sample of companies located in Singapore, Indonesia, the Philippines and Malaysia.

Pie Chart 1 presents the frequency of data breaches by primary industry classification. The industries represented include: financial services (FS), services (SV), industrial manufacturing (IM), technology (TC), retail (RT), public sector (PS), consumer (CN), transportation (TP), communications (CM), energy (EU), pharmaceuticals (PH), hospitality (HP), healthcare (HC), media (MD), education (ED), entertainment (ET) and research (RS).

Seventeen industries were represented in this year's study. The largest sectors were financial, services and industrial and manufacturing companies. Financial service companies include banks, insurance, investment management, brokerage and payment processors.

Pie Chart 1. Distribution of the sample by industry

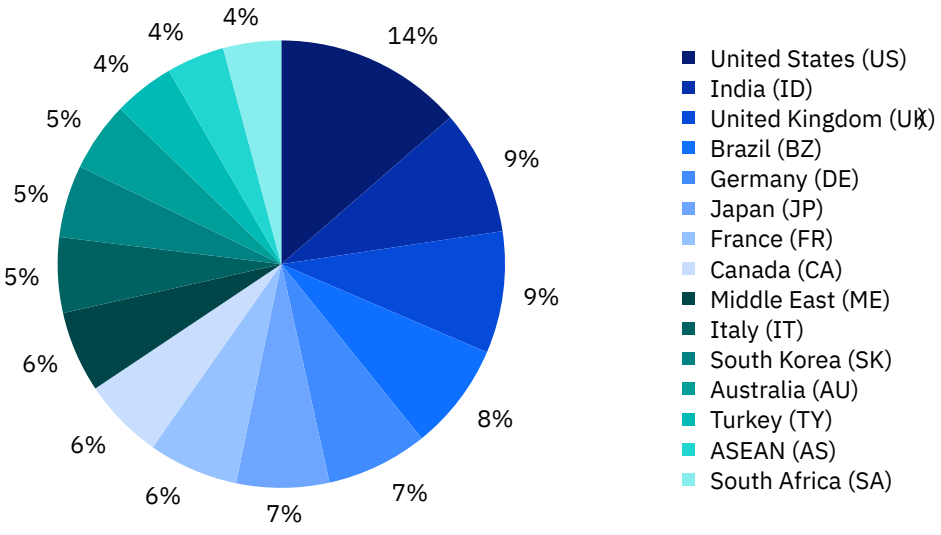
Consolidated view (n = 477)



Pie Chart 2 shows the distribution of 477 participating organisations within 13 countries and two regions. As can be seen, the US represents the largest segment with 65 organisations and ASEAN and South Korea represent the smallest samples each with 20 organisations.

Pie Chart 2. Percentage frequency of benchmark samples by country

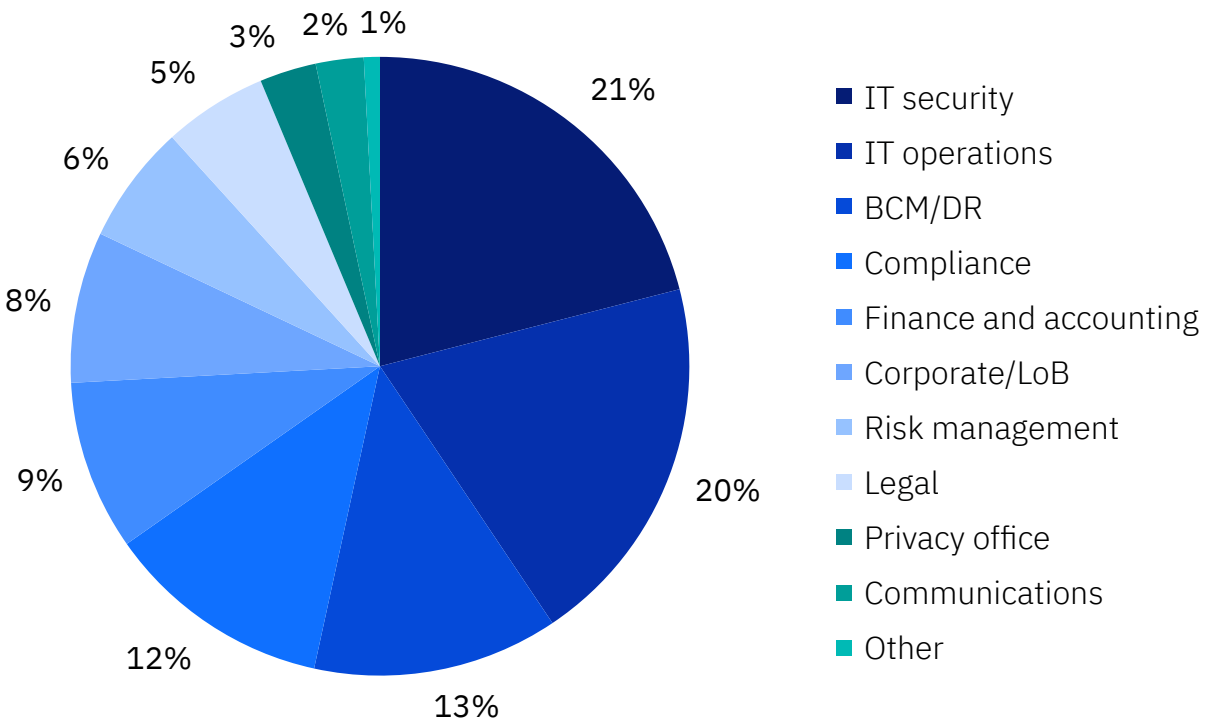
Consolidated view (n = 477)



Pie Chart 3 shows the distribution of 2,634 individuals who participated in interviews, representing 477 organisations within 11 countries and two regions. Twenty-one percent of interviewees were located in IT security, followed by 20 percent who were located in IT operations. Thirteen percent of respondents (or 338 individuals) were located in BCM or DR operations.

Pie Chart 3. Percentage frequency of interviewees by functional location

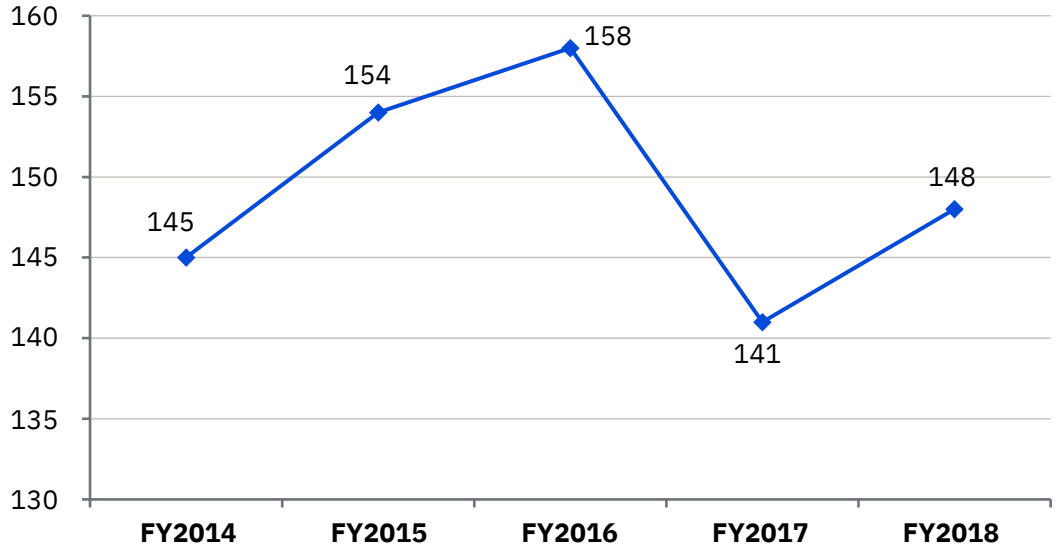
Consolidated view (n = 2,634)



Line Graph 1 shows the per capita cost of data breach for the consolidated sample of companies in various countries and regions. In FY2018, the cost increased by more than USD7 per compromised record, which represents a percentage increase of 4.8 percent. As can be seen, last year's study reported a USD17 decrease in per capita cost.

Line Graph 1. Global average cost per record

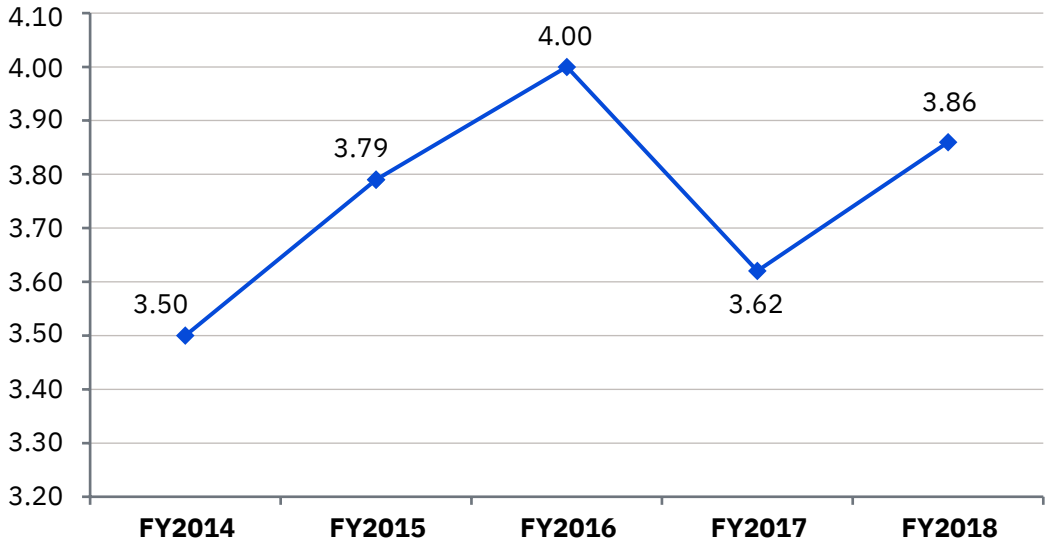
Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)
Measured in USD



Line Graph 2 shows the total average cost of data breach for the consolidated sample of companies located in multiple countries and regions. In FY2018, the cost increased by USD0.24 million per data breach incident, which represents a percentage increase of 6.4 percent.

