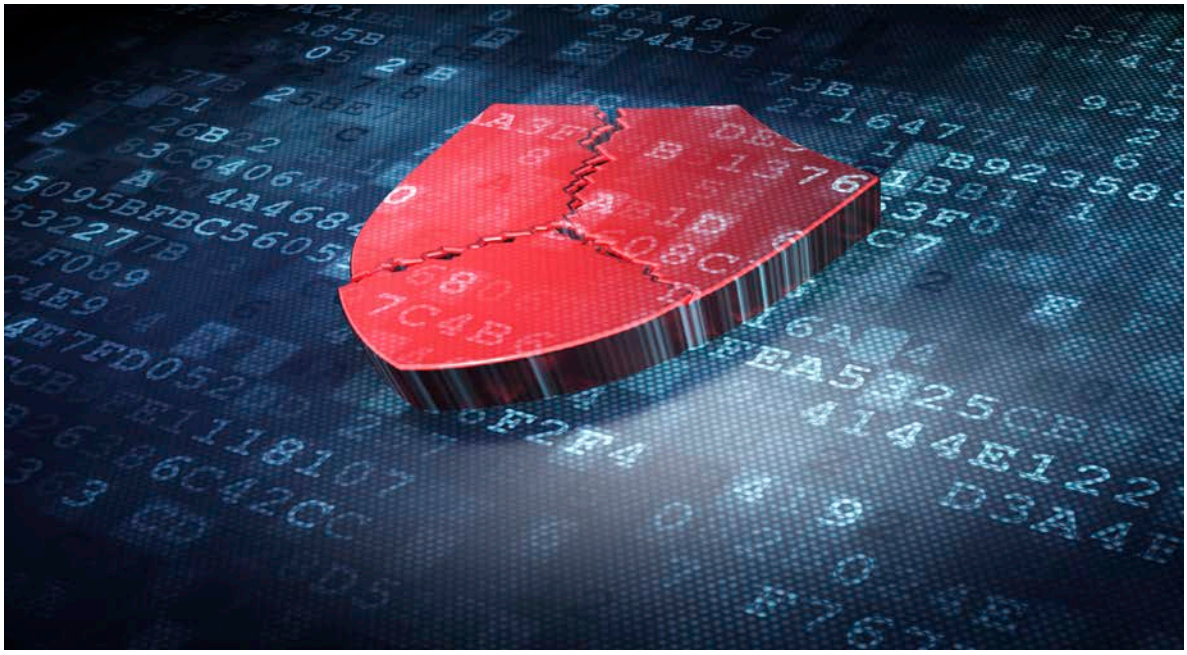


2014 Cost of Data Breach Study: Global Analysis

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
May 2014

2014[1] Cost of Data Breach Study: Global Analysis

Ponemon Institute, May 2014

Part 1. Introduction

IBM and Ponemon are pleased to release the ninth annual *Cost of Data Breach Study: Global Study.* According to the research, the average total cost of a data breach for the companies participating in this research increased 15 percent to $3.5 million[2]. The average cost paid for each lost or stolen record containing sensitive and confidential information increased more than 9 percent from $136 in 2013 to $145 in this year's study.

For the first time, our study looks at the likelihood of a company having one or more data breach occurrences in the next 24 months. Based on the experiences of companies participating in our research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or stolen and the company's industry. According to the findings, organizations in India and Brazil are more likely to have a data breach involving a minimum of 10,000 records. In contrast, organizations in Germany and Australia are least likely to have a breach. In all cases, it is more likely a company will have a breach involving 10,000 or fewer records than a mega breach involving more than 100,000 records.

In this year's study, 314 companies representing the following 10 countries participated: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India and, for the first time, the Arabian region (United Arab Emirates and Saudi Arabia). All participating organizations experienced a data breach ranging from a low of approximately 2,415 to slightly more than 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.

As the findings reveal, the consolidated average per capita cost of data breach (compiled for ten countries and converted to US dollars) differs widely among the countries. Many of these cost differences can be attributed to the types of attacks and threats organizations face as well as the data protection regulations and laws in their respective countries. In this year's global study, the average consolidated data breach increased from $136 to $145. However, German and US organizations on average experienced much higher costs at $195 and $201, respectively.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States nine years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France, Australia, India, Italy, Japan, Brazil and, for the first time this year, United Emirates and Saudi Arabia. To date, 1,279 business and government (public sector) organizations have participated in the benchmarking process since the inception of this research series.

As mentioned above, this year's study examines the costs incurred by 314 companies in 16 industry sectors after those companies experienced the loss or theft of protected personal data. It is important to note the costs presented in this research are not hypothetical but are from actual data loss incidents. They are based upon cost estimates provided by the 1,690 individuals we interviewed over a ten-month period in the companies that are represented in this research.

The following are the most salient country differences measured in US dollars:

- **The most and least expensive breaches.** German and US companies had the most costly data breaches ($201 and $195 per record, respectively). These countries also experienced the highest total cost (US at $5.85 million and Germany at $4.74 million). The least costly

[1]For the first time, this report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2013 calendar year.
[2]Local currencies were converted to U.S. dollars.
[3]The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

breaches occurred in Brazil and India ($70 and $51, respectively). In Brazil, the average total cost for a company was $1.61 million and in India it was $1.37 million.

- **Size of data breaches.** On average, U.S. and Arabian region companies had data breaches that resulted in the greatest number of exposed or compromised records (29,087 and 28,690 records, respectively). On average, Japanese and Italian companies had the smallest number of breached records (18,615 and 19,034 records, respectively).
- **Causes of data breaches differ among countries.** Companies in the Arabian region and in Germany were most likely to experience a malicious or criminal attack, followed by France and Japan. Companies in India were the most likely to experience a data breach caused by a system glitch or business process failure and UK companies were more likely to have a breach caused by human error.
- **The most costly data breaches were malicious and criminal attacks.** Consolidated findings show that malicious or criminal attacks are the most costly data breaches incidents in all ten countries. U.S. and German companies experience the most expensive data breach incidents at $246 and $215 per compromised records, respectively. Brazil and India had the least costly data breach caused by malicious or criminal attackers at $77 and $60 per capita, respectively.
- **Factors that decreased and increased the cost of a data breach.** Having a strong security posture, incident response plan and CISO appointment reduced the cost per record by $14.14, $12.77 and $6.59, respectively. Factors that increased the cost were those that were caused by lost or stolen devices (+ $16.10), third party involvement in the breach (+ $14.80), quick notification (+ $10.45) and engagement of consultants (+ $2.10).
- **Business continuity management reduced the cost of a breach**. For the first time, the research reveals that having business continuity management involved in the remediation of the breach can reduce the cost by an average of $8.98 per compromised record.
- **Countries that lost the most customers following a data breach.** France and Italy had the highest rate of abnormal customer turnover or churn following a data breach. In contrast, the Arabian region and India had the lowest rate of abnormal churn.
- **Countries that spent the most and least on detection and escalation.** On average, German and French organizations spent the most on detection and escalation activities such as investigating and assessing the data breach ($1.3 million and $1.1 million, respectively). Organizations in India and the Arabian region spent the least on detection and escalation at $320,763 and $353,735 respectively.
- **Countries that spent the most and least on notification.** Typical notification costs include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts and other efforts to make sure victims are alerted to the fact that their personal information has been compromised. U.S. and German organizations on average spent the most ($509,237 and $317,635 respectively). Brazil and India spent the least amount on notification ($53,772 and $19,841, respectively).
- **Will your organization have a data breach?** As part of understanding the potential risk to an organization's sensitive and confidential information, we thought it would be helpful to understand the probability that an organization will have a data breach. To do this, we extrapolate a subjective probability distribution for the entire sample of participating companies on the likelihood of a material data breach happening over the next two years. The results show that a probability of a material data breach involving a minimum of 10,000 records is more than 22 percent. In addition to overall aggregated results, we find that the probability or likelihood of data breach varies considerably by country. India and Brazil have the highest estimated probability of occurrence at 30 percent, while Germany has an approximate 2 percent rate of occurrence.

Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual's name plus a medical record and/or a financial record or debit card is 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 costs of a data breach can vary according to the cause and the 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 can include a retail company's database with an individual's name associated with credit card information and other personally identifiable information. Or, it could be a health insurer's record of the policyholder with physician and payment information. In this year's study, the average cost to the organization if one of these records is lost or stolen is $145.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through 1,690 interviews conducted over a ten-month period. Recruiting organizations for the 2014 study began in January 2013 and interviews were completed in March 2014. In each of the 314 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 do not collect any organization-specific information.

How do you calculate the cost of data breach? To calculate the average cost of data breach, we collect both the direct and indirect expenses incurred by the organization. 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 communication, 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 is the organization. In survey research, the unit of analysis is the individual. We recruited 314 organizations to participate in this study. Data breaches ranged from a low of 2,415 to slightly more than 102,000 compromised records.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as those 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. In order to be representative of the population of global organizations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than approximately 100,000 compromised records in our analysis.

Are you tracking the same organizations each year? Each annual study involves a different sample of companies. In other words, we are not tracking 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 in 2005, we have studied the data breach experiences of 1,279 organizations globally.

Part 2. Key Findings

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

- Understanding the cost of data breach
- Root causes of a data breach
- Factors that influence the cost of a data breach
- Trends in the frequency of compromised records and customer turnover or churn
- Trends in the cost components of a data breach
- The likelihood an organization will have a data breach

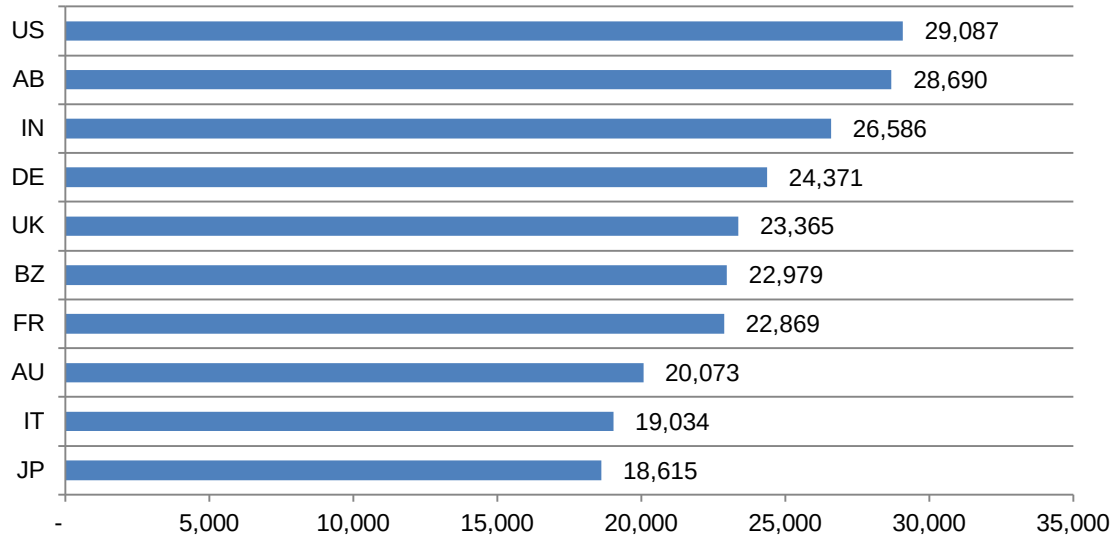
The following table lists the countries, legend and currency used in this report.

