2017 Cost of Data Breach Study

Germany

Benchmark research sponsored by IBM Security
Independently conducted by Ponemon Institute LLC
June 2017
Part 1. Introduction

IBM Security and Ponemon Institute are pleased to present the 2017 Cost of Data Breach Study: Germany, our ninth annual benchmark study on the cost of data breach incidents for companies located in Germany. This year, the per capita cost of data breach decreased from €154 to €149 and the average total cost of data breach decreased from €3.61 million in 2016 to €3.42 million in 2017. To date, 252 German organizations have participated in this research.

Ponemon Institute conducted its first Cost of Data Breach Study in the United States 12 years ago. Since then we have expanded the research to include the following countries and industries:

- 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 2017 study examines the costs incurred by 35 German companies in 13 industries following the loss or theft of protected personal data and the notification of breach victims as required by various laws. It is important to note that costs presented in this research are not hypothetical but are from actual data loss incidents. These costs are based on estimates provided by individuals interviewed over a 10-month period in the companies represented in this research.

The number of breached records per incident this year ranged from 5,001 to 81,800. The average number of breached records was 22,490. We did not recruit organizations with data breaches involving more than 100,000 compromised records. Such incidents are not representative of most data breaches and including them would have artificially skewed the research results.

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

---

1 This report is dated in the year of publication rather than the year of fieldwork completion. Please note that the majority of data breach incidents studied in the current report occurred in the 2016 calendar year.
2 The terms “cost per compromised record” and “per capita cost” have equivalent meaning in this report.
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.

- **An attack by a malicious insider or criminal is costlier than system glitches and negligence (human factor).**

Almost half of organizations represented in this research (47 percent) identified the root cause of the data breach as a malicious or criminal attack and the average cost was approximately $156. In contrast system glitches and human error or negligence averaged approximately $128 and $126, respectively. Factors that may decrease the cost are participation in threat sharing, use of security analytics and the recruitment and retention of knowledgeable personnel.

In conclusion, organizations in Australia, Germany, France and the United Kingdom were able to improve their ability to keep customers and, as a result, reduced the cost of data breach. Organizations in Australia, the United Kingdom and Germany also were able to limit the number of customer records lost or stolen and, as a result, had lower costs. Whereas, countries in the Middle East and the United States experienced a higher percentage of churn and had higher costs. Organizations in Brazil, India, the Middle East and South Africa had data breaches involving more lost or stolen records, which increased their costs. The individual country reports present in greater detail the cost components and factors that affected the cost.
The following are the most salient findings and implications for organizations:

**The cost of data breach continues to decline.** The per capita cost of data breach declined from €154 in 2016 to €149 in this year’s research, of which €90 pertains to indirect costs including abnormal turnover or churn of customers, and €59 pertains to direct costs. This year, the average total organizational cost of data breach decreased from €3.61 million in 2016 to €3.42 million in 2017.

**Companies more effectively reduce the size of data breach and loss of customers.** We report four key data breach metrics to compare differences between 2017 and 2016. The average total cost and per capita cost of data breach decreased by 5.4 percent and 3.3 percent, respectively. The average data breach size (number of records lost or stolen) decreased by 6.1 percent, and abnormal churn (the unexpected loss of customers following a data breach) declined by 3.4 percent.

**Certain industries have higher data breach costs.** Financial services, services and industrial companies generally had a per capita cost above the mean of €149. Public sector and transportation companies had a per capita cost well below the mean.

**Malicious or criminal attacks are most often the cause of a data breach.** Forty-six percent of organizations had a malicious or criminal attack. Thirty-four percent of data breaches involved system glitches, including a combination of both IT and business process failures, and 20 percent of all incidents involved a negligent employee or contractor (i.e. human factor).

**Malicious attacks are the costliest.** The costliest breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experienced malicious or criminal attacks had the highest per capita cost (€161). This was followed by system glitches at €146 and negligence or human error at €127.

**Four new factors are added to this year’s cost analysis.** The following factors that influence data breach costs were added to this year’s research: (1) compliance failures, (2) the extensive use of mobile platforms, (3) Chief Privacy Officer (CPO) appointment and (4) the use of security analytics. The appointment of a CPO and the use of security analytics decreased the cost of data breach by €1.2 and €7, respectively. However, data breaches caused by compliance failures and extensive use of mobile platforms, increased the per capita cost by €12 and €9.7 per compromised record, respectively.