Line Graph 2. Global average cost per incident

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)
Measured in USD millions



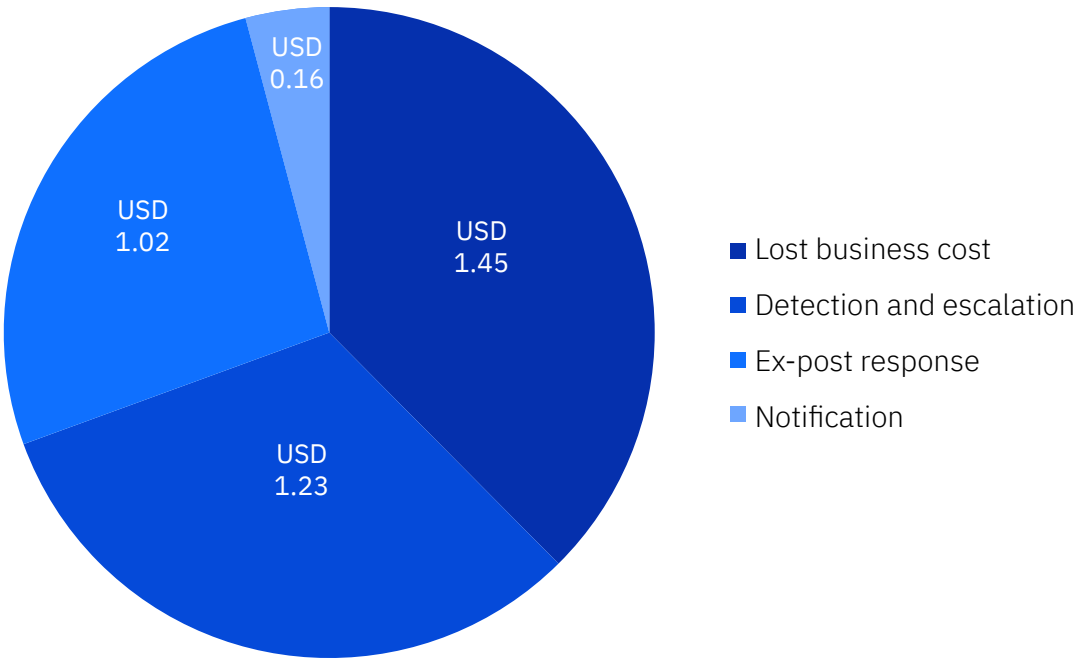
Following are the four high-level components of data breach cost expressed in USD millions:

- **Detection and escalation**: Activities that enable a company to reasonably detect the breach. Escalation activities are those necessary to report the breach 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. We also include costs that relate to communication with data protection regulators and other related parties
- **Ex-post response**: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimise potential harms. Redress activities also include ex-post response such as credit report monitoring or the reissuing of a new account (or credit card)
- **Lost business cost**: Activities that attempt to minimise the abnormal loss of customers as a result of the data breach event. In addition, we estimated the cost of new customer acquisition following the disclosure of the data breach. Finally, this section includes costs relating to business disruption and revenue losses.

The average total cost of data breach in the current year is USD3.86 million. As shown in Pie Chart 4, USD1.45 million is attributable to the most costly component, which is lost business cost. The least expensive component is data breach notification at USD0.16 million.

Pie Chart 4. Four cost components of data breach

Consolidated view (n=477)
Measured in USD millions

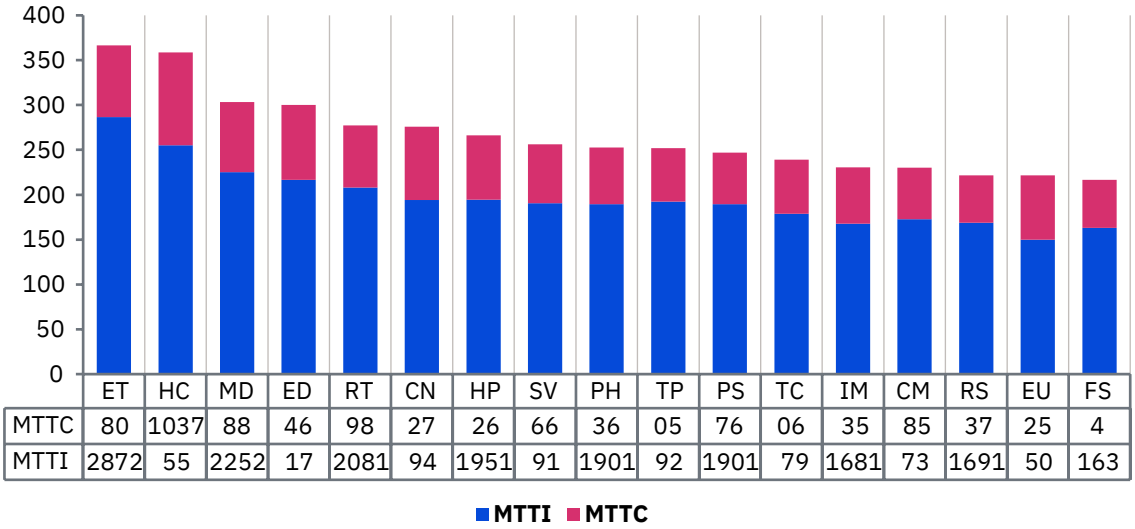


The faster the data breach can be identified and contained, the lower the costs. MTTI and MTTC metrics are used to determine the effectiveness of the incident response process.

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 477 companies, the MTTI averaged 197 days. Companies in the entertainment industry (ET) had the highest combined MTTC and MTTI at 367 days. In contrast, financial service (FS) companies had the lowest combined MTTC and MTTI at 217 days.

Figure 1. Days to identify and contain a data breach by industry

Consolidated view (n=477)

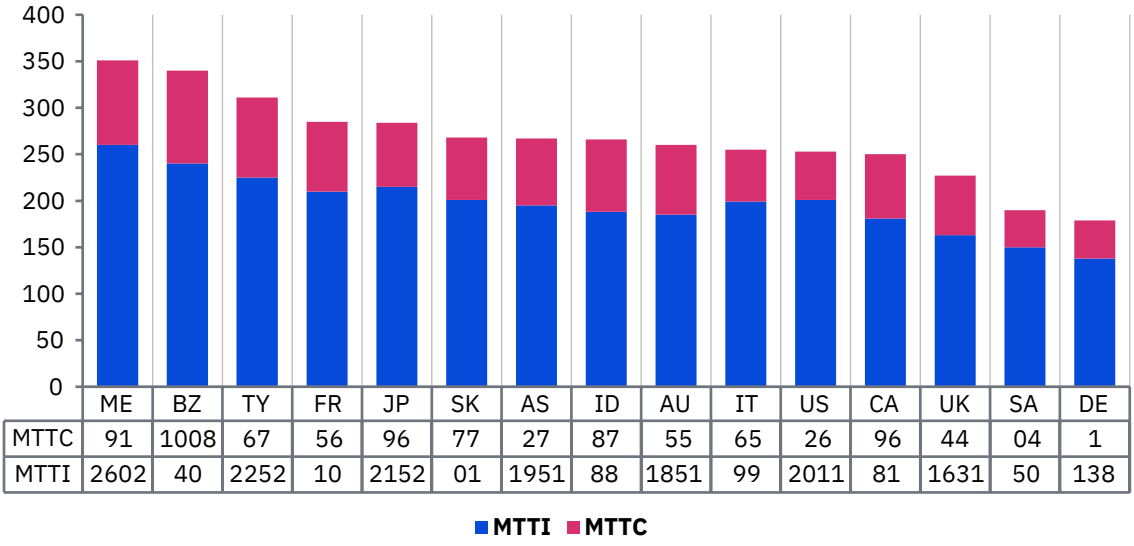


	ET	HC	MD	ED	RT	CN	HP	SV	PH	TP	PS	TC	IM	CM	RS	EU	FS
MTTC	80	1037	88	46	98	27	26	66	36	05	76	06	35	85	37	25	4
MTTI	2872	55	2252	17	2081	94	1951	91	1901	92	1901	79	1681	73	1691	50	163

Figure 2 reports the MTTI and MTTC for each country or regional sample. The Middle East has the highest days to identify and contain a data breach at 351 days. Whereas, at 179 days, German companies have the lowest days to identify and contain a data breach.

Figure 2. Days to identify and contain the data breach by country/region

Consolidated view (n=477)



	ME	BZ	TY	FR	JP	SK	AS	ID	AU	IT	US	CA	UK	SA	DE
MTTC	91	1008	67	56	96	77	27	87	55	65	26	96	44	04	1
MTTI	2602	40	2252	10	2152	01	1951	88	1851	99	2011	81	1631	50	138

Figure 3 shows the days to identify the data breach are lower for organisations that involved BCM and/or the DR team in the data breach incident response process. In FY2018, we show a saving of 44 days (214-170). Last year, we showed a savings of 43 days (213-171).

Figure 3. MTTI for organisations that involve or fail to involve BCM in the incident response process

Consolidated view (FY2015=350, FY2016=383, FY2017=419, FY2018=477)

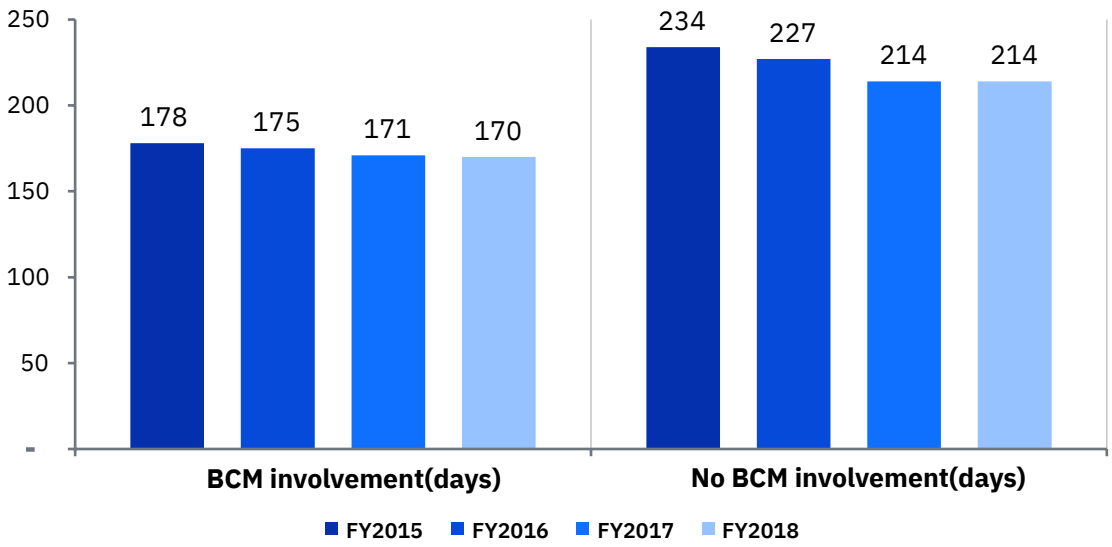


Figure 4 shows the days to contain the data breach incident are lower for organisations that involved BCM, or a time saving of 38 days (90-52). In FY2017, companies that involved BCM experienced a time saving of 35 days (85-50).

Figure 4. MTTC for organisations that involve or fail to involve BCM in the incident response process

Consolidated view (FY2015=350, FY2016=383, FY2017=419, FY2018=477)

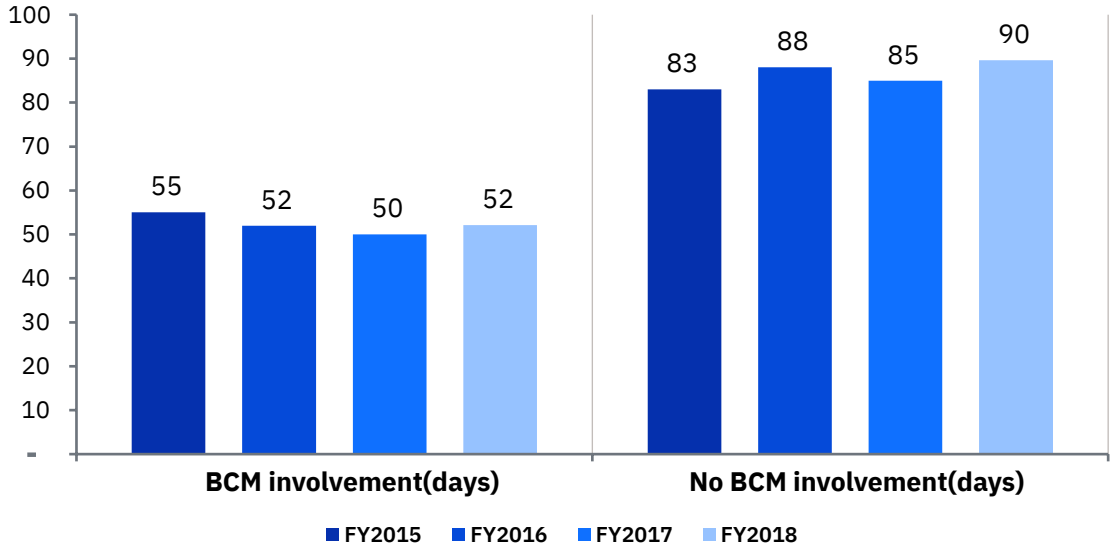


Figure 5 provides the extrapolated data breach cost per day that is associated with inefficiencies in identifying and containing the data breach. As shown, 215 companies (45 percent) without a BCM program have an average cost per day savings of USD6,705. In contrast, the average cost per day for the BCM group is USD4,881. The grand mean is USD5,703.