Table 1. Country legend	Legend	Case studies	Currency
Australia	AU	22	AU Dollar
Brazil	BZ	32	Real
France	FR	27	Euro
Germany	DE	30	Euro
India	IN	29	Rupee
Italy	IT	23	Euro
Japan	JP	26	Yen
United Arab Emirates & Saudi Arabia	AB	24	AED/SAR
United Kingdom	UK	40	GBP
United States	US	61	Dollar

Understanding the cost of data breach

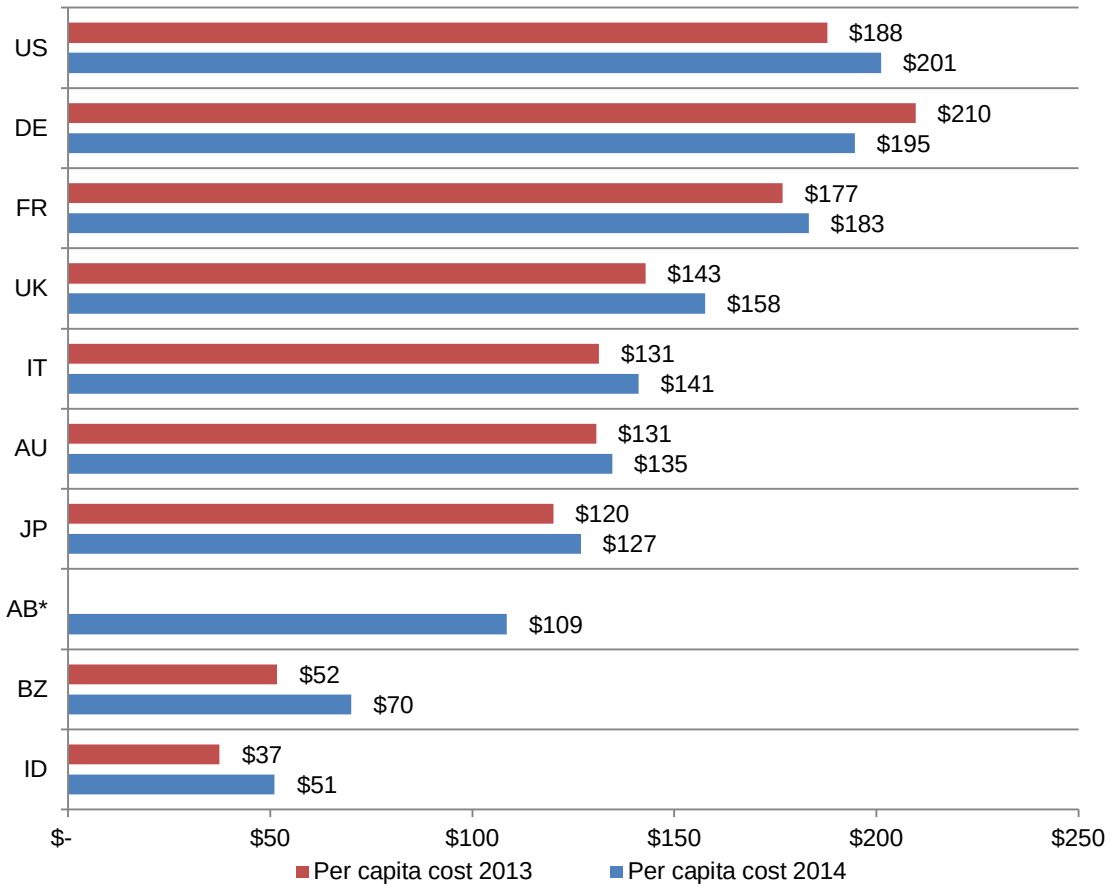
Number of exposed or compromised records. Figure 1 reports the average size of data breaches for organizations in the ten countries represented in this research. As shown, organizations in the U.S., the Arabian region and India had the largest average number of records lost or stolen.

Figure 1. The average number of breached records by country



The average per capita cost over two years. Figure 2 reports the average per capita cost of a data breach expressed in U.S. dollars for 10 country studies. As shown, there is a marked variation among country samples.[4] The consolidated average per capita cost for all countries was $145 compared to a $136 average cost calculated last year (excluding the Arabian region). The U.S. and Germany had the highest per capita costs at $201 and $195, respectively. India and Brazil had the lowest costs at $51 and $70, respectively.

Figure 2. The average per capita cost of data breach over two years
Measured in US$

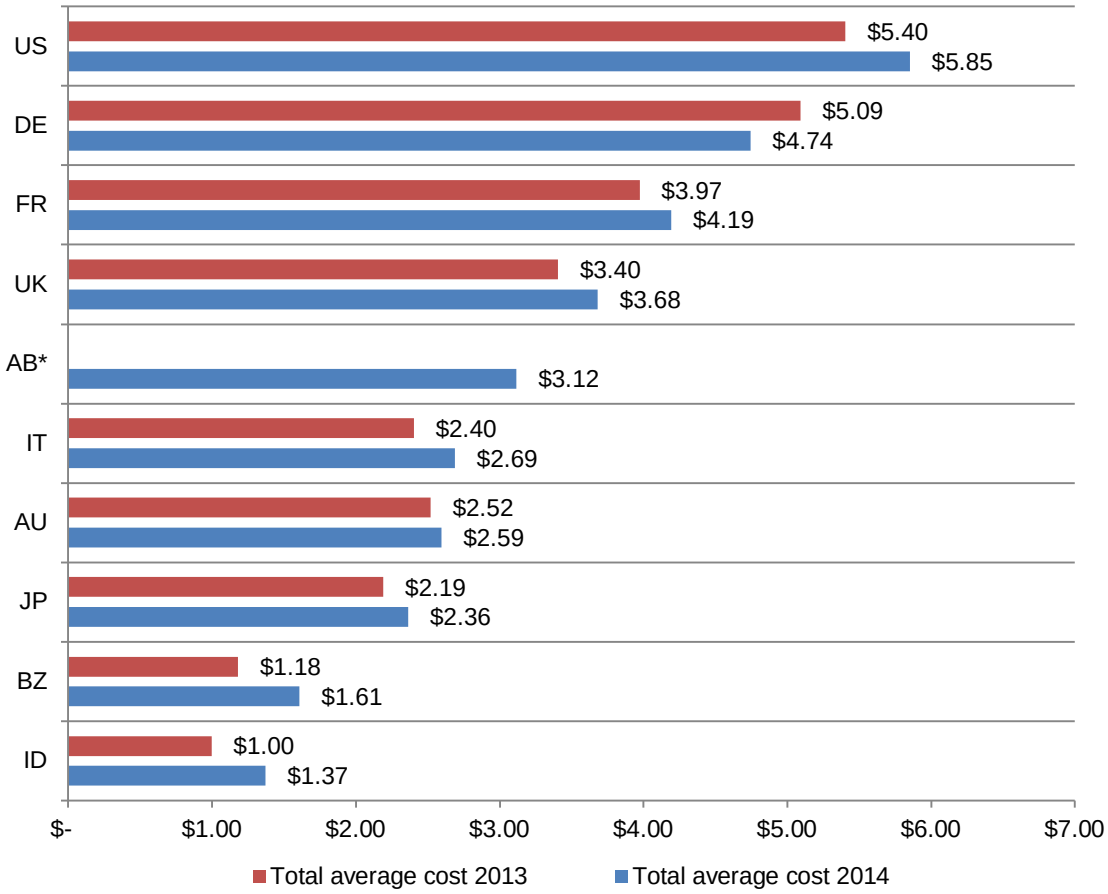


* Data not available for FY 2013

[4] Per capita cost is defined as the total cost of data breach divided by the size of the data breach (i.e., the number of lost or stolen records).

Average organizational cost of data breach varies by country. Figure 3 presents the total average cost of data breach for ten country studies in this year's study. As can be seen, the U.S. sample experienced the highest total average cost at more than $5.85 million, followed by Germany at $4.74 million. In sharp contrast, samples of Brazilian and Indian companies experienced the lowest total average cost at $1.61 million and $1.37 million, respectively.

