2013 Cost of Data Breach Study: United Kingdom

Benchmark research sponsored by Symantec
Independently Conducted by Ponemon Institute LLC
May 2013

2013[1] Cost of Data Breach Study: United Kingdom

Ponemon Institute, May 2013

Part 1. Executive Summary

Symantec Corporation and Ponemon Institute are pleased to present the *2013 Cost of Data Breach Study: United Kingdom*, our sixth annual benchmark study concerning the cost of data breach incidents for companies located in the UK. In this year's study, the average per capita cost of a data breach increased from £79 to £86.[2]

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States eight years ago and the United Kingdom six years ago. Since then, we have expanded the study to include Germany, France, Australia, Italy, Japan and, for the first time this year, Brazil. To date, 196 UK organisations have participated in the benchmarking studies since the inception of this research series six years ago.

Since Ponemon Institute began studying this issue, several EU countries have enacted laws requiring the controller of databases that contain personal information to inform affected individuals in the event of data loss or theft. In an effort to reduce administrative burdens and the cost of compliance with data protection laws, including data breach notification, the European Commission announced a proposal to reform the European Union's data protection framework. Announced in January 2012, the proposed regulation creates a single set of European rules that would be valid everywhere for all EU member countries.[3]

At present, the Information Commissioner's Office (ICO) has had the power to fine organisations up to £500,000 for failing to prevent data breaches.[4] The size of the imposed fine is proportional to the seriousness of the breach, the organisation's financial resources and the sector it services. The UK financial sector is regulated with even harsher penalties. Based on changes in the regulatory landscape, we believe organisations are taking the protection of sensitive and confidential data more seriously in order to avoid costly fines and the loss of reputation or marketplace image.

This year's study examines the costs incurred by 38 UK companies in 12 industry sectors after these companies experienced the loss or theft of protected personal data and then had to notify breach victims and/or regulators as required by law. 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 more than 300 individuals we interviewed over a 10-month period in the companies that are represented by this research.

The number of breached records per incident this year ranged from 3,534 records to 70,360 records in this year's study. The average number of breached records was 23,833. We do not include organizations that had data breaches in excess of 100,000 because they are not representative of most data breaches and to include them in this study would skew the results. The data breach costs for the 38 data breach case studies in this year's report are presented in Appendix 1.

This report examines a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-poste) response. We also analyse the economic impact of lost or diminished customer trust and confidence as measured by customer turnover or churn.

---

[1] The Cost of Data Breach report is dated as a 2013 publication. Please note that all data breach incidents studied in this year's report happened in the 2012 calendar year. Thus, all figures reflect the 2012 data breach incidents.

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

[3] See: European Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. EC.europa.eu/justice/data-protection/document/review/2012/com_2012_11_en.pdf.

[4] Bender on Privacy and Data Protection, David Bender, 31.05[1][a]©2011 Matthew Bender & Company, Inc.

The following are the most salient findings of our research:

- **The cost of data breach continues to rise**. For the sixth consecutive year, the cost per lost or stolen record has increased. Based on the experience of the 38 organisations participating in this study, the average per capita cost increased from £79 to £86. The organisational cost also increased from £1.75 to million to £2.04 million. In the context of this report, we define a record as information that identifies an individual and regulations require notification of data breach victims.

- **Fewer customers remain loyal following the data breach**. Abnormal churn as a result of the data breach incident increased by 7 percent in 2012. Consistent with earlier studies, certain industries, such as financial services, pharmaceutical companies and service organisations, are more susceptible to customer churn.

- **While negligence is the main cause of data breach, malicious or criminal attacks are most costly**. Thirty-seven percent of data breaches involved negligent employees or contractors (a.k.a. human factor). Malicious or criminal attacks have increased slightly from 31 percent to 34 percent of data breaches. This type of breach is also the most costly. Specifically, the per capita cost of data breach caused by malicious or criminal attacks (exfiltration) was £102. Data breaches due to system or business process failures was £79 and data breaches caused by employee or contractor negligence was £76 per compromised record.

- **Lost business costs increased from £779 thousand in 2011 to £921 thousand in 2012**. These costs refer to abnormal turnover of customers (a higher than average loss of customers for the industry or organisation), increased customer acquisition activities, reputation losses and diminished goodwill. Lost business cost has steadily increased over six years from a low of approximately £500 thousand in 2007.

- **Certain organisational factors reduce the overall cost**. If the organisation has a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as £13 per compromised record. In addition, a strong security posture and the appointment of a CISO reduced the cost as much as £13 and £9 per compromised record, respectively. Finally engaging outside consultants to assist with the breach response also saved £4 and quick notification saved £2 per record. When considering the average number of records lost or stolen, these factors can provide significant and positive financial benefits.