**The more records lost, the higher the cost of the data breach.** In this year’s study, companies that had a data breach involving less than 10,000 records had an average cost of data breach of €1.46 million. Companies that had a data breach with more than 50,000 lost or stolen records had an average cost of €7.30 million.

**The more churn, the higher the cost of data breach.** Companies that had a churn rate of less than 1 percent the average total cost was €2.52 million. In contrast, companies that lost more than 4 percent of their existing customers had an average total cost of data breach of €6.32 million.

**Certain industries are more vulnerable to churn.** Companies in financial services, life science and services experienced relatively high abnormal churn. In contrast, public sector, media and retail companies experienced a relatively low abnormal churn.

---

3Malicious and criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.
Detection and escalation costs increase. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Detection and escalation costs increased from €1.00 million in 2016 to €1.13 million in 2017.

Notification costs decrease. These costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements and engagement of outside experts. This year’s average notification costs were €0.19 million, a slight decrease from last year’s study (€0.21 million in notification costs).

Post data breach costs decrease. Following a data breach, organizations typically have costs associated with help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average post data breach costs decreased from €1.11 million in 2016 to €1.02 in this year’s study.

Lost business costs decrease. Lost business costs significantly decreased in this year’s study. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. These costs decreased from €1.29 million to €1.08 million in 2017.

Direct and indirect costs decrease. Indirect costs include the time, effort and other organizational resources used to resolve the data breach. This includes employees’ assistance in data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn. Indirect costs decreased from €92 to €90. Direct costs refer to the direct expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services. Direct costs decreased from €62 in 2016 to €59 in 2017.

The time to identify and contain data breaches impacts costs. In this year’s study, it took companies an average of 141 days to detect that an incident occurred and an average of 43 days to contain an incident. If the mean time to identify (MTTI) was less than 100 days, the average cost to identify was €2.39 million. However, if the MTTI was greater than 100 days, the cost rose to €4.45 million. If the mean time to contain (MTTC) the breach was less than 30 days, the average cost was €2.71 million. If the MTTC was 30 days or longer, the cost rose to €4.12 million.
Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual’s name and a medical record and/or a financial record or debit card are potentially put at risk—either in electronic or paper format. In our study, we have identified three main causes of a data breach. These are a malicious or criminal attack, system glitch or human error. The cost of data breach may vary according to the cause and safeguards in place at the time of the data breach.

What is a compromised record? We define a record as information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples include a retail company’s database with an individual’s name associated with credit card information and other personally identifiable information, or a health insurer’s record of the policyholder with physician and payment information. In this year’s study, each lost or stolen record cost the organization an average of €149.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a 10-month period. Recruiting organizations for the 2017 study began in February 2016 and interviews were completed in March 2017. In each of the 35 participating organizations, we spoke with IT, compliance and information security practitioners who are knowledgeable about their organization’s data breach and the costs associated with resolving the breach. For privacy purposes, we did not collect any organization-specific information.

How do you calculate the cost of data breach? To calculate the average cost of data breach, we collected both the direct and indirect expenses the organization incurs. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communications as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

How does benchmark research differ from survey research? The unit of analysis in the Cost of Data Breach Study was the organization. In survey research, the unit of analysis is the individual. We recruited 35 organizations to participate in this study. Data breaches ranged from a low of 5,001 compromised records to slightly more than 81,800 compromised records.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as one involving millions of lost or stolen records? The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience. To be representative of the population of German organizations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we did not include data breaches of more than 100,000 compromised records in our analysis.

Do you track the same organizations each year? Each annual study involves a different sample of companies. In other words, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company’s industry, headcount, geographic footprint and size of data breach. Since starting this research more than nine years ago, we have studied the data breach experiences of 252 German organizations.
Part 2. Key Findings

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

- Trends in the cost of data breach
- The root causes of a data breach
- Factors that influence the cost of data breach
- Trends in the cost components of a data breach
- Time to identify and contain data breaches affects the cost
- Trends in practices to reduce the risk and consequences of a data breach

Trends in the cost of data breach

The cost of data breach decreases. Figure 1 reports the nine-year average per capita cost of a data breach.\(^4\) According to this year’s benchmark findings, data breaches cost companies an average of €149 per compromised record, of which €90 pertains to indirect costs such as abnormal turnover or churn of existing and future customers. Last year’s indirect costs were €92. Direct costs, such as investment in technologies or legal fees, decreased from €62 to €59.