Figure 5. Cost per day for BCM and non-BCM companies

Consolidated view

Measured in USD

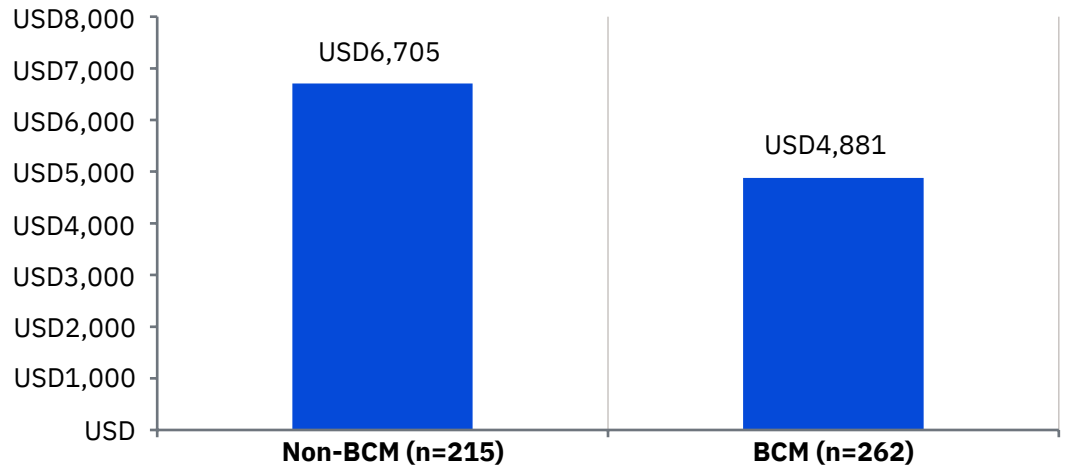
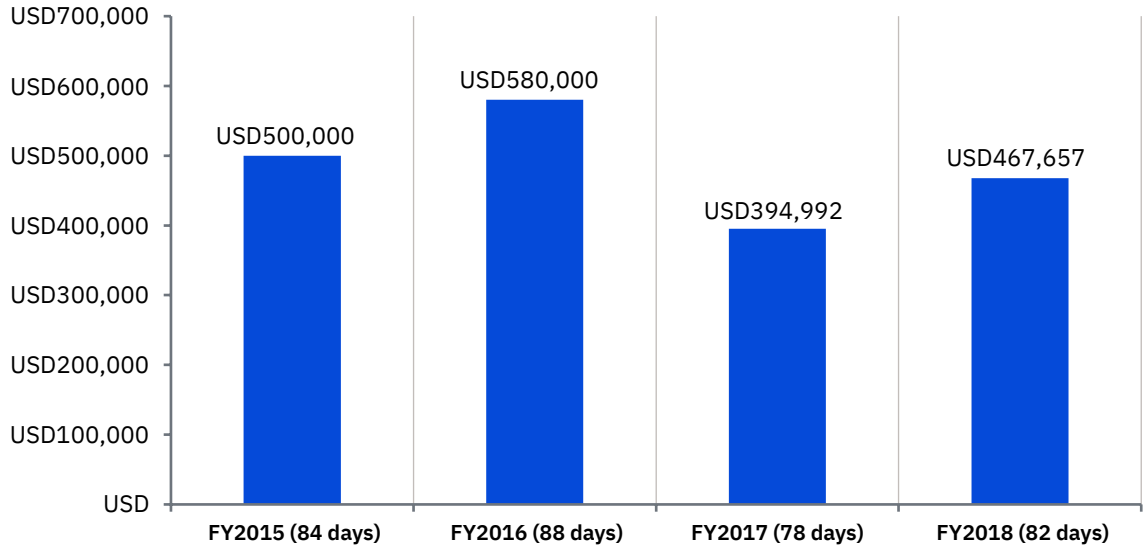


Figure 6 reports data breach cost savings, which is defined as the cost per day times the reduction in mean time to identify and contain the breach over the past four years. In FY2018, we compute an average savings of USD467,657 (USD5,703 times 82 days). Last year's extrapolated average data breach cost savings was USD394,992.

Figure 6. Total cost savings by involving the BCM team over four years

Consolidated view

Measured in USD



In this year's study, we calculate the MTTR. The MTTR was created from a subsample of 56 companies that experienced a data breach in both the FY2017 and FY2016 timeframe. This variable contains costs incurred up to one year after the data breach was most likely contained.

As shown in Figure 7, MTTR differences between the BCM and non-BCM groups are significant. Specifically, the MTTR from non-BCM companies is 70 days compared to 39 days for BCM companies.

Figure 7. Total time to identify, contain and recover from the data breach

Consolidated view

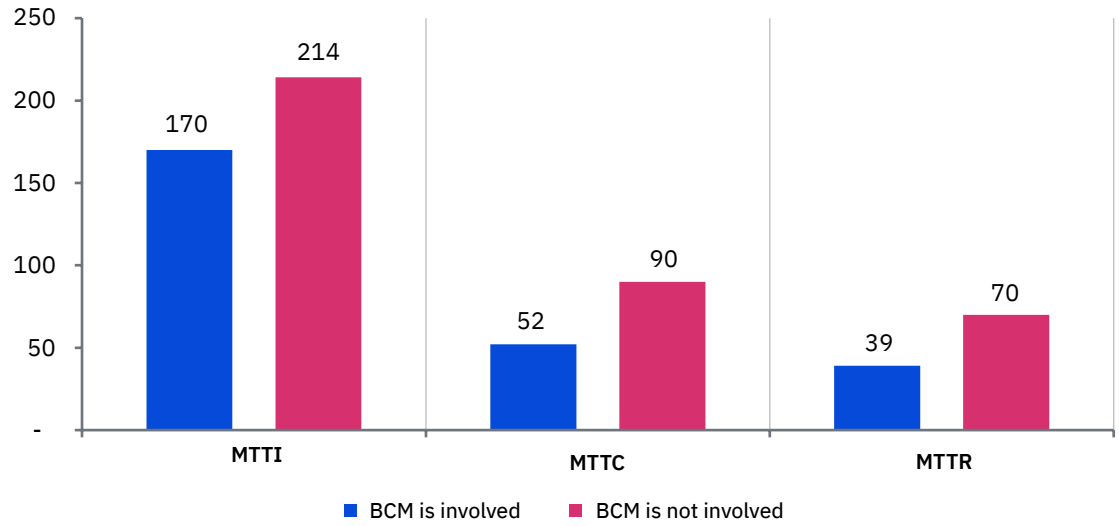
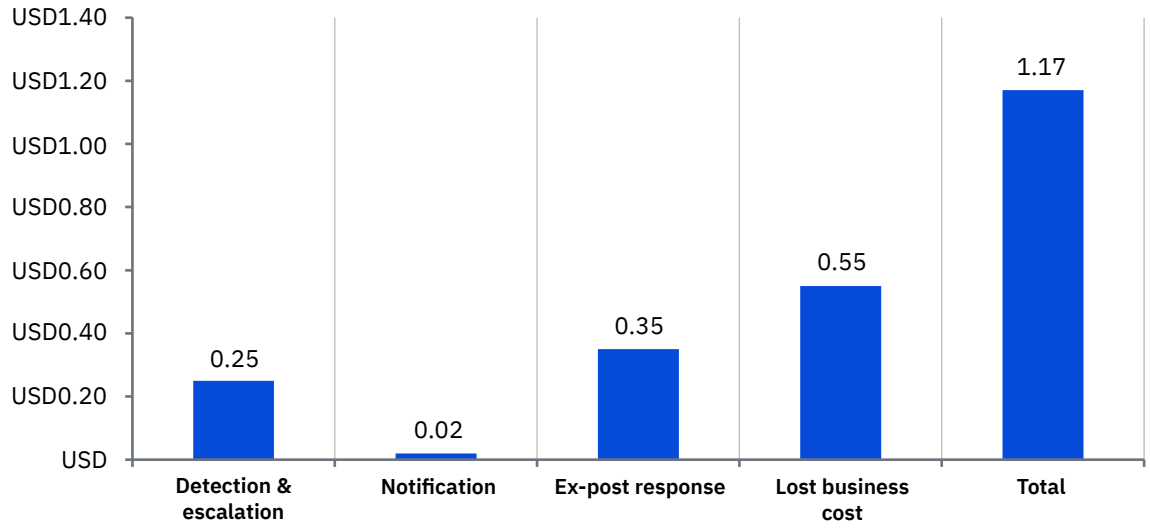


Figure 8 shows the average total costs of recovery. Similar to the findings from our sample of 477 companies, we find the largest cost category pertains to lost business costs at USD0.55 million. The lowest cost category is notification at only USD20,000.

Figure 8. Four cost components for the MTTR

Consolidated view

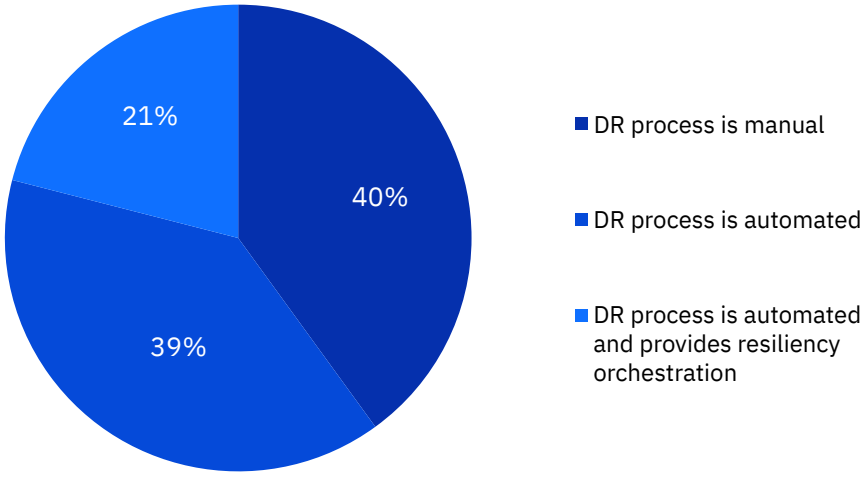
USD millions



Manual vs. automated DR processes. Pie Chart 5 shows 40 percent of our sample of companies deploys manual DR processes and another 39 percent say their company deployed a DR process that is primarily automated. Twenty-one percent of companies' DR processes are automated with resiliency orchestration. Last year's analysis showed only 16 percent of benchmarked companies used an automated DR process with resiliency orchestration.