- **Specific attributes or factors of the data breach also can increase the overall cost**. For example, data breaches caused by or occurring at a third-party organisation such as a vendor or business partner increased per capita cost by £17. Finally, data breach incidents involving the loss or theft of data bearing devices increased the cost by as much as £10 per compromised record.

- **Ex-poste response and detection costs increased slightly.** The costs associated with ex-poste response increased from approximately £451 thousand in 2011 to £508 thousand in 2012. Ex-poste response costs refer to all activities that attempt to address victim, regulator and plaintiff counsels' concerns about the breach incident. This cost category also includes legal and consulting fees that attempt to reduce business risk and liability. Redress, identity protection services and free or discounted products are also included in this cost category.

  Similarly, the costs associated with detection and escalation activities increased from £377 thousand in 2011 to £454 thousand in 2012. This category refers to activities that enable a company to detect the breach and determine its root cause. It also includes upstream and lateral communications that are required to focus activities and keep management informed.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a ten-month period. Recruiting organisations for the 2012 study began in January 2012 and interviews were completed in December. In each of the 38 participating organisations, we spoke with IT, compliance and information security practitioners who are knowledgeable about their organisation's data breach and the costs associated with resolving the breach. For privacy purposes we do not collect any organisation-specific information.

How do you calculate the cost of a data breach?

To calculate the average cost of data breach, we collect both the direct and indirect expenses paid by the organisation. 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 acquisition rates. For a detailed explanation about Ponemon Institute's benchmark methodology, please see Part 4 of this report.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of Data Breach* study is the organisation. In survey research, the unit of analysis is the individual. As discussed previously, we recruited 38 organisations to participate in this study.

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 data breach in our research does not apply to catastrophic breaches. Primarily because these are not typical of the breaches most organisations experience. In order to be representative of the population of UK organisations 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 100,000 compromised records.

Are you tracking the same organisations 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 2007, we have studied the data breach experiences of 196 UK organisations.

Part 2. Key Findings

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

- Cost of data breach per record and organisation
- Cost of data breach by industry
- Root cause of data breach
- Factors that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following cost components: detection and escalation, notification, lost business, direct and indirect and post data breach
- Preventive measures taken after the breach
- Percentage changes in cost categories

The cost of data breach increases. Figure 1 reports the average per capita cost of data breach.[5] As can be seen, for six consecutive years the average per capita cost has increased. According to this year's benchmark findings, data breaches cost companies an average of £86 per compromised record – of which £43 (half) pertains to indirect costs including abnormal turnover or churn of customers. Last year's average per capita cost was £79 with an average indirect cost of £37.

Figure 1. The average per capita cost of data breach over six years
Bracketed number defines the benchmark sample size

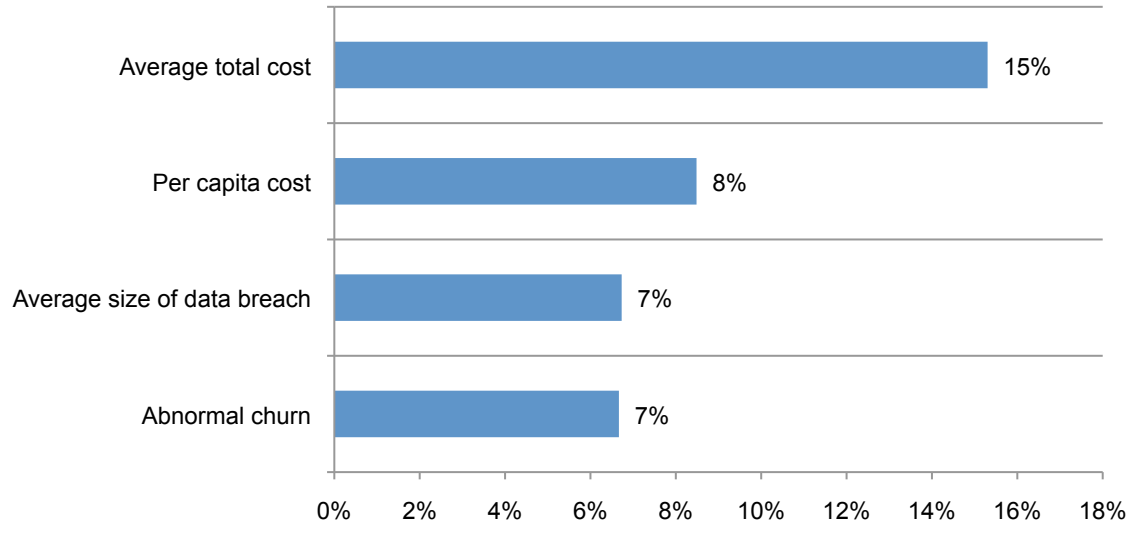
[5]Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records.