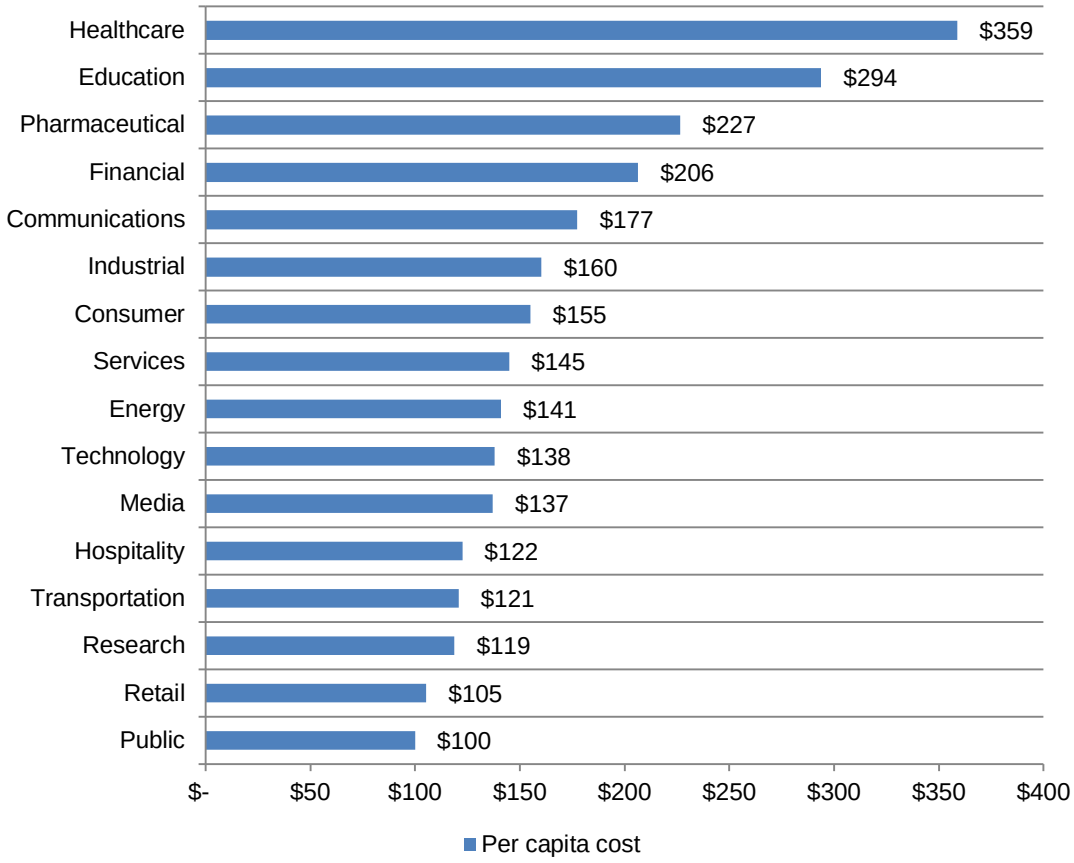
Figure 3. The average total organizational cost of data breach over two years
Measured in US$ ($000,000 omitted)



* Data not available for FY 2013

Certain industries have higher data breach costs. Figure 4 reports the per capita costs for the consolidated sample by industry classification. Heavily regulated industries such as healthcare, education, pharmaceutical and financial services had a per capita data breach cost substantially above the overall mean of $145. Public sector organizations and retail companies had a per capita cost well below the overall mean value.

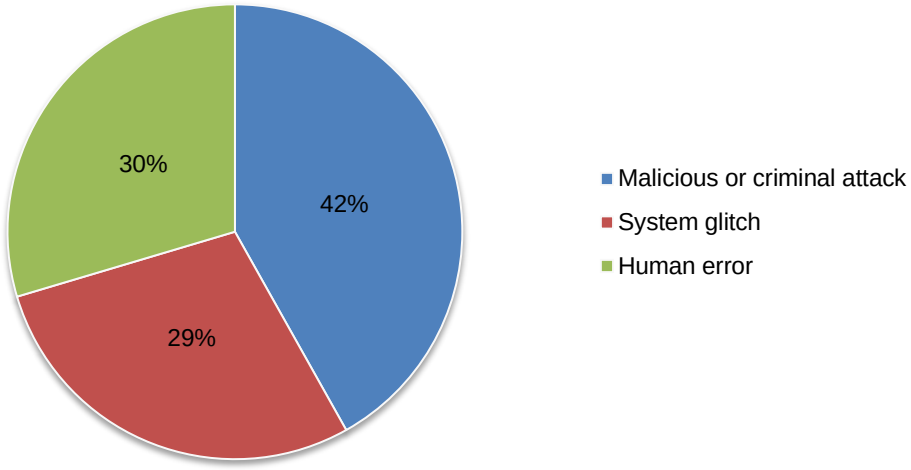
Figure 4. Per capita cost by industry classification
Consolidated view (n=314)



The root causes of data breach

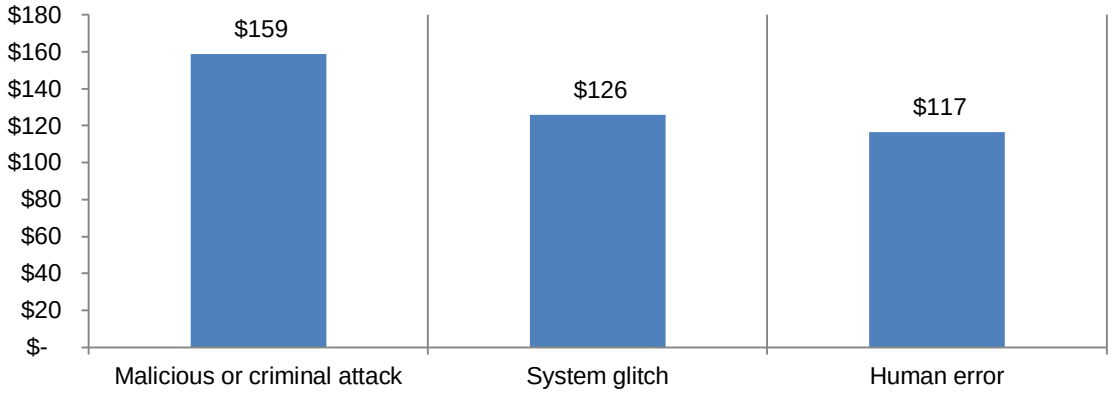
Malicious or criminal attacks are most often the cause of data breach globally.[5] Figure 5 provides a summary of the main root causes of data breach on a consolidated basis for all ten countries represented in the research. Forty-two percent of incidents involved a malicious or criminal attack, 30 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures.[6]

Figure 5. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=314)



Malicious attacks are more costly globally. Figure 6 reports the per capita cost of data breach for three root causes of the breach incident on a consolidated basis. These results show data breaches due to malicious or criminal attacks cost companies increased from and average of $157 in last year's study to $159. This is significantly above the consolidated mean of $145 per compromised record and the per capita cost for breaches caused by system glitch and human factors ($126 and $117, respectively). Last year, system glitches averaged $122 and human error stayed the same at $117.

Figure 6. Per capita cost for three root causes of the data breach
Consolidated view (n=314)
Measured in US$



[5]Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Malicious attacks can be caused by hackers or criminal insiders (employees, contractors or other third parties).
[6]The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Figure 7 presents the main root causes of data breach for 10 country samples. At 50 percent, organizations in the Arabian region and Germany were most likely to experience a malicious or criminal attack. In contrast, Indian and Brazilian companies were least likely to experience such data breaches. Indian companies were most likely to experience a data breach caused by a system glitch or business process failure.

Figure 7. Distribution of the benchmark sample by root cause of the data breach

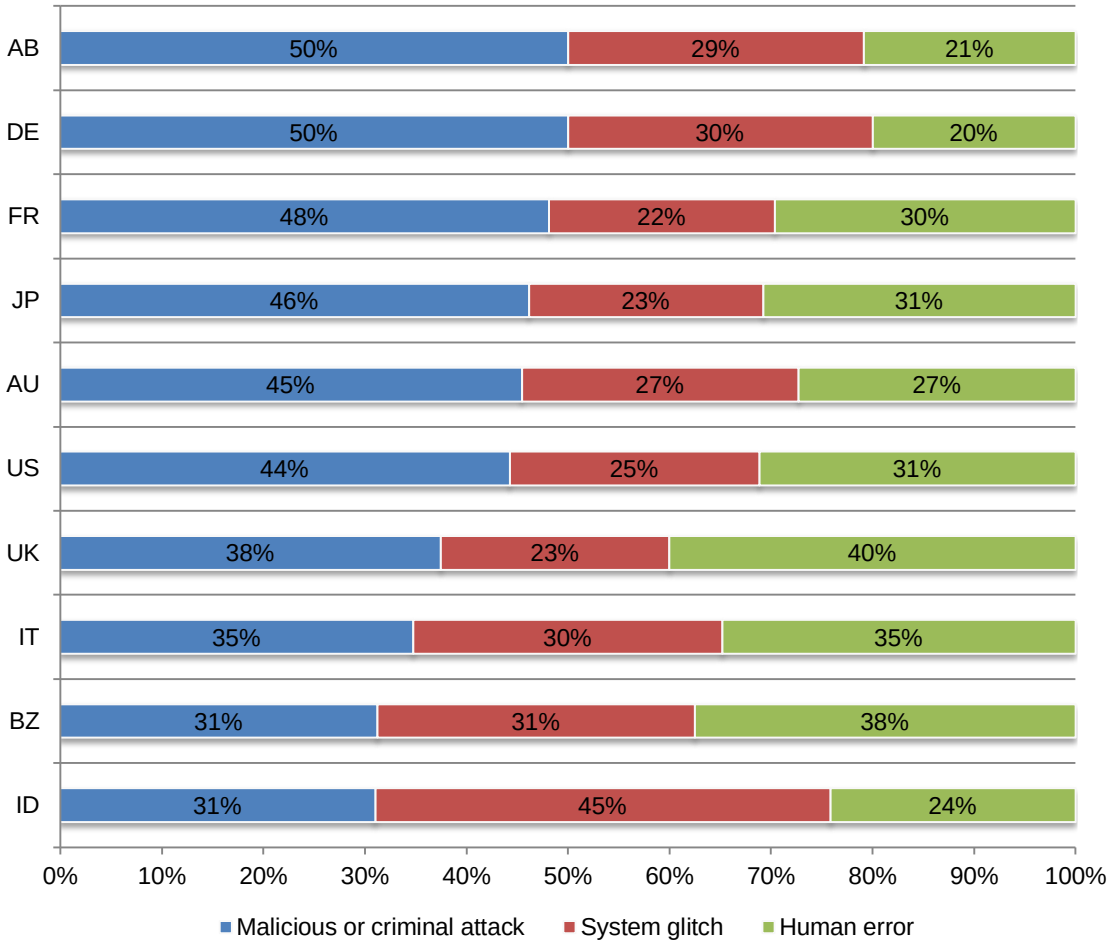
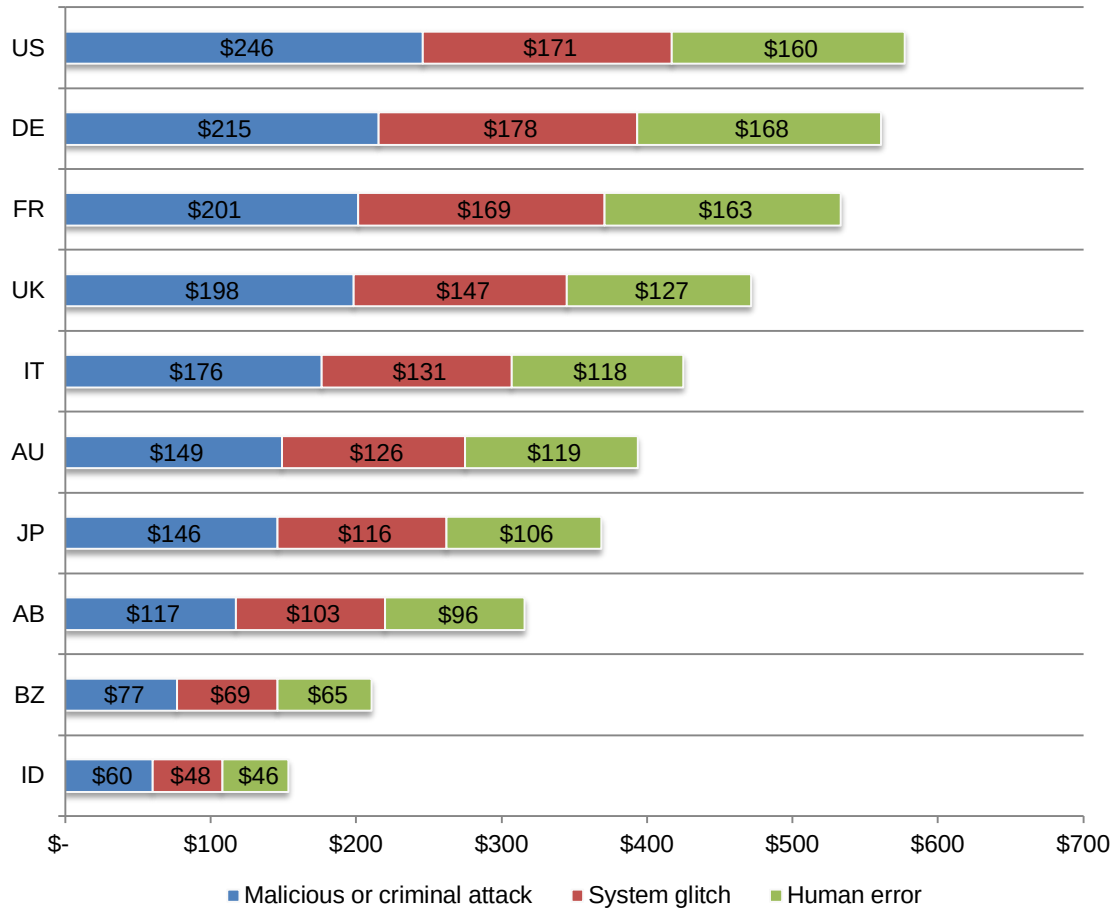