Figure 1. The average per capita cost of data breach over the past nine years
Bracketed number defines the benchmark sample size
Measured in Euros

\(^4\)Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of compromised records.
The average total organizational cost of data breach decreases. Figure 2 shows the nine-year trend in the total organizational cost of data breach. This year, the average total cost of data breach decreased from €3.61 million in 2016 to €3.42 million this year.

Figure 2. The average total organizational cost of data breach over the past nine years
Measured in Euros (millions)

Measures reveal why data breach costs decrease. Figure 3 reports four key data breach metrics that reveal differences between 2017 and 2016. The average total cost and per capita cost decreased, 5.4 percent and 3.3 percent, respectively. The average data breach size (number of records lost or stolen) decreased by 6.1 percent and abnormal churn, the greater than expected loss of customers following a data breach, declined by 3.4 percent. This suggests organizations have successfully maintained the loyalty of their customers following the breach incident.

Figure 3. Cost of data breach measures
Net change defined as the difference between the 2017 and 2016 results
Certain industries have higher data breach costs. Figure 4 reports the per capita costs for 13 industries. While a small sample size prevents us from generalizing differences among industry categories, financial services, services and industrial companies generally had a per capita cost above the mean of €149. Public sector and transportation companies generally had a per capita cost well below the mean.

Figure 4. Per capita cost by industry
Measured in Euros

<table>
<thead>
<tr>
<th>Industry</th>
<th>Per Capita Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>€ 217</td>
</tr>
<tr>
<td>Services</td>
<td>€ 203</td>
</tr>
<tr>
<td>Industrial</td>
<td>€ 177</td>
</tr>
<tr>
<td>Life science</td>
<td>€ 173</td>
</tr>
<tr>
<td>Energy</td>
<td>€ 162</td>
</tr>
<tr>
<td>Consumer</td>
<td>€ 155</td>
</tr>
<tr>
<td>Technology</td>
<td>€ 151</td>
</tr>
<tr>
<td>Communications</td>
<td>€ 132</td>
</tr>
<tr>
<td>Media</td>
<td>€ 129</td>
</tr>
<tr>
<td>Retail</td>
<td>€ 125</td>
</tr>
<tr>
<td>Hospitality</td>
<td>€ 116</td>
</tr>
<tr>
<td>Transportation</td>
<td>€ 100</td>
</tr>
<tr>
<td>Public sector</td>
<td>€  95</td>
</tr>
</tbody>
</table>
The root causes of a data breach

Most data breaches are caused by malicious or criminal attacks. Figure 5 summarizes the main root causes of a data breach for all 35 German organizations. Forty-six percent had a malicious or criminal attack. Thirty-four percent involved system glitches, including a combination of both IT and business process failures, and 20 percent of all incidents involved a negligent employee or contractor (human factor).

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

Malicious attacks are the costliest. Figure 6 reports the per capita cost of data breach for three conditions or root causes of the breach incident. Malicious or criminal attacks resulted in the highest per capita cost of €161. This was followed by system glitch at €146, and negligence or human error resulted in a per capita cost of €127.

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

---

4 Malicious and criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

6 Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation.
Factors that influence the cost of data breach

Four new factors are added to this year’s cost analysis. As shown in Figure 7, the following factors that influence data breach costs were added to this year’s research: (1) compliance failures, (2) the extensive use of mobile platforms, (3) CPO appointment and (4) the use of security analytics. The appointment of a CPO and the use of security analytics decreased the cost of data breach by €1.2 and €7, respectively. However, data breaches caused by compliance failures and the extensive use of mobile platforms, increased the per capita cost by €12 and €9.7 per compromised record, respectively.

To illustrate how these factors may affect cost, the extensive use of encryption reduced the average per capita cost from €149 to €133.4 (decreased cost = -€15.6). In contrast, a data breach involving third parties increased the average per capita cost from €149 to €161.5 (increased cost = +€12.5).