Average organisational cost of data breach increases. The total average cost of data breach over six years is shown in Figure 2. The total cost of data breach actually increased from £1.75 million to £2.04 million – or, a 15 percent rise from the previous year.

Figure 2. The average total organisational cost of data breach over six years
£000,000 omitted (sample size in brackets)

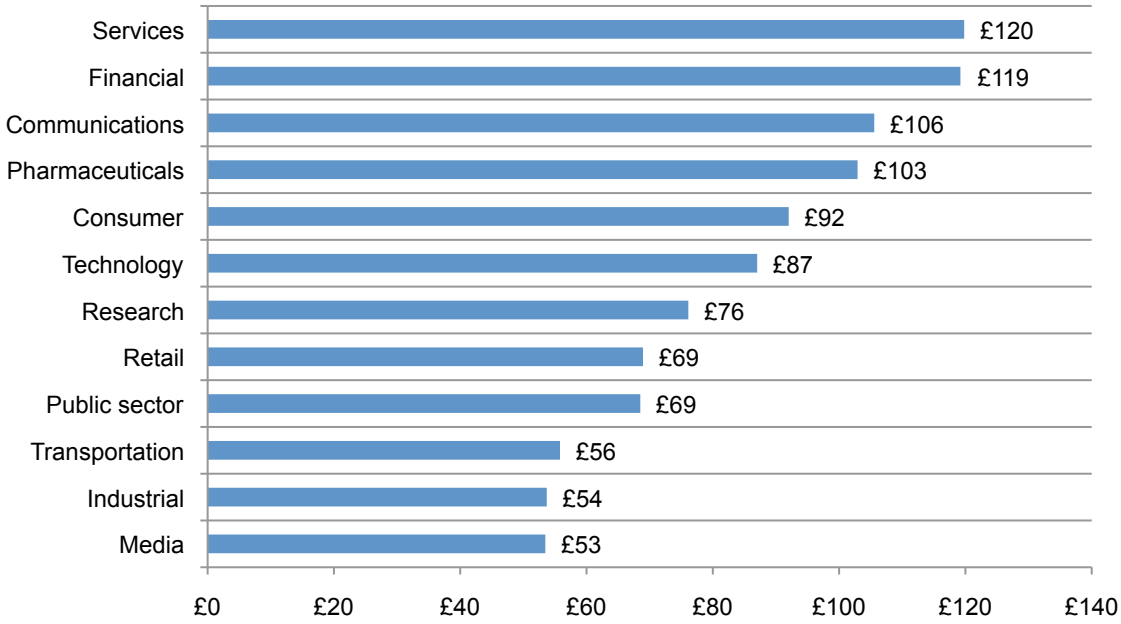
Key cost of data breach measures. Figure 3 reports four key metrics that help explain why the cost of data breach has increased. Per capita cost, average total cost, average size (number of comprised records) and abnormal churn increased by 7 percent between 2012 and 2011. Abnormal churn is defined as the greater than expected loss of customers in the normal course of business. The average total cost of data breach at 15 percent represents the largest percentage increase in the cost of data breach.

Figure 3. Cost of data breach measures
Net change defined as the difference between the 2012 and 2011 results



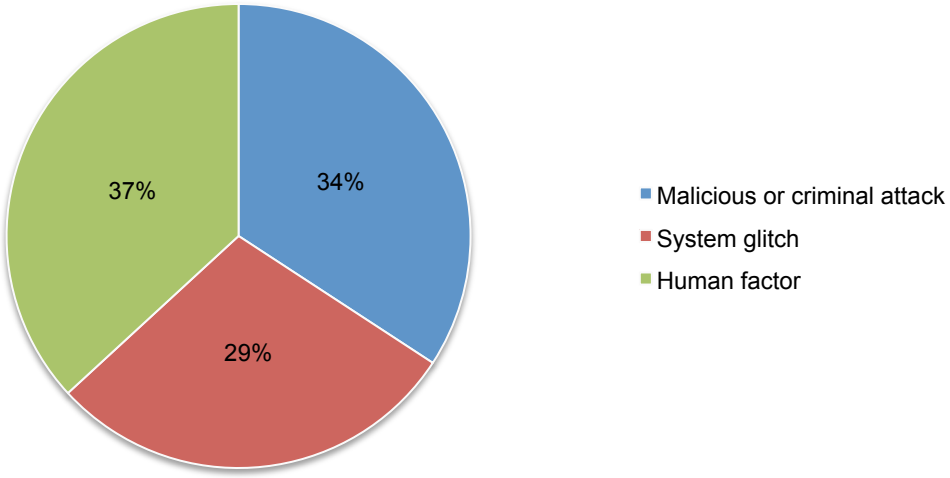
Certain industries experience more costly data breaches. Figure 4 reports the per capita costs for the 2012 study by industry classification. While small sample size prevents us from generalising industry cost differences, the pattern of 2012 industry results is consistent with prior years. Accordingly, services, financial services, communications and pharmaceutical companies have a per capita cost above the mean. Media, industrial, transportation and public services have a per capita cost below the mean.