Figure 8 reports the per capita cost of data breach by country sample for three root causes. These results clearly show data breach costs resulting from malicious or criminal attacks were consistently higher than those costs resulting from system glitches or human error. This graph also shows wide variation across country samples. That is, the U.S. cost of a malicious or criminal data breach incident was $246 per compromised record. In India, this per capita cost was only $60.

Figure 8. Per capita cost for three root causes of the data breach
Measured in US$

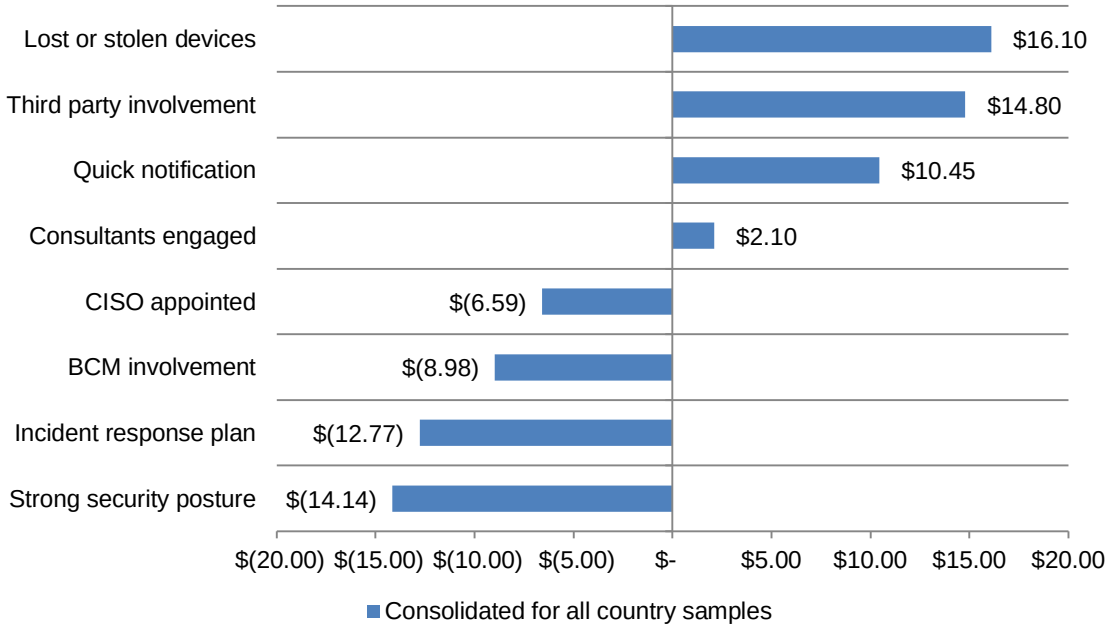


Factors that influence the cost of data breach
Measured in US$ consolidated view (n=314)

A strong security posture results in the greatest decrease in the cost of data breach. As shown in Figure 9, a strong security posture, incident response planning, business continuity management and a CISO with enterprise-wide responsibility decreases the per capita cost of data breach (shown as negative numbers). Lost or stolen devices, third party involvement in the incident, quick notification and engagement of consultants increases the per capita cost of data breach (shown as positive numbers).

For example, companies that had a strong security posture at the time of the data breach could reduce the average per record cost to $131.86 ($145 - $14.14). However, if the data breach involved lost or stolen devices the cost per record could increase to $161.10 ($145 + $16.10)

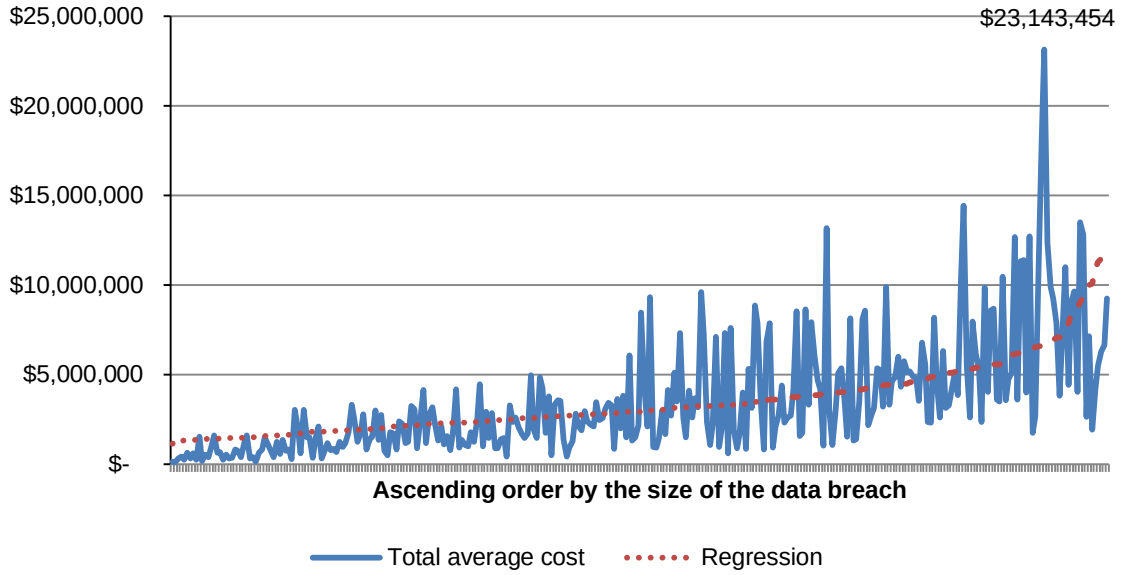
Figure 9. Impact of eight factors on the per capita cost of data breach



Trends in frequency of compromised records and customer turnover

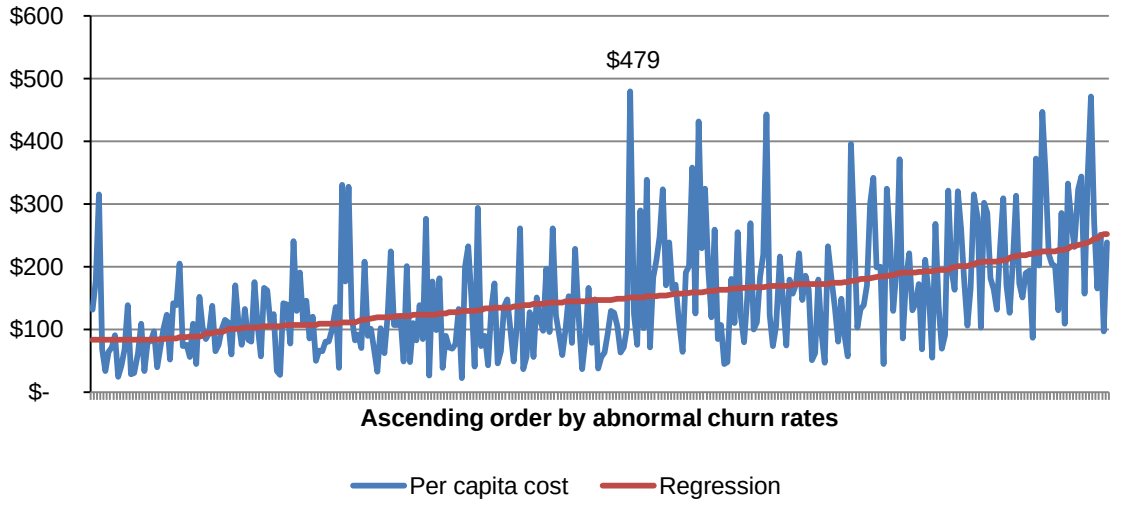
The more records lost, the higher the cost of the data breach. Figure 10 shows the relationship between the total cost of data breach and the size of the incident for 314 organizations in ascending order by the size of the breach incident. The regression line clearly indicates that the size of the data breach incident and total costs are linearly related. In this year's study, the cost ranged from $135,603 to $23,143,454

Figure 10. Total cost of data breach by size of the data breach
Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope.
Measured in US$



The more churn, the higher the per capita cost of data breach. Figure 11 reports the distribution of per capita data breach costs in ascending rate of abnormal churn for 314 organizations. The regression line is upward sloping, which suggests that abnormal churn and per capita costs are linearly related.