**Figure 7. Impact of 20 factors on the per capita cost of data breach**

Measured in Euros

![Chart showing the impact of various factors on the per capita cost of data breach.](chart)

- Extensive use of encryption: €15.6
- Incident response team: €11.9
- Participation in threat sharing: €8.8
- BCM involvement: €8.0
- Employee training: €8.0
- Extensive use of DLP: €7.1
- Use of security analytics: €7.0
- CISO appointed: €6.4
- Board-level involvement: €5.5
- Insurance protection: €4.2
- Data classification schema: €3.9
- CPO appointed: €1.2
- Consultants engaged: €1.0
- Provision of ID protection: €1.8
- Rush to notify: €2.7
- Lost or stolen devices: €6.5
- Extensive use of mobile platforms: €9.7
- Extensive cloud migration: €10.9
- Compliance failures: €12.0
- Third party involvement: €12.5

Difference from mean
The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of a data breach and the size of the incident in ascending order by size range. In this year’s study, the average cost of data breach for companies with a data breach involving less than 10,000 records was €1.46 million. If the incident involved more than 50,000 lost or stolen records, the average total cost was €7.30 million.

**Figure 8. Average total cost of data breach by size**
Measured in Euros (millions)

![Bar chart showing cost of data breach by size]

The more churn, the higher the cost of data breach. Figure 9 reports the average total cost of data breach in ascending range of abnormal churn. Companies that had a churn rate of less than 1 percent, had an average data breach cost of €2.52 million. In contrast, companies that lost more than 4 percent of existing customers as the result of a data breach had an average total cost of €6.32 million.

**Figure 9. Average total cost of data breach by abnormal churn rate**
Measured in Euros (millions)

![Bar chart showing cost of data breach by churn rate]
Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate for 13 industries. Although a small sample size prevents us from generalizing the effect of industry on churn, our industry results are consistent with previous studies. Financial services, life science and services experienced relatively high abnormal churn. In contrast, public sector, media and retail companies experienced a relatively low abnormal churn.\(^7\)

**Figure 10. Abnormal churn rates by industry**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Abnormal Churn Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>6.0%</td>
</tr>
<tr>
<td>Life science</td>
<td>5.5%</td>
</tr>
<tr>
<td>Services</td>
<td>5.2%</td>
</tr>
<tr>
<td>Industrial</td>
<td>4.1%</td>
</tr>
<tr>
<td>Transportation</td>
<td>3.2%</td>
</tr>
<tr>
<td>Communications</td>
<td>2.9%</td>
</tr>
<tr>
<td>Consumer</td>
<td>2.4%</td>
</tr>
<tr>
<td>Technology</td>
<td>2.3%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>2.0%</td>
</tr>
<tr>
<td>Energy</td>
<td>1.8%</td>
</tr>
<tr>
<td>Retail</td>
<td>1.3%</td>
</tr>
<tr>
<td>Media</td>
<td>1.0%</td>
</tr>
<tr>
<td>Public sector</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

\(^7\)Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.
Trends in the cost components of a data breach

Detection and escalation costs reach a new high. Figure 11 shows the costs associated with the detection and escalation of the data breaches over the past nine years. The average detection and escalation costs increased from €1.00 million in 2016 to €1.13 million in 2017. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors.

Figure 11. Average detection and escalation costs over the past nine years
Measured in Euros (millions)

Notification costs continue to decline. Figure 12 reports the costs associated with notification activities. This year’s average notification costs decreased to €0.19 million from €0.21 million in 2016. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements and engagement of outside experts.

Figure 12. Average notification costs over the past nine years
Measured in Euros (millions)
Post data breach costs decrease. Figure 13 shows the costs associated with ex post (after-the-fact) activities over nine years. These costs decreased from an average of €1.11 million in 2016 to €1.02 million in this year’s study. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions.

Figure 13. Average ex post response costs over the past nine years
Ex post costs measured in Euros (millions)

Lost business costs decrease. Figure 14 shows that lost business costs associated with data breach incidents decreased from €1.29 million in 2016 to €1.08 million in 2017. Such costs include abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

Figure 14. Average lost business costs over the past nine years
Lost business costs measured in Euros (millions)
Both indirect and direct costs decrease. Figure 15 reports the direct and indirect cost components of data breach on a per capita basis. Indirect costs decreased by €2, from €92 in 2016 to €90 in this year’s research. Direct costs decreased by €3, from €62 in 2016 to €59 million in 2017.

Indirect costs include the time, effort and other organizational resources deployed to remediate a data breach. These costs include employees’ assistance to help in the data breach notification efforts or in the investigation of the incident. Indirect costs also include the loss of goodwill and customer churn. Direct costs refer to the direct expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm or offering victims identity protection services.

**Figure 15. Trends in indirect and direct costs over the past nine years**
Measured in Euros

![Bar chart showing trends in indirect and direct costs over the past nine years](image)
The time to identify and contain data breaches affects the cost

The faster the data breach is identified and contained, the lower the costs. The 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 respond and resolve the data breach.