Pie Chart 5. Percentage frequency by the type of DR process deployed by companies

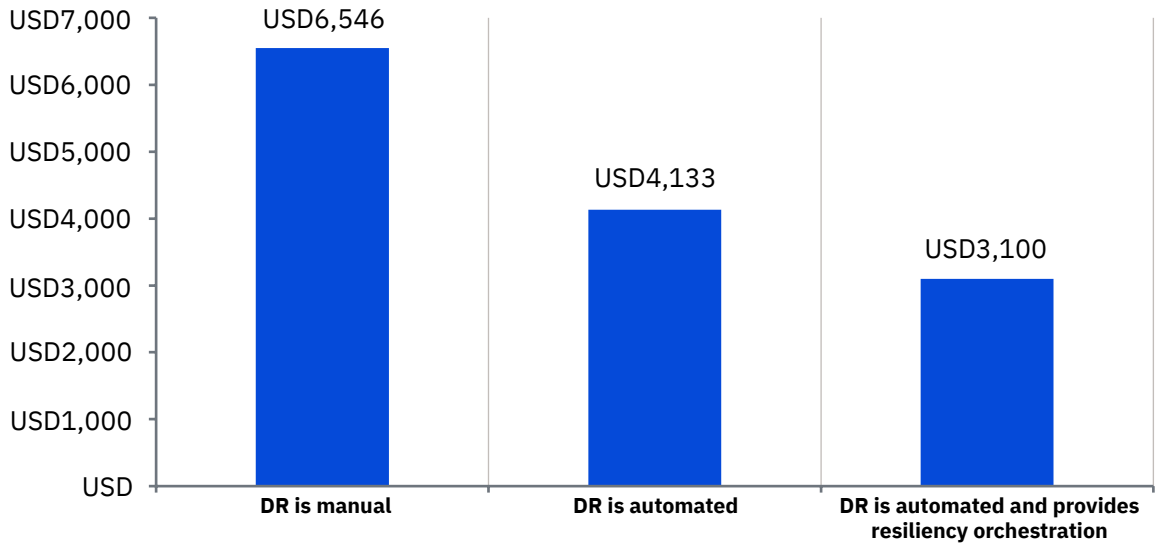
Consolidated view (n = 262)



DR automation and orchestration reduces the per day cost of a data breach. Figure 9 shows the cost impact of an automated DR process. BCM companies that have a manually operated DR process experienced an estimated average data breach cost of USD6,546 per day. In contrast, BCM companies with an automated DR process experienced an average cost of USD4,133. Companies that automate the DR process, which includes resiliency orchestration, realised the lowest per diem cost of USD3,100.

Figure 9. The impact of DR processes on cost per day

Consolidated view
Measured in USD



Factors that influence the cost of data breach. As shown in Figure 10, there are 22 factors that can either increase (negative numbers) or decrease (positive numbers) the cost of data breach. These cost categories are overlapping; hence, they cannot be added together to estimate a total per capita cost savings based on the occurrence of these 22 factors.

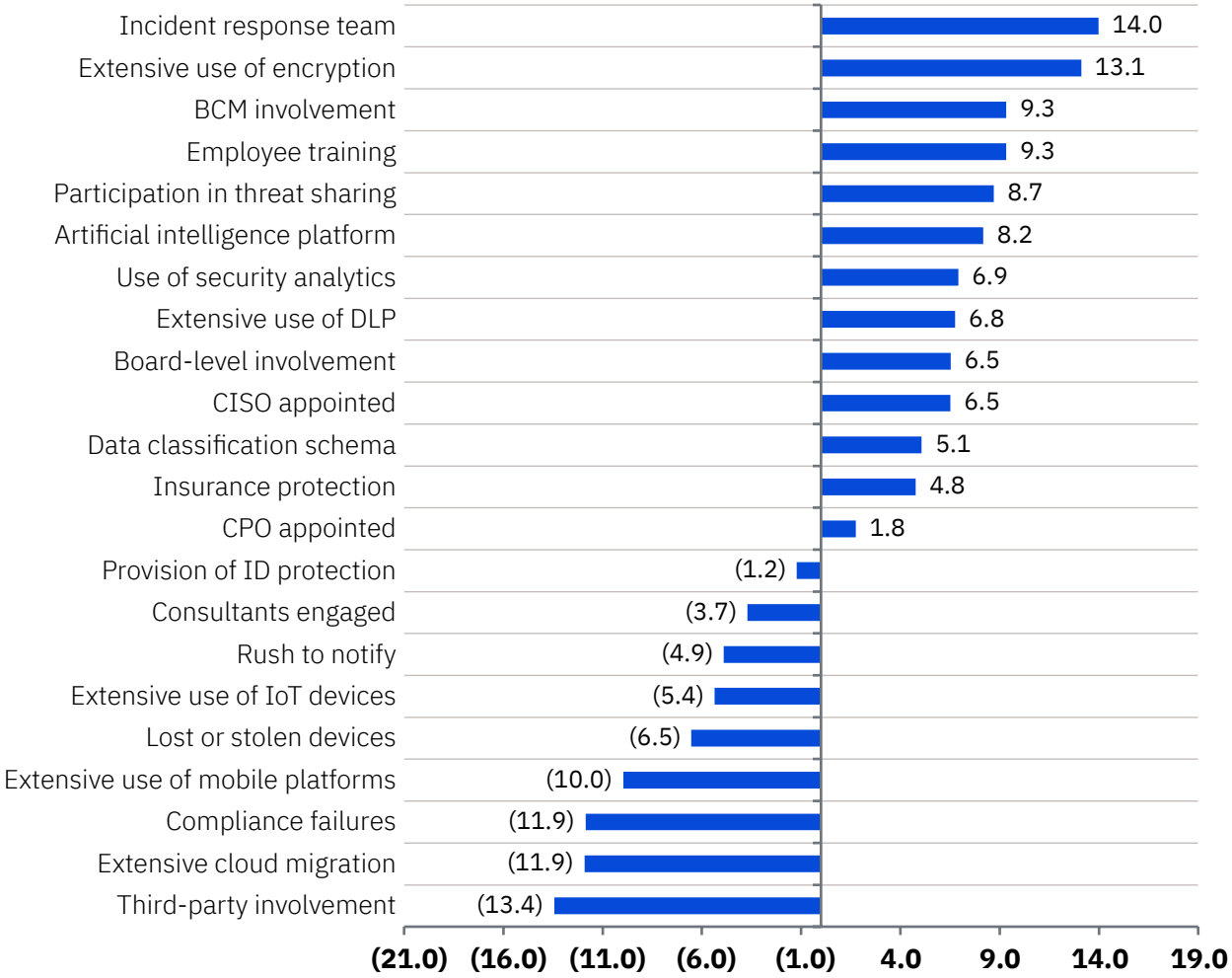
For example, the existence of a strong incident response team resulted in an average decrease in the per capita cost of data breach by USD14 and BCM also decreased the average cost of data breach by USD9.3 per compromised record. Last year's per capita cost savings from BCM involvement was USD10.9.

In contrast, compliance failures can increase the cost by an average of USD11.9. If the breach took place when the company was migrating an extensive amount of data to the cloud, the cost increased by USD11.9 due to the complexity of determining the types of data lost or stolen.

Figure 10. Impact of 22 factors on the per capita cost of data breach

Consolidated view (n = 477)

Measured in USD



BCM's contribution to incident response planning. Figure 11 provides a summary of BCM involvement in the data breach incident response planning and execution. Of the 477 companies in this global study, 262 (55 percent) had BCM involvement. The remaining 215 companies did not involve their BCM team or only involved BCM on an ad hoc basis. Last year's analysis showed 54 percent of companies involved BCM in the data breach incident response.

Figure 11. How does BCM contribute to the data breach incident response process?

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)

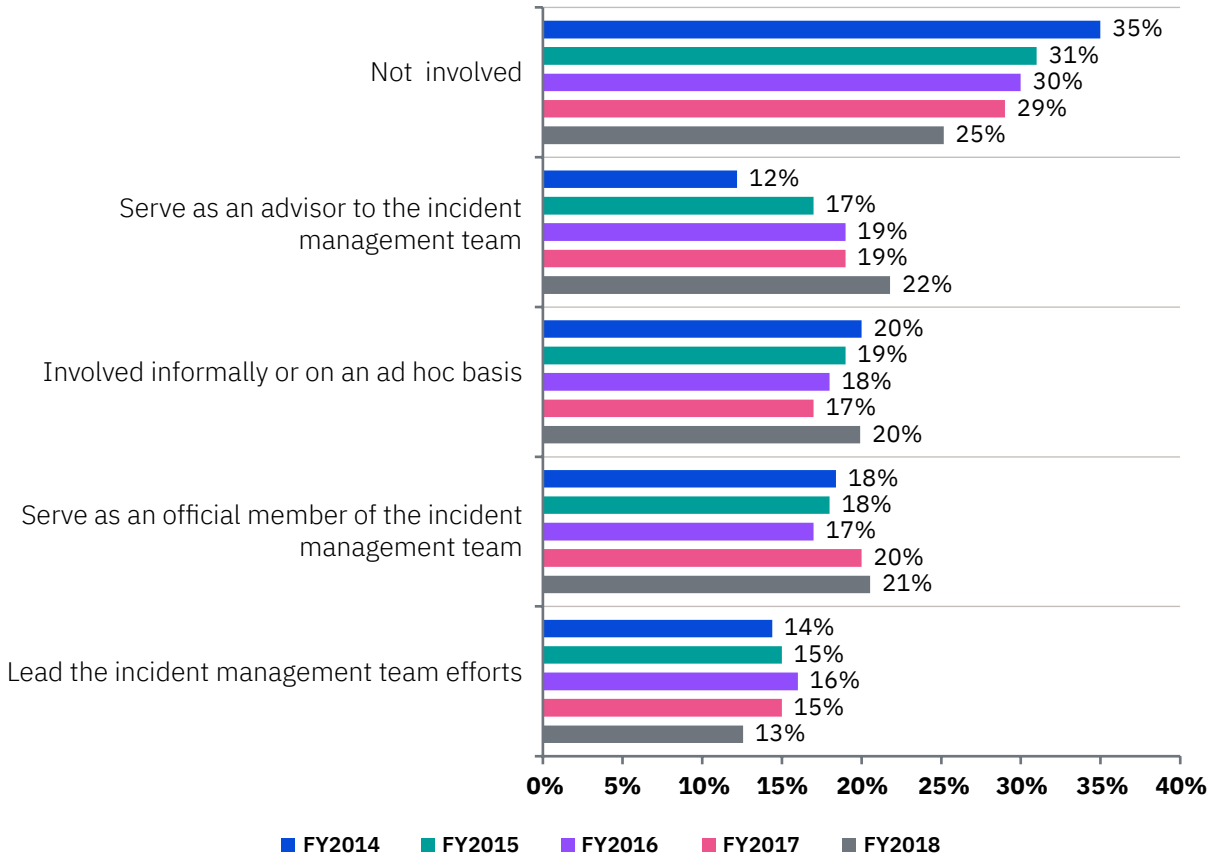


Figure 12 reports the percentage of BCM team involvement in incident planning and execution for country and regional samples. Similar to the last four years, Germany had the highest rate of BCM involvement, with 76 percent of German companies reporting they had a BCM or DR team in place. In contrast, only 30 percent of Turkish companies had BCM involvement. It is also important to note that the FY2018 results are greater than or equal to the five-year average.