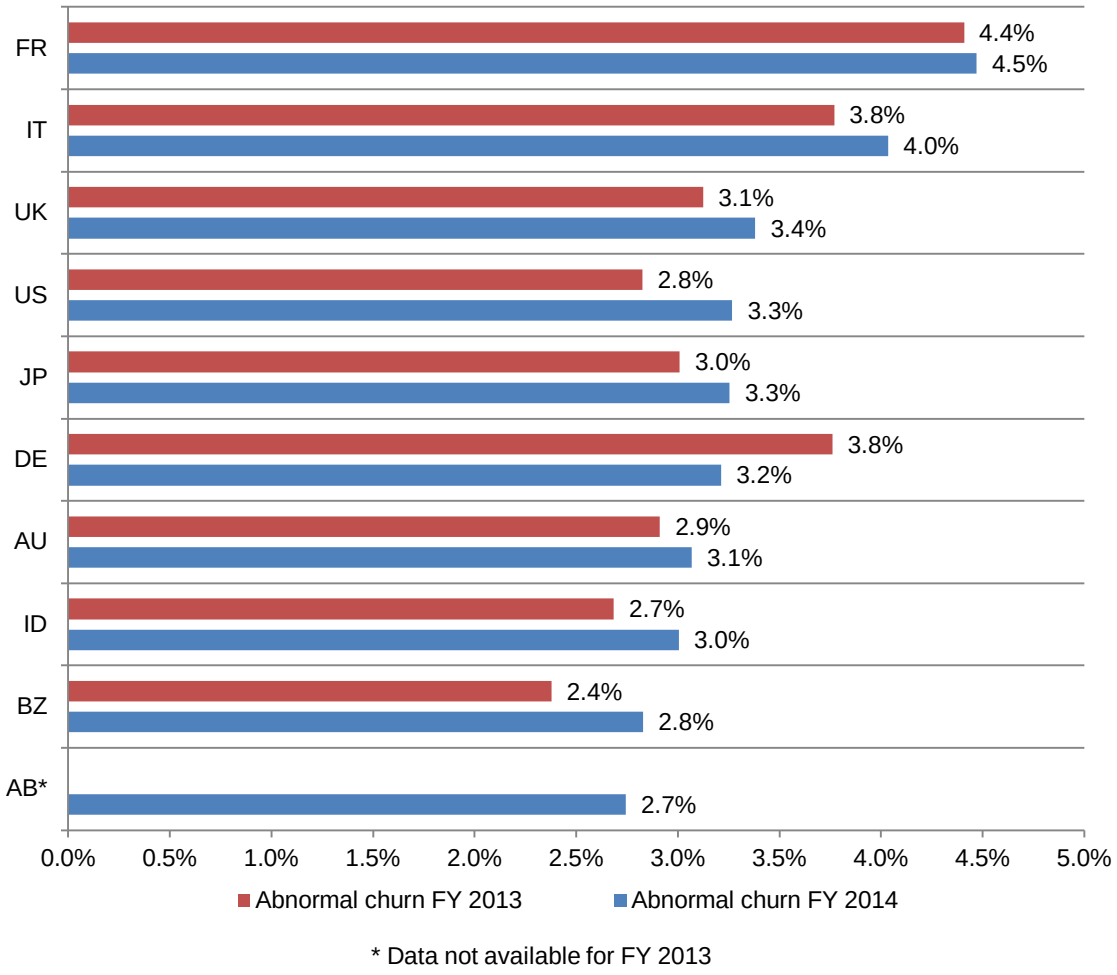
Figure 11. Distribution of abnormal churn rates in ascending order by per capita costs
Regression = Intercept + {abnormal churn rate) x β, where β denotes the slope.
Measured in US$



Certain countries are more vulnerable to churn. Figure 12 reports the average abnormal rates for the 10 countries represented in this research. Our 2014 results show marked differences among countries. France continued to experience the highest rate of churn followed by Italy. The Arabian region and Brazil experienced the lowest rate of churn.

The implication of this finding is that organizations in countries with high churn rates could significantly reduce the costs of data breach by putting an emphasis on customer retention activities to preserve reputation and brand value.

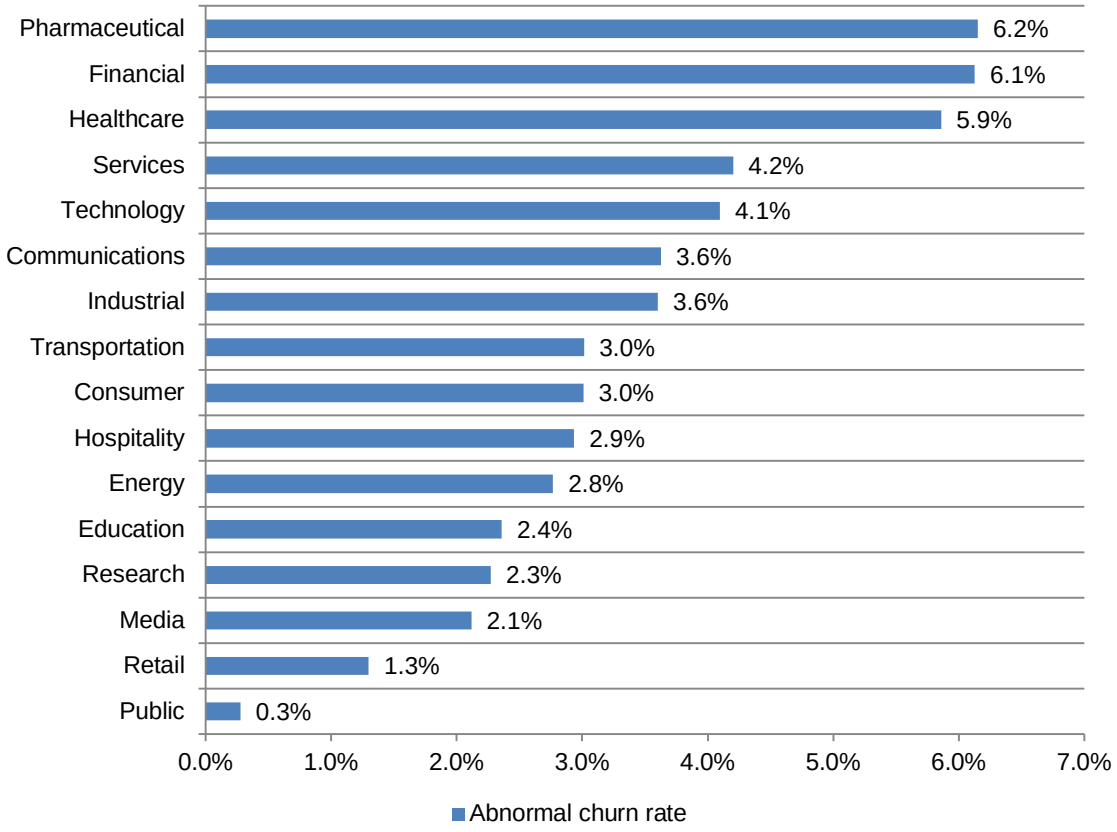
Figure 12. Abnormal churn rates over two years by country sample



* Data not available for FY 2013

Certain industries are more vulnerable to churn. Figure 13 reports the abnormal churn rate of benchmarked organizations for the 2014 study. While a small sample size prevents us from generalizing the affect of industry on customer churn rates, Pharmaceutical, financial services and healthcare organizations tend to experience relatively high abnormal churn and public sector and retail companies tend to experience a relatively low abnormal churn.[7]

Figure 13. Abnormal churn rates by industry classification of benchmarked companies
Consolidated view (n=314)

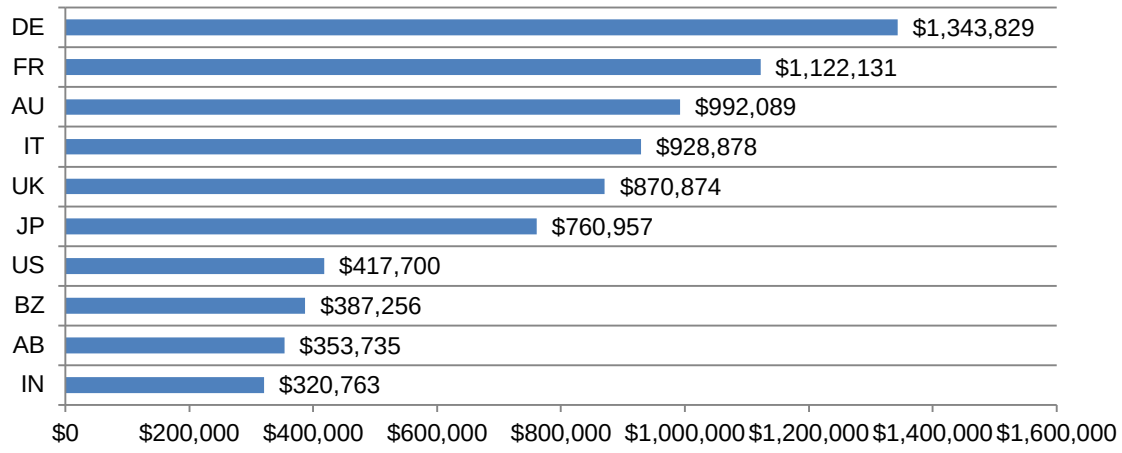


[7]Public sector organizations utilize a different churn framework given that customers of government organizations typically do not have an alternative choice.