As shown in Figure 16, it took an average of 141 days to detect an incident and an average of 43 days to contain an incident.

**Figure 16. Days to identify and contain the data breach**

![Bar chart showing mean time to identify (MTTI) and mean time to contain (MTTC).]

Figure 17 highlights the importance of having an incident response plan in place. If the MTTI was less than 100 days, the average cost to identify the data breach was €2.39 million. However, if the MTTI was greater than 100 days, the average cost rose significantly to €4.45 million.

**Figure 17. Mean time to identify and average total cost**

Measured in Euros (millions)

![Bar chart showing total cost for different MTTI values.](image)
Similarly, if the time it took to contain a breach was less than 30 days, the cost to contain the breach was €2.71 million. If it took 30 days or longer to contain the breach, the cost rose significantly to €4.12 million, as shown in Figure 18.

**Figure 18. Mean time to contain and average total cost**
Measured in Euros (millions)

The most difficult and time-consuming incident to detect and contain, as shown in Figure 19, was a malicious or criminal attack (217 days). Data breaches caused by human error or system glitches took far less time to detect and contain (119 days and 176 days, respectively).

**Figure 19. Days to identify and contain the data breach by root cause**
Trends in practices to reduce the risk and consequences of a data breach

Companies reported lower costs to respond to and remediate a data breach. Investments in encryption, incident response planning, participation in threat sharing and involvement of business continuity management programs following a data breach all appear to have reduced data breach costs.

Table 1 reports the preventive measures companies implemented following a data breach over the past eight years. The most popular measures or steps taken were: the expanded use of encryption (69 percent), endpoint security solutions (55 percent), security intelligence systems (49 percent), strengthening of perimeter controls (46 percent), and security certification or audit (44 percent).

Since 2010, investments in identity and access management have increased by 9 percent. Investments in training and awareness programs have increased by 4 percent. Security certification and audit has increased by 3 percent. Deployment of all other preventive measures decreased.

<table>
<thead>
<tr>
<th>Table 2. Preventive measures and controls implemented after the data breach</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data loss prevention (DLP) solutions</td>
<td>59%</td>
<td>51%</td>
<td>56%</td>
<td>53%</td>
<td>49%</td>
<td>47%</td>
<td>45%</td>
<td>41%</td>
</tr>
<tr>
<td>Endpoint security solutions</td>
<td>59%</td>
<td>75%</td>
<td>68%</td>
<td>64%</td>
<td>59%</td>
<td>53%</td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td>Expanded use of encryption</td>
<td>77%</td>
<td>70%</td>
<td>65%</td>
<td>67%</td>
<td>61%</td>
<td>69%</td>
<td>70%</td>
<td>69%</td>
</tr>
<tr>
<td>Identity and access management solutions</td>
<td>27%</td>
<td>24%</td>
<td>30%</td>
<td>28%</td>
<td>26%</td>
<td>34%</td>
<td>35%</td>
<td>36%</td>
</tr>
<tr>
<td>Manual control practices</td>
<td>14%</td>
<td>11%</td>
<td>9%</td>
<td>9%</td>
<td>12%</td>
<td>9%</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>Security certification or audit</td>
<td>41%</td>
<td>34%</td>
<td>45%</td>
<td>48%</td>
<td>39%</td>
<td>41%</td>
<td>40%</td>
<td>44%</td>
</tr>
<tr>
<td>Security intelligence systems</td>
<td>68%</td>
<td>58%</td>
<td>62%</td>
<td>59%</td>
<td>55%</td>
<td>53%</td>
<td>55%</td>
<td>49%</td>
</tr>
<tr>
<td>Strengthening of perimeter controls</td>
<td>73%</td>
<td>69%</td>
<td>61%</td>
<td>55%</td>
<td>50%</td>
<td>53%</td>
<td>50%</td>
<td>46%</td>
</tr>
<tr>
<td>Training and awareness programs</td>
<td>27%</td>
<td>26%</td>
<td>23%</td>
<td>21%</td>
<td>21%</td>
<td>25%</td>
<td>26%</td>
<td>31%</td>
</tr>
</tbody>
</table>

*Please note that a company may be implementing more than one preventive measure.
Table 2 provides the percentage cost changes for 11 cost categories over nine years. As can be seen, most cost categories appear to be relatively stable over time. The two highest cost categories were investigation and forensics and lost customer business.