Figure 12. BCM participation rate by country sample versus five-year average

Consolidated view (FY2014=315, FY2015=350, F 2016=383, FY2017=419, FY2018=477)
*Historical data are not available for all years

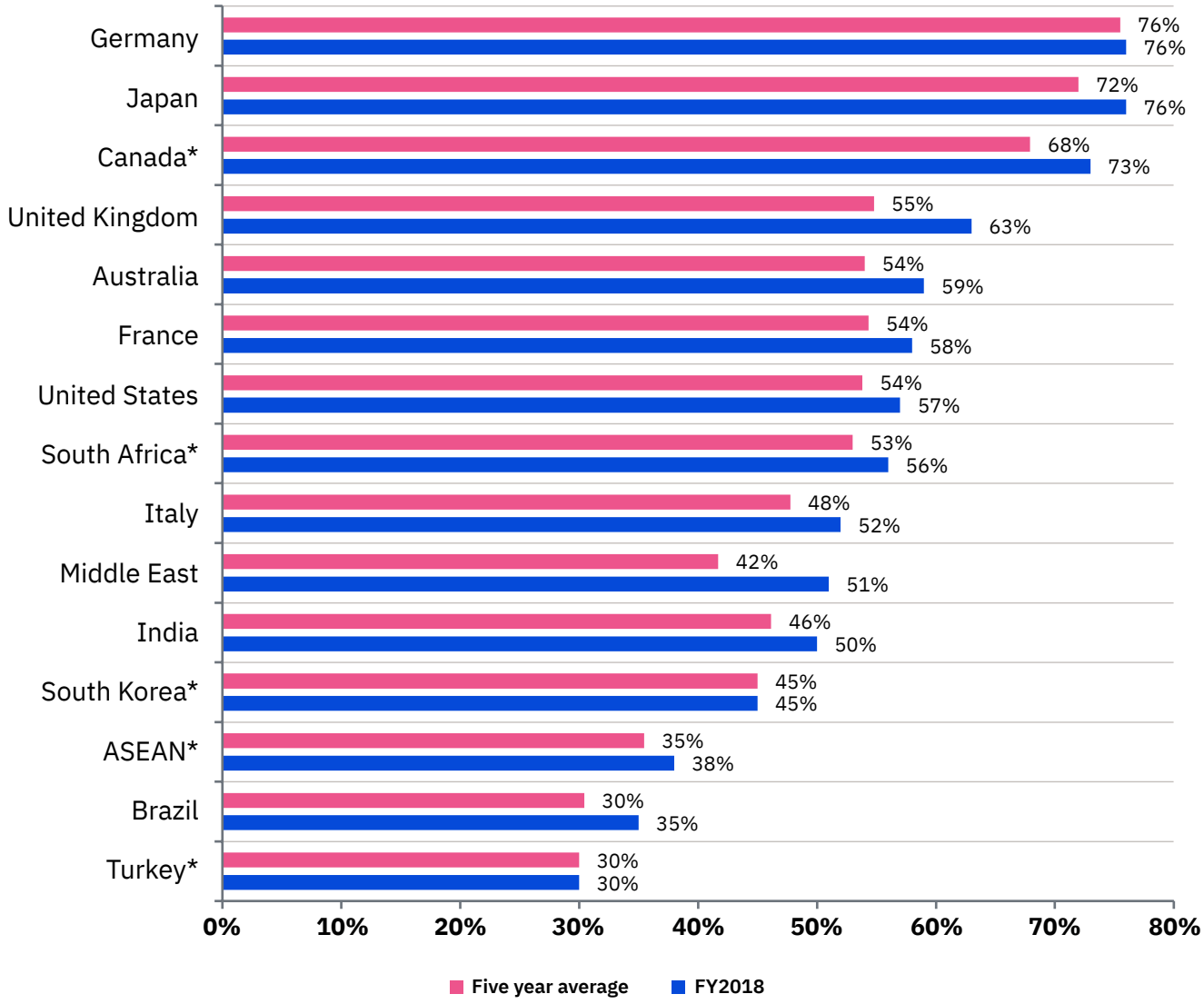
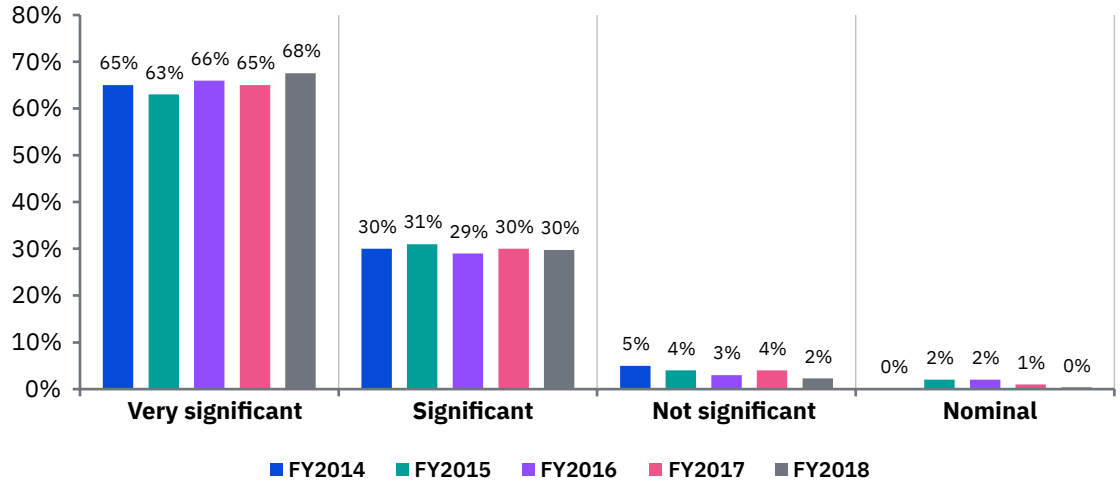


Figure 13 shows the level of BCM involvement in incident response planning and execution. For this year's study, 68 percent of companies rate this involvement as very significant. Another 30 percent rate BCM involvement as significant. Last year's study showed that 65 and 30 percent rated BCM involvement as very significant or significant, respectively.

Figure 13. What best describes BCM's contribution to the incident response process?

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)



BCM reduces the per capita cost of data breach. Figure 14 reports the average per capita cost of data breach over five 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 ± USD9.3. Last year's per capita cost savings for BCM companies was ±USD10.9.

Figure 14. Per capita cost of data breach for companies with or without BCM involvement

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)
Measured in USD

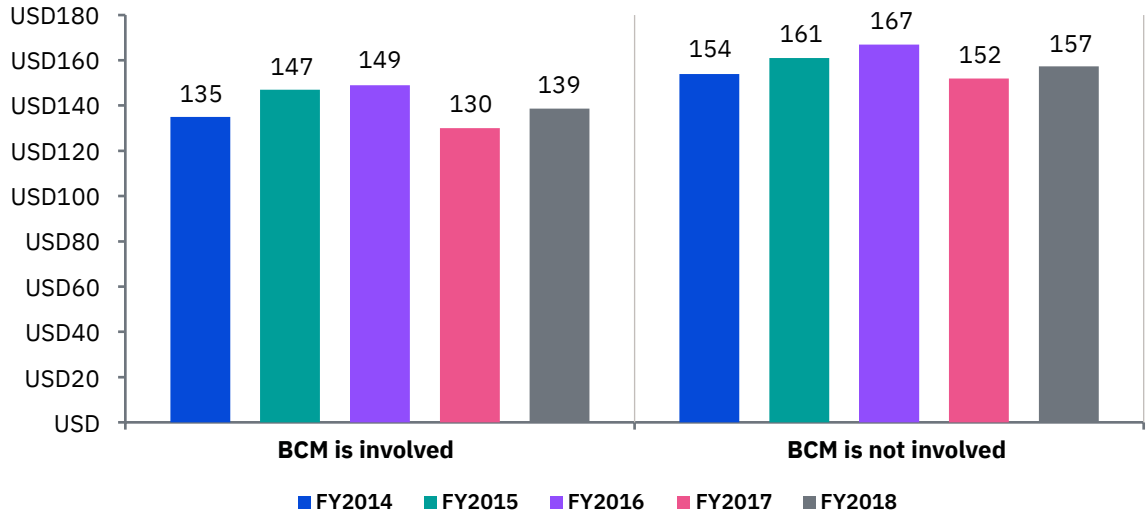
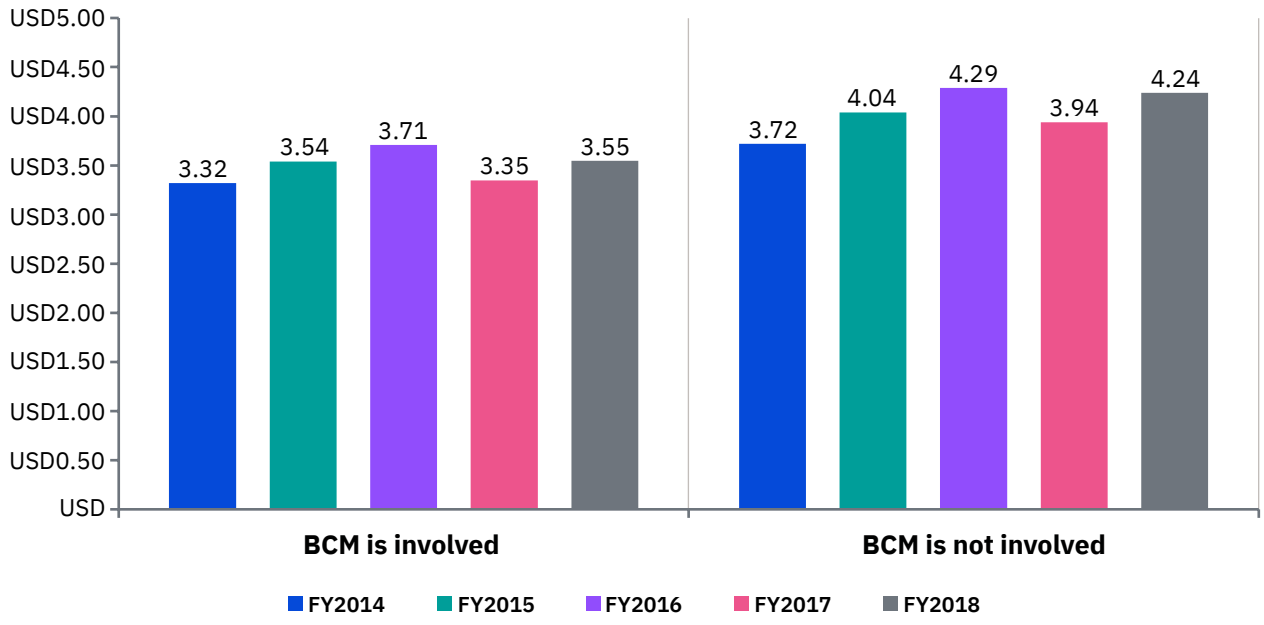


Figure 15 reports the total cost of data breach over five years for companies that involved the BCM team in incident response planning and execution and those that did not. Similar to the above, those companies involving BCM experienced a lower total cost of data breach than those that did not involve BCM. In this year's study, the difference in the total cost between companies that did and did not involve BCM is USD0.69 million (USD4.24-USD3.55). In percentage terms over the past year, per capita cost decreased by 10 percent for companies in the BCM group and nine percent for the non-BCM group.