Trends in the cost components of a data breach

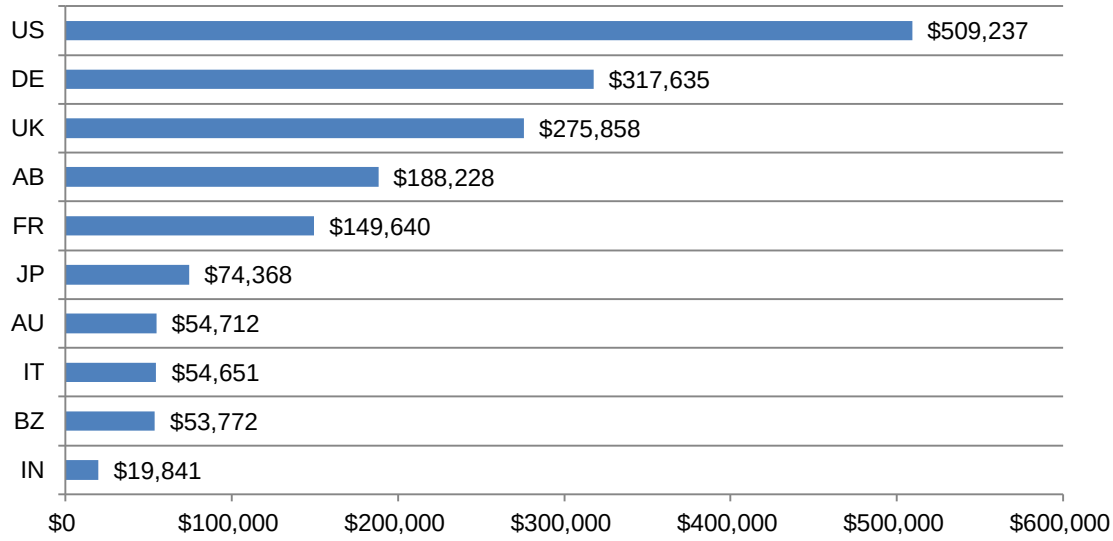
Detection and escalation costs are highest in Germany. Figure 14 presents the costs associated with detection and escalation of data breach incidents in 10 countries. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. As noted, German companies experienced the highest detection and escalation costs and India and the Arabian region experienced the lowest.

Figure 14. Average detection and escalation costs
Measured in US$



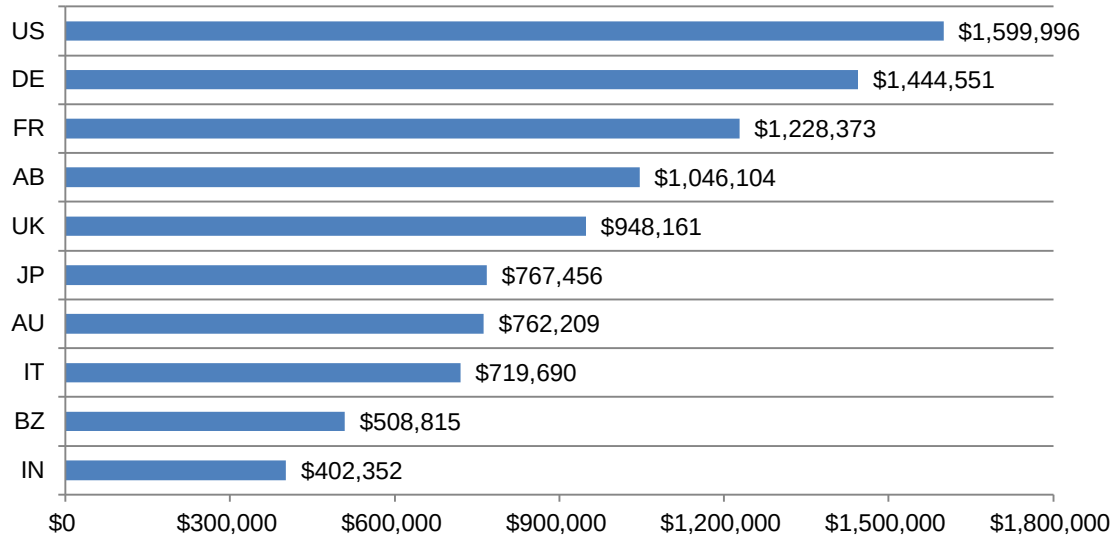
Data breach notification laws in the U.S. impact notification costs. Figure 15 reveals that companies in the U.S. have a significantly higher cost to notify victims of a data breach. India and Brazil have the lowest costs. Notification costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up.

Figure 15. Average notification costs
Measured in US$



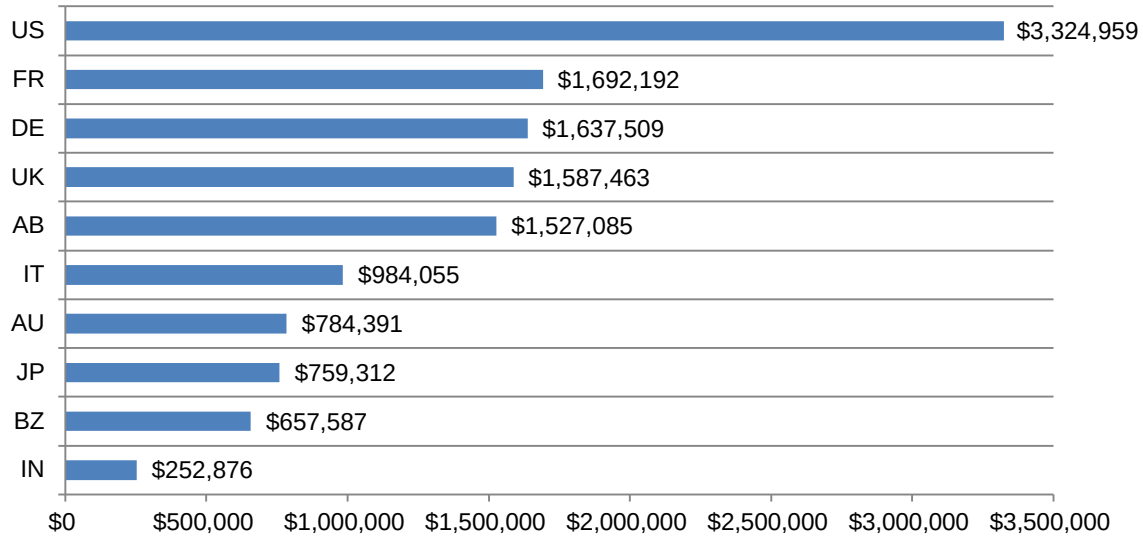
Post data breach costs are highest in the U.S. and Germany. Figure 16 shows the distribution of costs associated with ex-post (after-the-fact) activities for 10 countries. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The lowest costs were in Brazil and India.

Figure 16. Average post data breach costs
Measured in US$



U.S. organizations have the highest lost business costs. Lost business costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The highest lost business cost was an average of $3.3 million and the lowest was $252,876 in India.

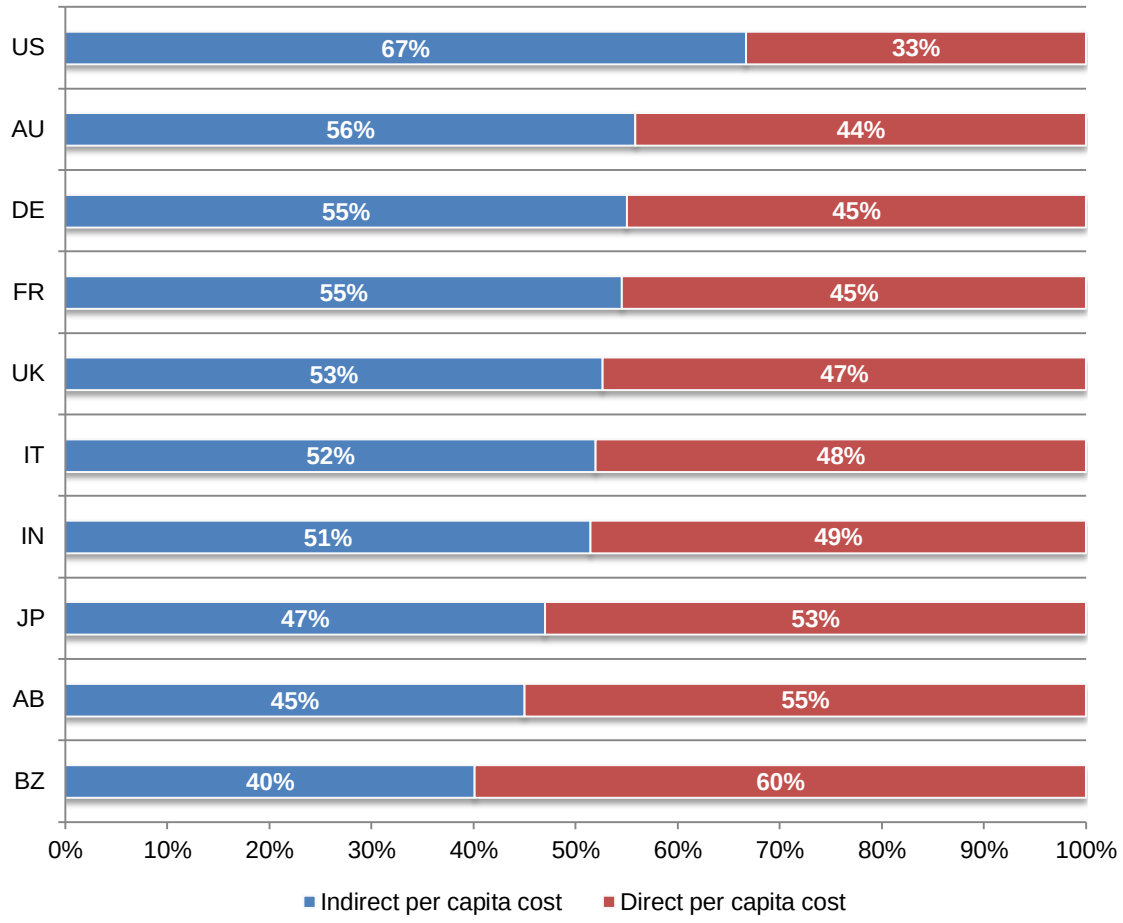
Figure 17. Average lost business costs
Measured in US$



The proportion of direct and indirect costs of data breach varies by country. 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. Indirect costs include the time, effort and other organizational resources spent during the data breach resolution. It includes the use of existing employees 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.

Figure 18 reports the direct and indirect components of a data breach on a percentage basis for 10 countries. As shown, companies in the U.S. have the highest indirect costs. Brazil and the Arabian region have the highest direct costs.