<table>
<thead>
<tr>
<th>Table 2. Percentage data breach cost categories</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations and forensics</td>
<td>31%</td>
<td>29%</td>
<td>27%</td>
<td>32%</td>
<td>34%</td>
<td>32%</td>
<td>35%</td>
<td>35%</td>
<td>37%</td>
</tr>
<tr>
<td>Audit and consulting services</td>
<td>10%</td>
<td>8%</td>
<td>9%</td>
<td>10%</td>
<td>9%</td>
<td>11%</td>
<td>10%</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>Outbound contact costs</td>
<td>9%</td>
<td>10%</td>
<td>10%</td>
<td>9%</td>
<td>7%</td>
<td>6%</td>
<td>5%</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>Inbound contact costs</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>5%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Public relations/communications</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Legal services – defense</td>
<td>2%</td>
<td>3%</td>
<td>3%</td>
<td>2%</td>
<td>4%</td>
<td>2%</td>
<td>4%</td>
<td>5%</td>
<td>4%</td>
</tr>
<tr>
<td>Legal services - compliance</td>
<td>5%</td>
<td>4%</td>
<td>4%</td>
<td>6%</td>
<td>5%</td>
<td>7%</td>
<td>6%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Free or discounted services</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Identity protection services</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Lost customer business</td>
<td>29%</td>
<td>32%</td>
<td>33%</td>
<td>29%</td>
<td>29%</td>
<td>28%</td>
<td>29%</td>
<td>30%</td>
<td>27%</td>
</tr>
<tr>
<td>Customer acquisition cost</td>
<td>5%</td>
<td>6%</td>
<td>6%</td>
<td>5%</td>
<td>5%</td>
<td>7%</td>
<td>6%</td>
<td>7%</td>
<td>6%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Part 4. 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 in which they engage to resolve a 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 for data breach victims and regulators
- Implementing call center procedures and specialized training

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

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services offered to breach victims
- 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, though not as a direct cash outlay.
- **Opportunity cost** – the costs 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 as follows:

- **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.
- **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 costs stem from present and future customers' diminished trust or confidence. Accordingly, Ponemon 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 and 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 based on estimates provided by management during the benchmark interview process.\(^8\)

- **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.\(^9\) In these cases, we expect the business cost category to be lower when data breaches do not involve customer or consumer data (including transactional payment information).

---

\(^8\)In several instances, turnover is partial, as in cases where breach victims 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.

\(^9\)In this study, we consider citizen, patient and student information as customer data.
Part 4. Organizational Characteristics and Benchmark Methods

Figure 20 shows the distribution of benchmark organizations by their primary industry classification. In this year’s study, 13 industries were represented. The largest sectors were industrial, financial services and technology. Financial services companies include banks, insurance, investment management and payment processors.

Figure 20. Distribution of the benchmark sample by industry segment

All participating organizations experienced one or more data breach incidents during the past year. Our benchmark instrument captured descriptive information from IT, compliance and information security practitioners about the full cost impact of a breach involving the loss or theft of customer or consumer information. Moreover, our instrument required these practitioners to estimate opportunity costs associated with program activities.

Estimated data breach cost components were captured using a rating form. In most cases, the researcher conducted follow-up interviews to obtain additional facts, including estimated abnormal churn rates resulting from the company’s most recent breach event involving 1,000 or more compromised records.10

---

10 Our sampling criteria only included companies experiencing a data breach between 1,000 and 100,000 lost or stolen records sometime during the past 12 months. We excluded catastrophic data breach incidents to avoid skewing overall sample findings.
Data collection methods did not include actual accounting information, but instead relied on 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, labor and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You may 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 cost category presented 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 better quality results.
Part 5. Limitations

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, inherent limitations with this benchmark research need to be carefully considered before drawing conclusions from findings.

- **Non-statistical results**: Our study draws on a representative, non-statistical sample of 35 German organizations that experienced 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. Thirty-five companies completed the benchmark process. Non-response bias was not tested so it is always possible that 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 the results is influenced by the degree to which the frame is representative of the population of companies being studied. We believe that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- **Company-specific information**: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

- **Unmeasured factors**: To keep the interview script concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

- **Extrapolated cost results**: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. Although certain checks and balances can be incorporated into the benchmark process, the possibility exists 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 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 the following:

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 country reports are available at [www.ibm.com/security/data-breach](http://www.ibm.com/security/data-breach)

---

Ponemon Institute LLC  
*Advancing Responsible Information Management*

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