Figure 15. Total cost of data breach for companies with or without BCM involvement

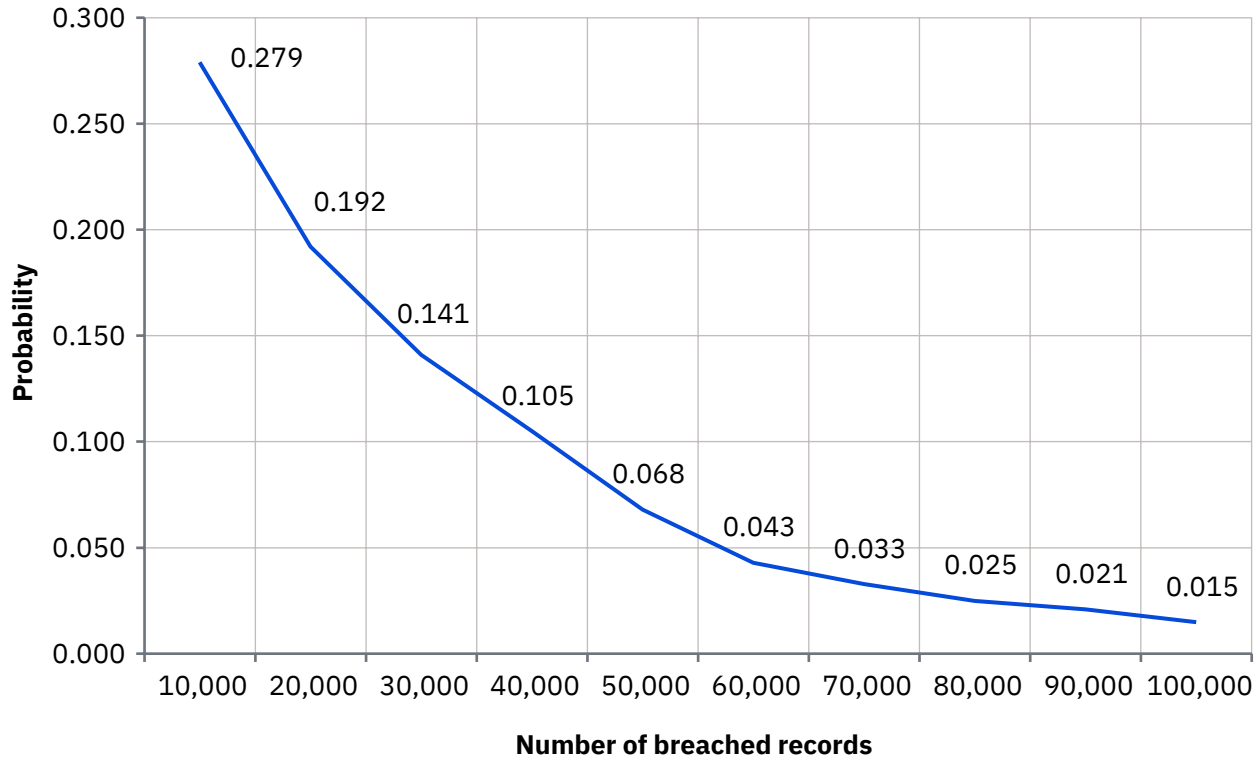
Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)
USD millions



The larger the data breach, the less likely the organisation will have another breach in the next 24 months. Figure 16 reports the average likelihood of data breach involving a minimum of 10,000 or more records over the forthcoming 24 months for companies that involve the BCM team and those that do not. This year's average likelihood of data breach for all 477 companies was 27.9 percent.

The following chart shows the subjective probability distribution of data breach incidents involving a minimum of 10,000 and a maximum of 100,000 compromised records over a 24-month period[8]. As can be seen, the likelihood of data breach steadily decreases as the number of breached records increases. The likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 27.9 percent over a 24-month period. The chance of a data breach involving a minimum of 100,000 records is less than 1 percent.

Figure 16. Probability of a data breach involving a minimum of 10,000 and a maximum of 100,000 records

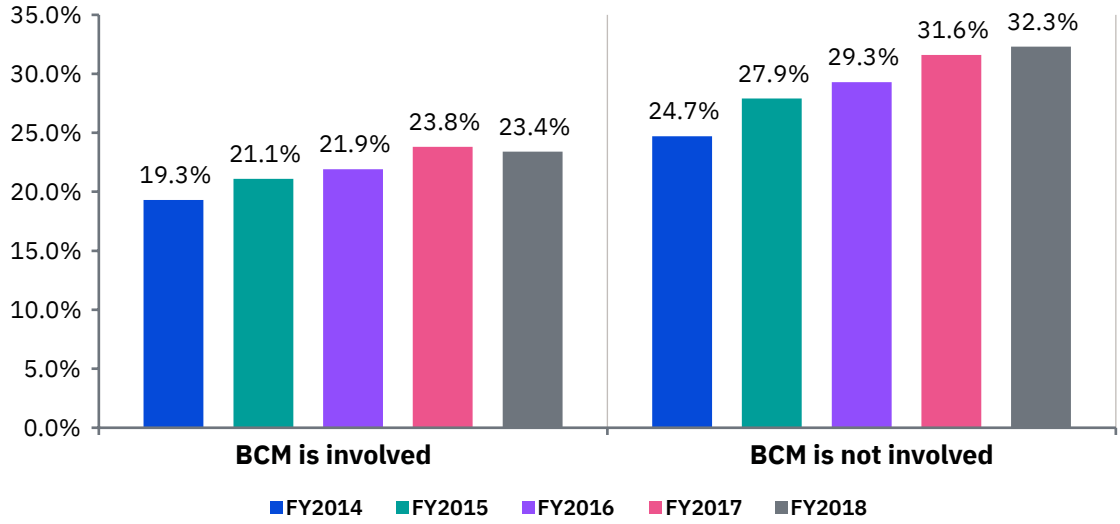


[8]Estimated probabilities were captured from sample respondents using a point estimation technique. Key individuals such as the CISO or CPO, who participated in cost assessment interviews provided their estimate of data breach likelihood for 10 levels of data breach incidents (ranging from 10,000 to 100,000 lost or stolen records). The time scale used in this estimation task was the forthcoming 24-month period. An aggregated probability distribution was extrapolated for each of the 477 participating companies.

Over the past five years, we found that organisations that involved the BCM team experienced a lower likelihood of recurrence than those that did not involve BCM. As shown in Figure 17, the difference in the likelihood of one or more material data breaches between companies that did and did not involve BCM is 8.9 (32.3-23.4) percent. Last year's difference was 7.8 (31.6-23.8) percent.

Figure 17. Likelihood of a material data breach for companies with or without BCM involvement over the next 24 months

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)

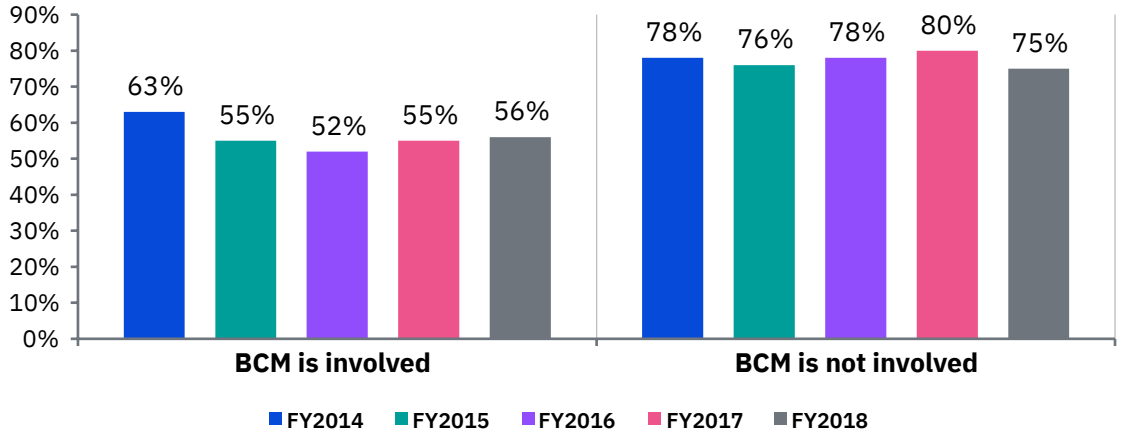


BCM minimises disruptions to business operations when a data breach occurs. Figure 18 reveals differences between companies with or without BCM involvement with respect to material disruption to business processes.

In FY2018, 78 percent of companies without BCM involvement said the data breach incident caused a material disruption to their business processes. In contrast, 56 percent of companies with BCM involvement said they had a material disruption. A consistent pattern holds true for all five years.

Figure 18. Did the data breach cause a material disruption to business processes?

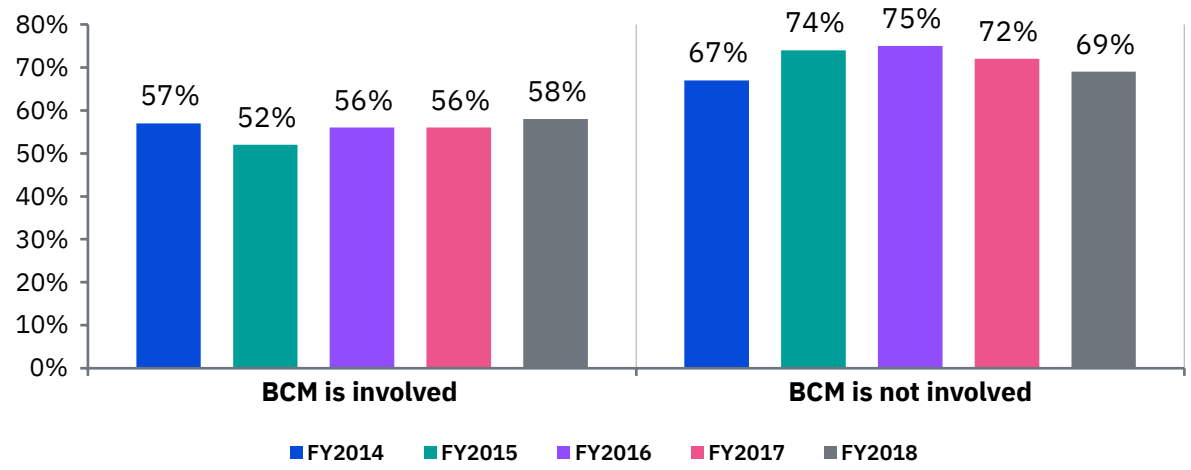
Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)



BCM involvement improves the resilience of IT operations. Similar to the above, Figure 19 shows differences between companies with or without BCM involvement with respect to material disruption to IT operations. As reported for FY2018, 69 percent of companies without BCM involvement said the data breach incident caused a material disruption to IT operations. In contrast, 58 percent of companies with BCM involvement said the incident caused a material disruption to IT operations. Results show a consistent pattern over five years.

Figure 19. Did the data breach incident cause a material disruption to IT operations?