Figure 18. Percentage direct and indirect per capita data breach costs

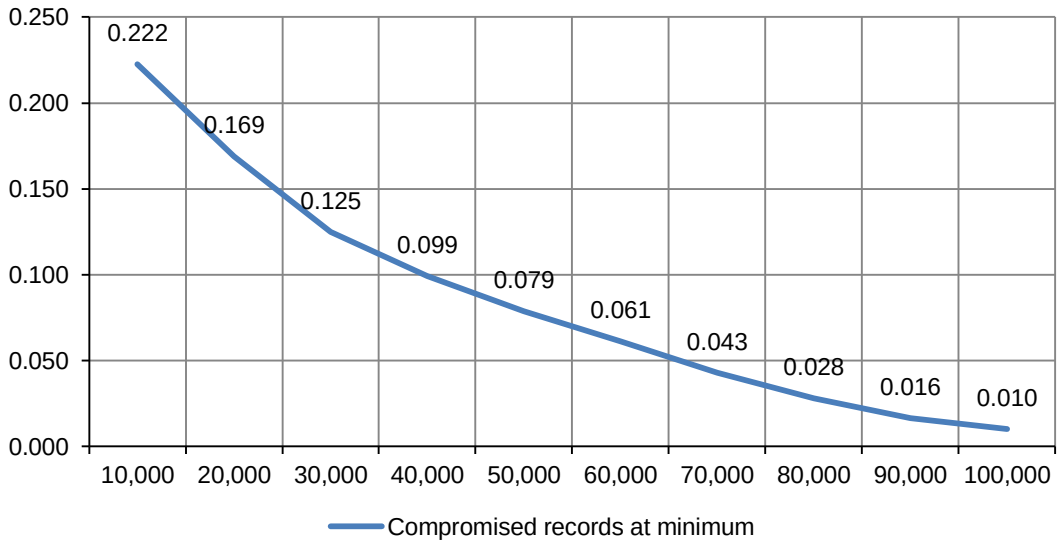


The likelihood that an organization will have a data breach

Companies are far more likely to have a small data breach than a mega breach. For the first time our research provides an analysis of the likelihood of one or more data breach occurrences in the next 24 months. Based on the experiences of organizations in our research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or stolen and the company's industry.

Figure 19 shows the subjective probabilities of breach incidents involving a minimum of 10,000 to 100,000 compromised records.[8] As can be seen, the likelihood of data breach steadily decreases as the size increases. While the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 22 percent over a 24-month period, the chances of a data breach involving a 100,000 records is less than 1 percent.

Figure 19. Probability of a data breach involving a minimum of 10,000 to 100,000 records

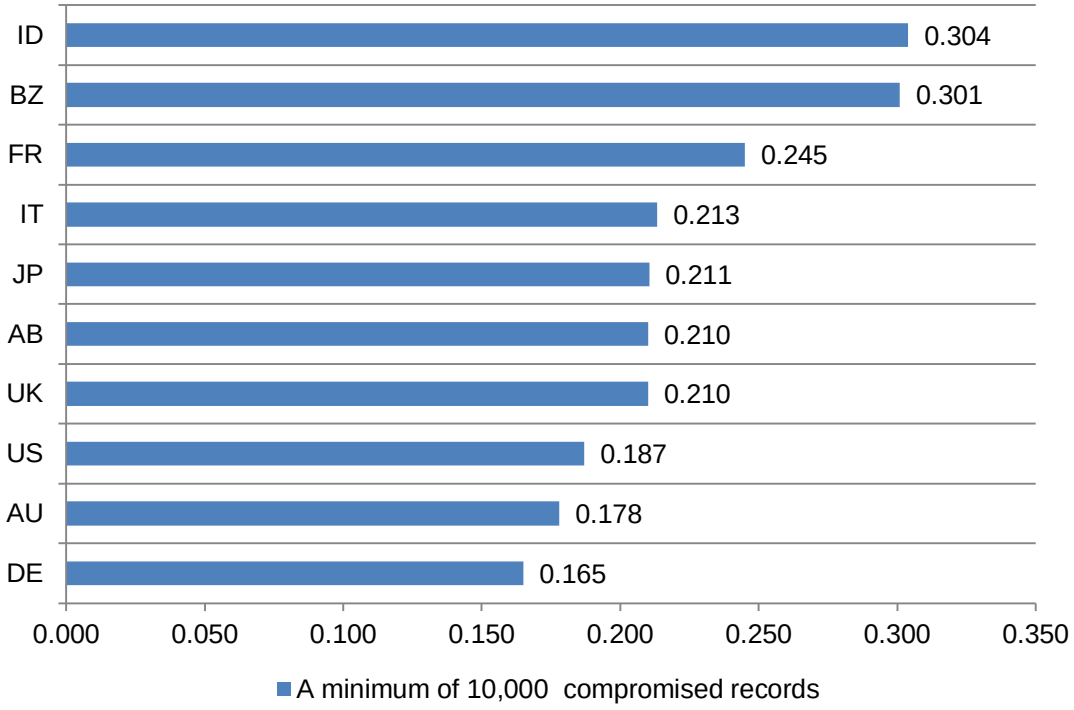


[8]Estimated probabilities were captured from sample respondents using a point estimation technique. Key individuals such as the CISO or CPO who participated in cost assessment interviews provided their estimate of data breach likelihood for 10 levels of data breach incidents (ranging from 10,000 to 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 one of the 314 participating companies.

Organizations in certain countries are more likely to have a data breach. Figure 20 summarizes the probability of a data breach involving a minimum of 10,000 records for the 10 countries in this research. While a small sample size prevents us from generalizing country differences, the estimated likelihood of a material data breach varies considerably across countries.

India and Brazil appear to have the highest estimated probability of occurrence. Germany and Australia have the lowest probability.

Figure 20. Probability of a data breach involving a minimum of 10,000 records by industry



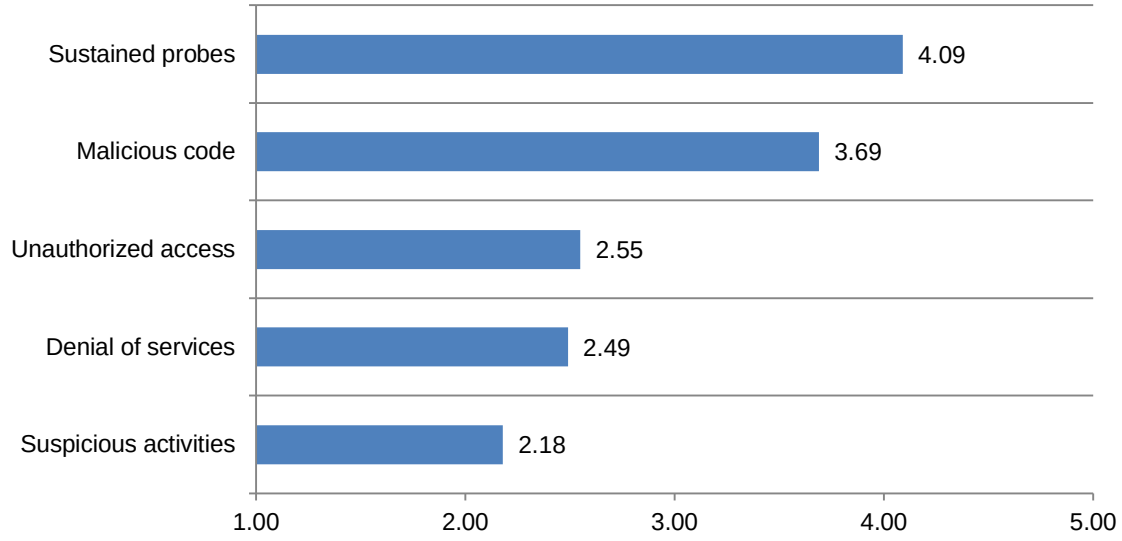
Part 3. Global Security Findings

This year's *Cost of Data Breach Study* reveals that the most common cause of a data breach, with the exception of India, is a malicious insider or criminal attack. In this year's study, we asked companies represented in this research what worries them most about security incidents, what investments they are making and the existence of a security strategy.

According to the findings, the ideal amount to invest over the next 12 months to execute their organization's security strategy averages $14 million. However, in the next 12-month period, companies anticipate having an average of about half that amount, or $7 million.

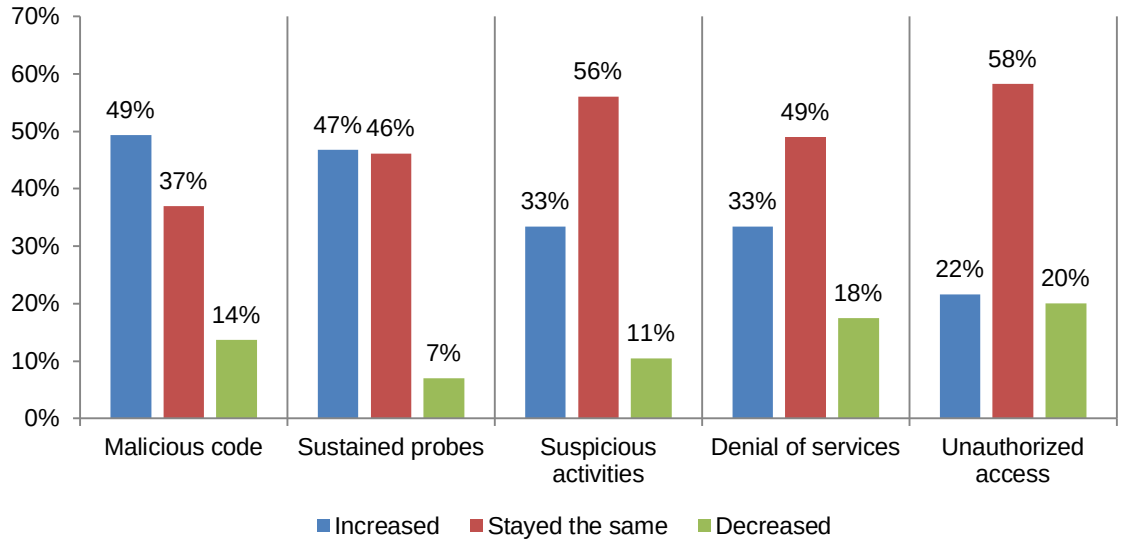
Following is a consolidated analysis of the key findings for all 10 countries. As shown in Figure 21, the greatest threats to an organization's security are considered to be sustained probes and malicious code. The least threatening are suspicious activities and denial of services.