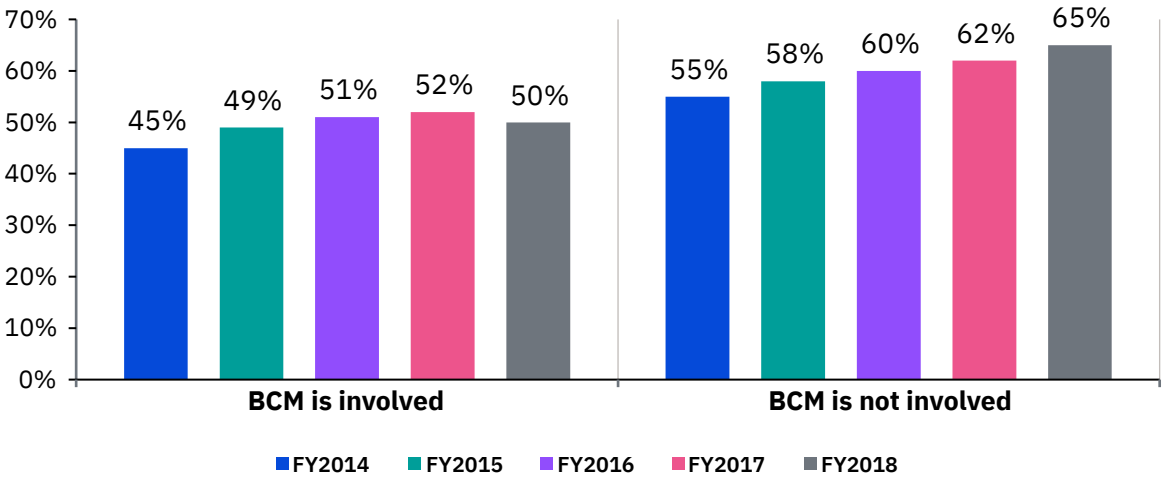
Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)



BCM can protect a company's reputation following a data breach. Figure 20 shows the difference in the ability to protect reputation following a data breach. In this year's study, 65 percent of companies without BCM programs said the data breach had a negative material impact on the organisation's reputation, brand or marketplace image. In contrast, 50 percent of companies that involved BCM said the incident had a negative impact on the organisation's reputation or brand. Results show a consistent pattern for all five years.

Figure 20. Did the data breach have a negative material impact on reputation?

Consolidated view (FY2014=315, FY2015=350, FY2016=383, FY2017=419, FY2018=477)



Total cost of a mega breach

For the first time this year, we attempt to measure the cost of data breaches involving more than one million compromised records (a.k.a. mega breach). Our cost model is based on the analysis of 11 companies that experienced a mega breach.

We then conducted a Monte Carlo simulation to predict the exposure value a company might experience as a result of a mega data breach that was discovered sometime over the past four years, ranging in size from 1 million to 50 million consumer records. Using this method, we are able to estimate both the total cost and per capita cost of the mega breach. As shown in Figure 21, this analysis reveals a parabolic cost curve, where the rate of cost increase flattens out as the size of the breach approaches 50 million records.

Figure 21. Simulated mega breach cost curve

Measured in USD

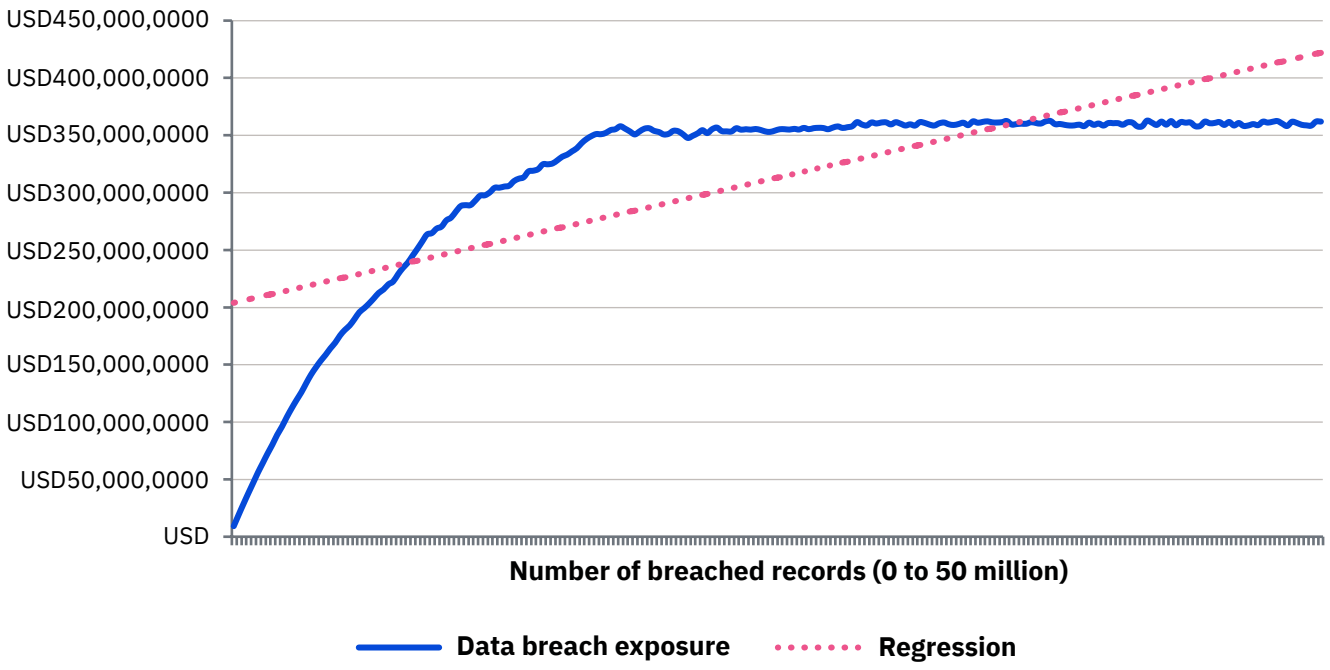
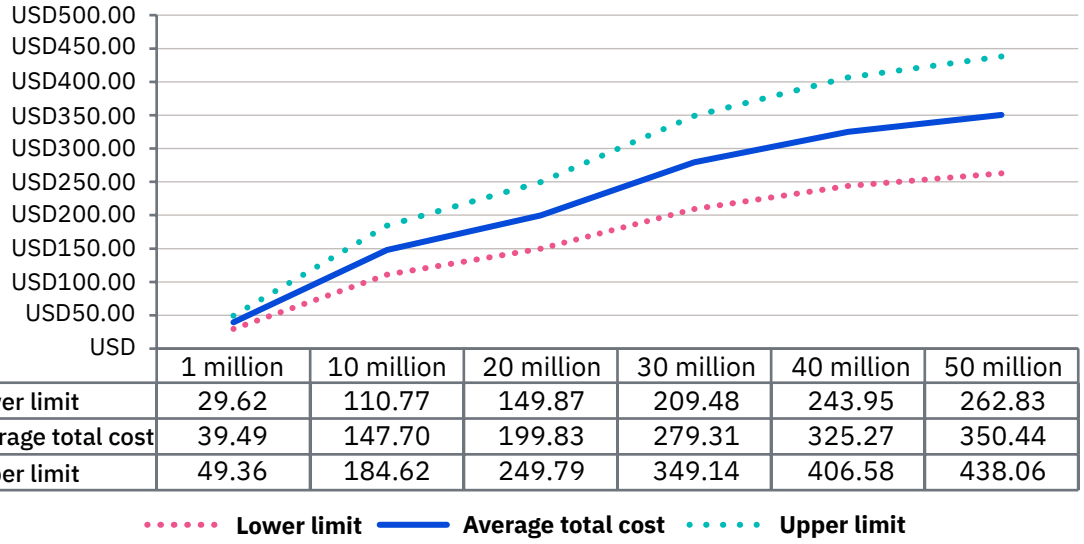


Figure 22 shows the nonparametric precision interval at six levels of data breach ranging from 1 million to 50 million lost or stolen records.

Figure 22. Precision interval at the 95 percent level of confidence

Measured in USD millions



	1 million	10 million	20 million	30 million	40 million	50 million
Lower limit	29.62	110.77	149.87	209.48	243.95	262.83
Average total cost	39.49	147.70	199.83	279.31	325.27	350.44
Upper limit	49.36	184.62	249.79	349.14	406.58	438.06

Drawing upon our traditional cost framework, Table 2 reports four cost components of data breach compiled from 11 companies that experienced a mega breach coupled with Monte Carlo simulation.

Table 2. Four mega breach components

Number of breached records	Detection & escalation	Notification	Ex-post response	Lost business cost	Total cost (USD millions)
1,000,000	11,682,870	567,130	12,225,694	15,012,731	39,488,426
10,000,000	44,851,852	1,878,009	48,039,120	52,926,157	147,695,139
20,000,000	62,481,481	3,174,306	67,170,833	67,005,556	199,832,176
30,000,000	88,407,407	4,151,389	91,763,194	94,989,352	279,311,343
40,000,000	102,537,037	5,903,009	106,411,343	110,413,657	325,265,046
50,000,000	110,998,725	6,498,576	115,028,472	117,919,213	350,444,986

Figure 23 shows the estimated total cost at six size levels of data breach ranging from one to 50 million lost or stolen records. Drawing from our mega cost framework, a data breach involving 1 million compromised records yields a total cost of USD39.49 million. At 50 million records, we estimate a total cost of USD350.44 million.

Figure 23. Average total cost of mega breach

Measured in USD millions

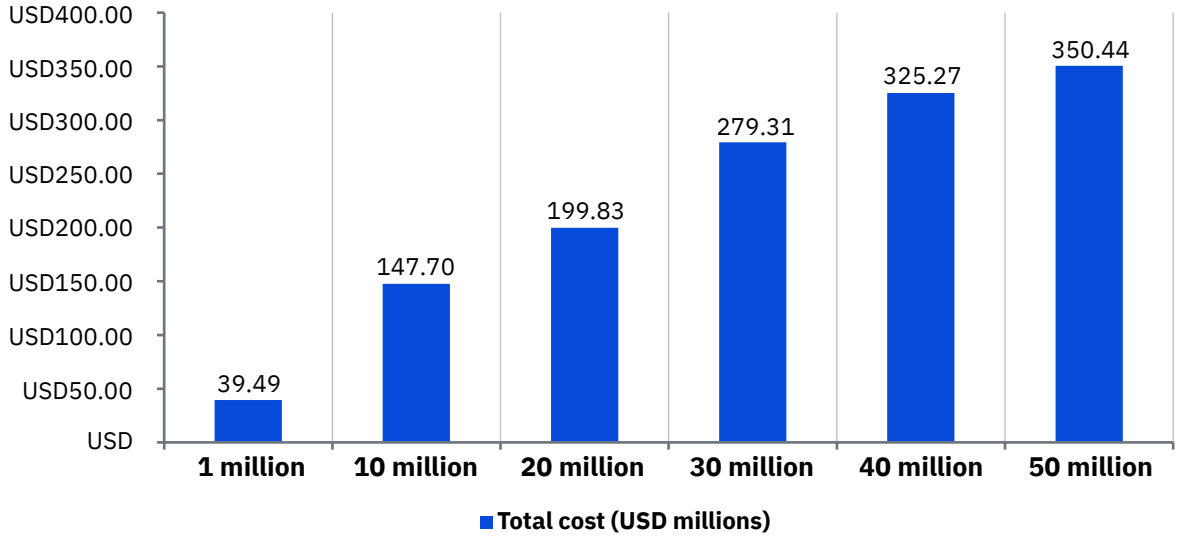
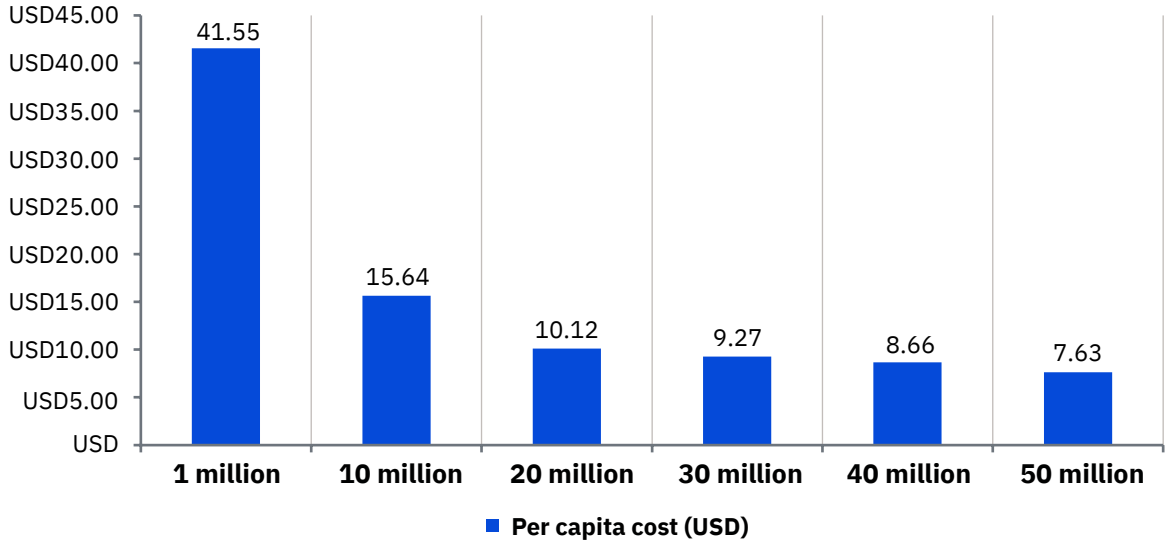


Figure 24 shows the estimated per capita cost of mega breach at six data breach levels ranging from 1 million to 50 million lost or stolen records. According to our framework, a data breach involving 1 million compromised records yields a per record cost of USD41.55. At 50 million records, we estimate a per capita cost of USD7.63. Please note that per capita cost plateaus beyond 50 million records. The main reason for this inverse relationship between per capita cost and breach size is the fact that a substantial amount of total cost is fixed – rather than variable.

Figure 24. Per capita cost of mega breach

Measured in USD

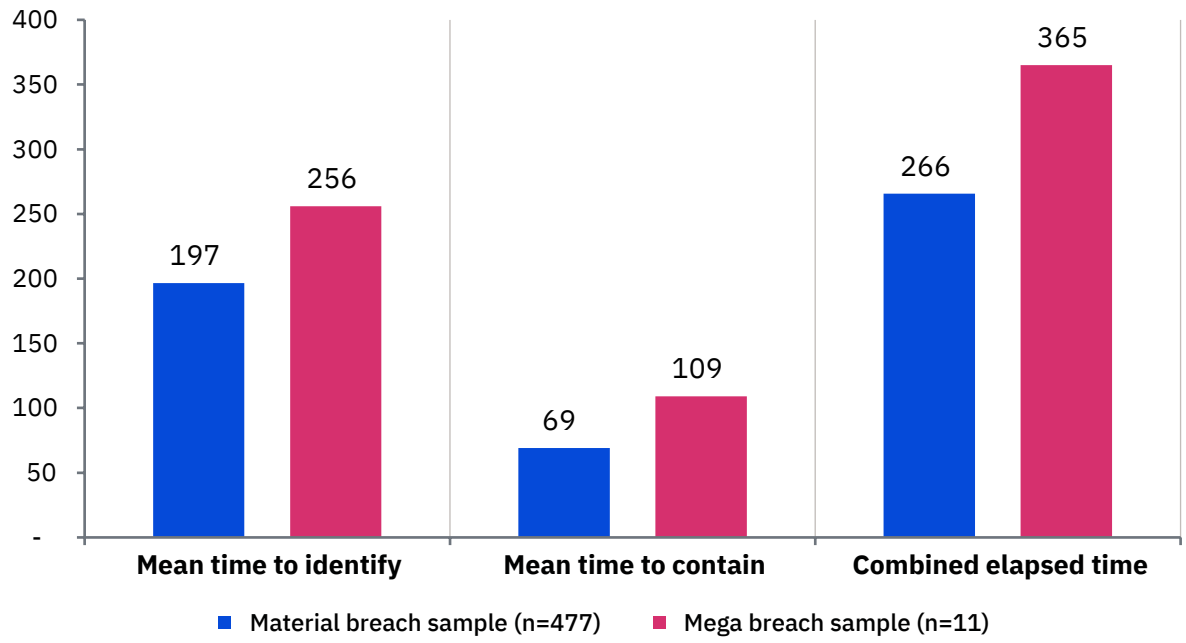


Comparison of primary and mega data breach companies. Figure 26 shows the MTTI and the MTTC a data breach for our primary sample of 477 companies, versus our small sample of 11 mega breach companies.

Figure 25 shows the consolidated MTTI data breaches at 197 days (primary sample) versus 256 days (mega breach sample). Similarly, the primary sample shows the consolidated MTTC the data breach at 69 days versus 109 days for the mega breach sample. The mega breach sample shows a total of 365 days to identify and contain the data breach, which is 99 days greater than the primary sample.

Figure 25. Mean days to identify and contain data breaches for the primary and mega breach samples

Consolidated view



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 based on actual use. Companies participating in this benchmark research are asked to estimate the cost for all the activities necessary to resolve the data breach. Typical activities for the discovery of 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
- Organising the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures for data breach victims and regulators
- Implementing call centre procedures and specialised training

The following are typical activities conducted in the aftermath of discovery:

- Audit and consulting services
- Legal services for defence
- Legal services for compliance
- Free or discounted services offered 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 categorise the costs as direct and indirect, as defined below:

- **Direct cost** – the direct expense outlay to accomplish a given activity.
- **Indirect cost** – the amount of time, effort and other organisational resources allocated to data breach resolution, but not as a direct cash outlay.

Our study also examines the core process-related activities that drive a range of expenditures associated with an organisation'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 centres are:

- **Detection and escalation**: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion and 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. Also included are costs that relate to communication with data protection regulators and other related parties.
- **Ex-post response**: Communication with victims of a breach to help them minimise potential harms and other assistance, such as credit report monitoring or establishing a new account or credit card.
- **Lost business**: Activities that attempt to minimise the abnormal loss of customers as a result of the data breach event. This includes the estimated number of target customers who will not have a relationship with the organisation as a consequence of the breach. This number is presented as an annual percentage (i.e., churn rate). Also included in this category are the costs of acquiring new customers and costs related to business disruption and revenue loss.

Part 4. Organisational Characteristics

Pie Chart 6 shows the distribution of benchmark organisations by total headcount. The largest segment included companies with 1,001 to 5,000 employees. The smallest segment included companies with more than 75,000 employees.

Pie Chart 6. Global headcount of participating companies

Consolidated view (n = 477)

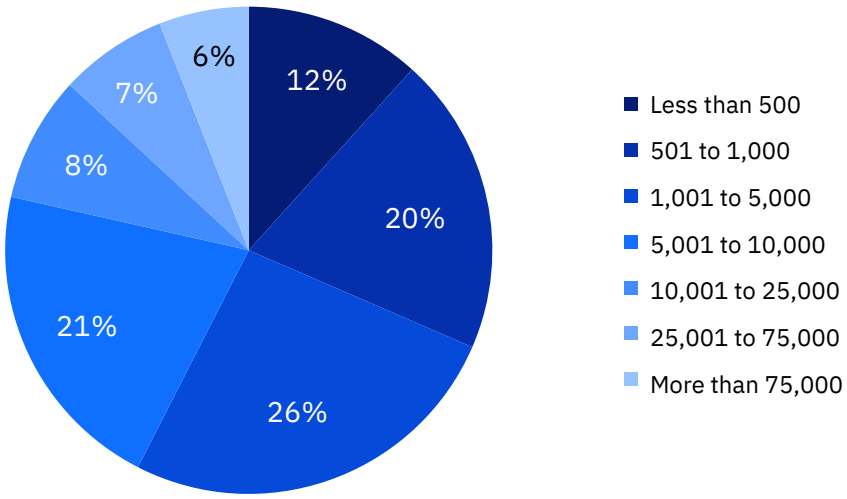
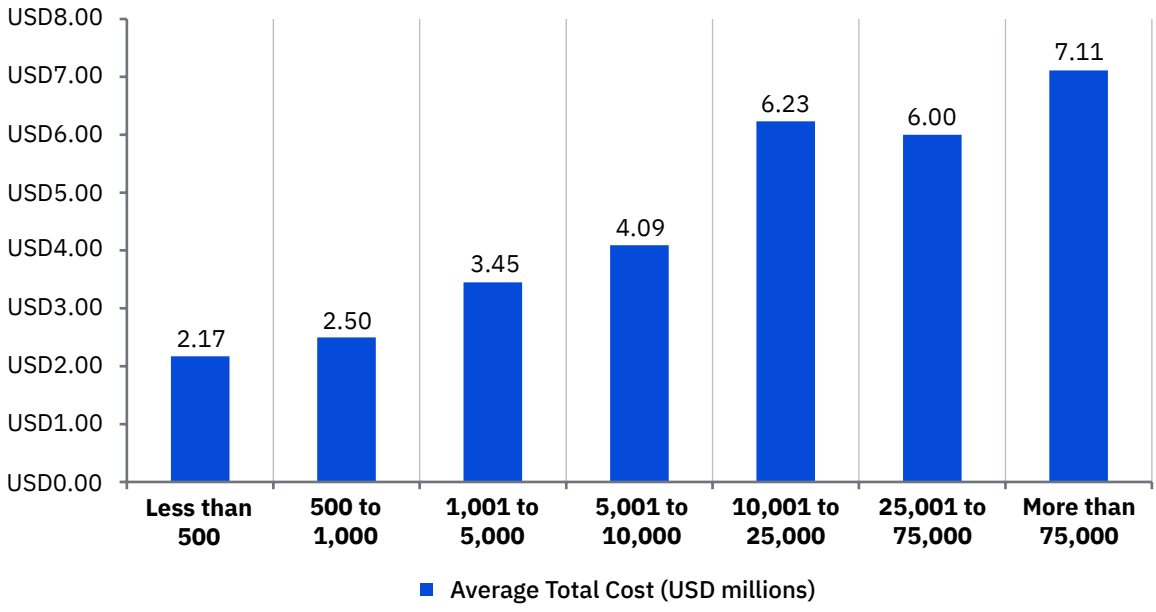


Figure 26. The following chart shows a systematic interrelationship between organisational size as measured by global headcount and total data breach cost. As can be seen, for companies with fewer than 500 full-time equivalents, the total data breach cost is USD2.17 million compared to USD7.11 million for companies with more than 75,000 employees.

Figure 26. Average total cost of data breach by global headcount (size)



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

How to use the number line

The number line provided under each data breach cost category is one way to obtain your best estimate for the sum of cash outlays, labour and overhead incurred. Please mark only one point somewhere between the lower and upper limits set below. 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]

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

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 better quality results.

Part 5. Limitations

Our study utilises a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from 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, 477 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 organisational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.
- **Extrapolated cost results**: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email:

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

Ponemon Institute

Advancing Responsible Information Management

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

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.