Figure 21. Types of security incidents based on the severity of threat
1 = the least severe to 5 = the most severe
Consolidated view (n=314)



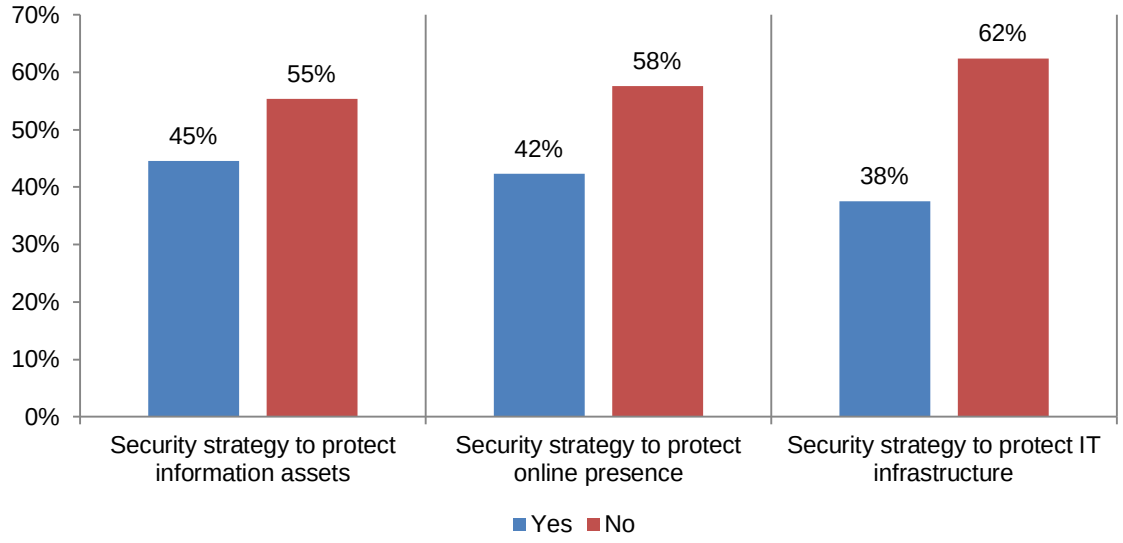
Why malicious code and sustained probes are a concern. Figure 22 shows why these threats are the biggest worries for IT security. According to 49 percent of companies, malicious code is expected to increase and 47 percent expect sustained probes to become more of a problem. Only 22 percent believe unauthorized access will increase in activity and 20 percent actually see it decreasing.

Figure 22. Changes in security threats over the forthcoming year
Consolidated view (n=314)



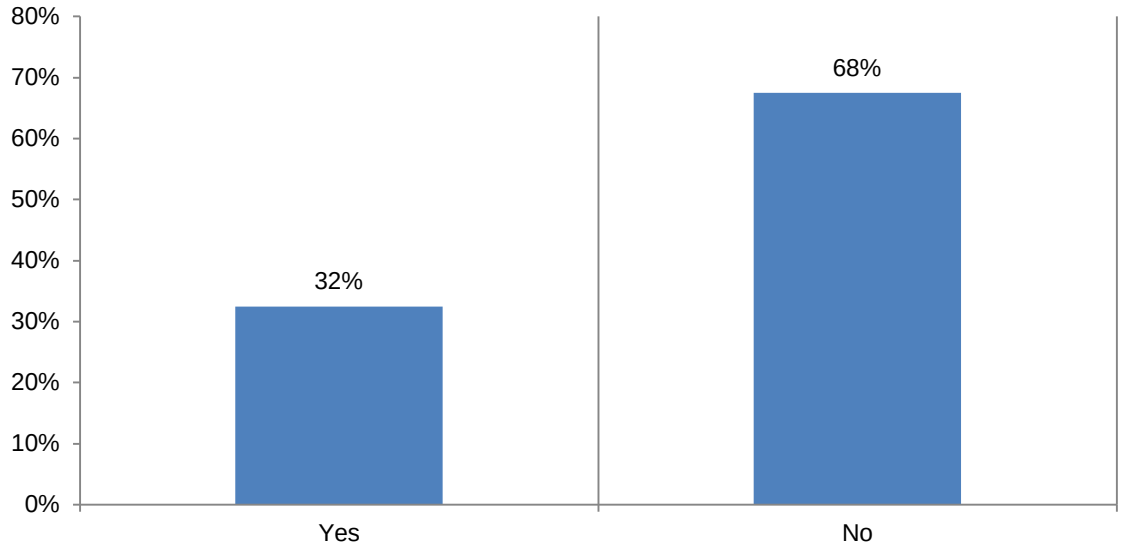
Companies need to improve their strategic approach to threats. As shown in Figure 23, strategies to protect online presence, information assets and infrastructure do not exist for most of the companies represented in this research. Strategies are most likely to exist to protect information assets. As discussed above, the budget to execute their organization's security strategy and mission is far less than what they believe is needed and could explain these findings.

Figure 23. Current security strategy
Consolidated view (n=314)



About one-third of companies are incorporating cyber insurance as part of their risk management strategy. According to Figure 24, 32 percent of organizations in this research have a cyber insurance policy to manage the risk of attacks and threats. Of those who have cyber insurance, 54 percent are satisfied with the coverage.

Figure 24. Does the organization have a data breach protection or cyber insurance policy?
Consolidated view (n=314)



An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. While it has been suggested that having insurance encourages companies to slack off on security, our research suggests the opposite. Those companies with good security practices are more likely to purchase insurance.

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 they engage in to resolve the data breach.

Typical activities for discovery and the immediate response to the data breach include the following:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organizing the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call center procedures and specialized training

The following are typical activities conducted in the aftermath of discovering the data breach:

- Audit and consulting services
- Legal services for defense
- Legal services for compliance
- Free or discounted services to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

Once the company estimates a cost range for these activities, we categorize the costs as direct, indirect and opportunity as defined below:

- *Direct cost* – the direct expense outlay to accomplish a given activity.
- *Indirect cost* – the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- *Opportunity cost* – the cost resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been reported to victims (and publicly revealed to the media).

Our study also looks at the core process-related activities that drive a range of expenditures associated with an organization's data breach detection, response, containment and remediation. The costs for each activity are presented in the Key Findings section (Part 2). The four cost centers are:

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

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

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

- Turnover of existing customers: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.[9]

- 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.[10] In these cases, we would expect the business cost category to be lower when data breaches do not involve customer or consumer data (including payment transactional information).

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

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

Part 5. Organizational characteristics and benchmark methods

Figure 25 shows the distribution of benchmark organizations by their primary industry classification. In this year's study, 16 industries are represented. The largest sector is financial services, which includes banks, insurance, investment management and payment processors.

Figure 25. Distribution of the benchmark sample by industry segment
Consolidated view (n=314)

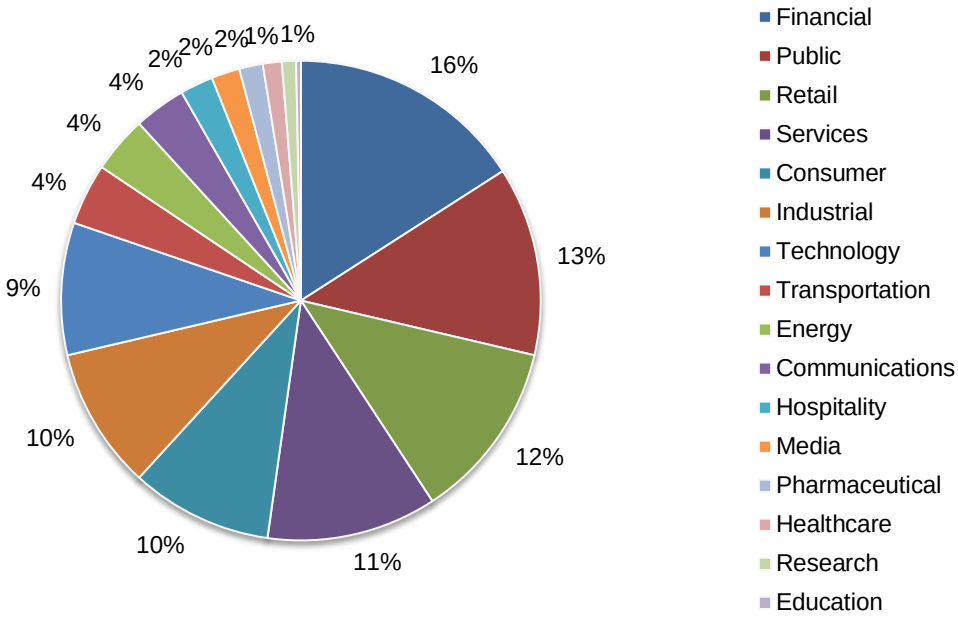
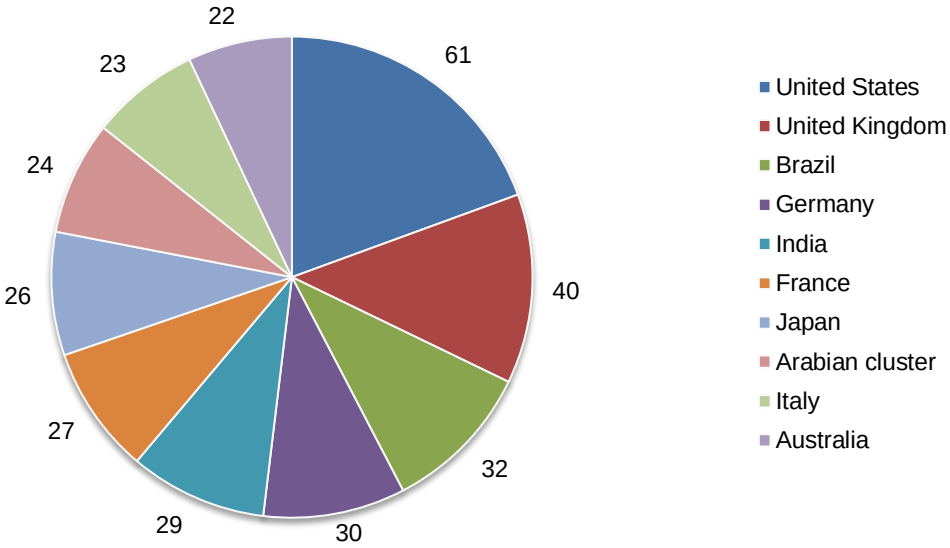


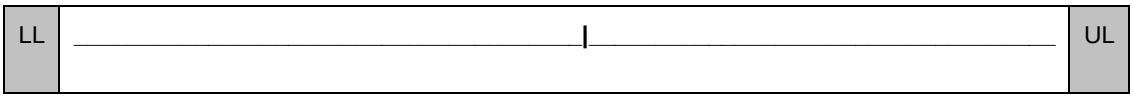
Figure 26. Sample sizes for ten country studies



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

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

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



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

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

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

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

Part 6. Limitations

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

- Non-statistical results: Our study draws upon a representative, non-statistical sample of global entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

- Non-response: The current findings are based on a small representative sample of benchmarks. In this global study, 314 companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.

- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

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

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

- Extrapolated cost results: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

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

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

Complete copies of all country reports are available at www.ibm.com/services/costofbreach.

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.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.