Figure 4. Per capita cost by industry classification of benchmarked companies



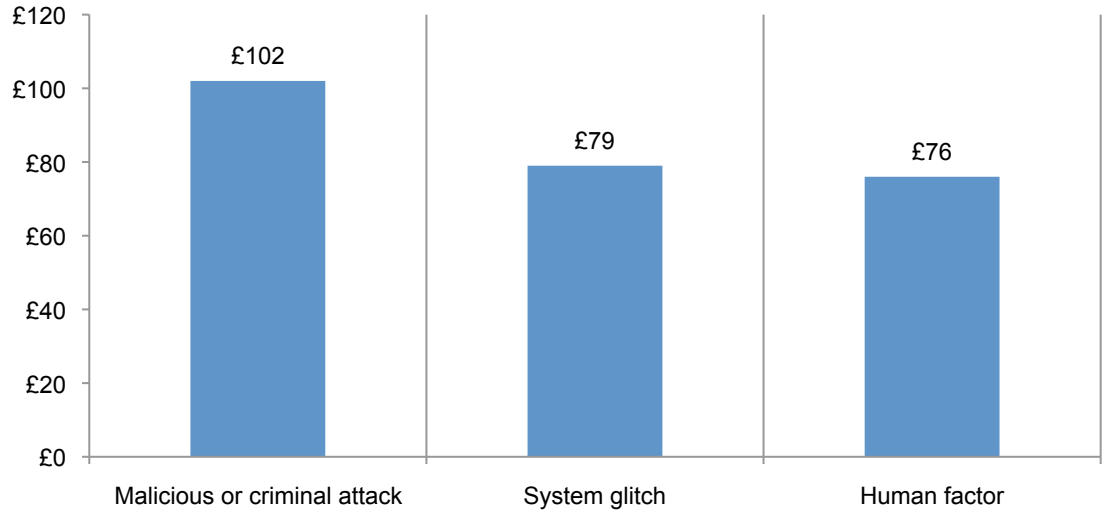
Negligence is the top root cause of data breaches. Figure 5 provides a summary of the main root causes of data breach for all 38 organisations. Thirty-seven percent of incidents involved a negligent employee or contractor (human factor), 29 percent involved system glitches, including a combination of both IT and business process failures, and 34 percent experienced a malicious or criminal attack.[6]

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



Malicious attacks are most costly. The exfiltration of data by hackers or criminal insiders result in a much higher per capita cost of data breach than incidents involving employee error (a.k.a. human factor). Figure 6 reports the per capita cost of data breach for three conditions or root causes of the breach incident. This pattern of results is consistent with prior years' research. Accordingly, companies that experienced malicious or criminal attacks had per capita costs of £102, while companies experiencing system glitches or employee mistakes had a per capita costs at £79 and £76, respectively.[7]

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



[6]Malicious and criminal attacks increased slightly from 31 percent in the 2011 study.
[7]Malicious or criminal attacks that resulted in data theft include: malware, theft of data-bearing devices. malicious insiders such as rogue employees or contractors and SQL injection, phishing (including spear phishing) and other Internet-based attacks.

Seven factors that influence the cost of data breach. We identified seven factors that influence the cost consequences of a data breach incident. These attributes are as follows:

- **The company had an incident management plan**. Forty-two percent of organisations in our benchmark sample had a data breach incident management plan in place at the time of the data breach event.
- **The company had a relatively strong security posture at the time of the incident**. Fifty percent of organisations had a security effectiveness score (SES) at or above the normative average. We measured the security posture of each participating company using the Security Effective Score (SES) as part of the benchmarking process.[8]
- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Thirty-nine percent have centralised the management of data protection with the appointment of a C-level information security professional.
- **Data was lost due to third party error**. Thirty-two percent of organisations had a data breach caused by a third party, such as vendors, outsourcers, cloud providers and business partners.
- **The company notified data breach victims quickly.** Thirty-seven percent of organisations notified data breach victims within 30 days after the discovery of data loss or theft.
- **The data breach involved lost or stolen devices.** Thirty-two percent of organisations had a data breach as a result of a lost or stolen mobile device, which included laptops, desktops, smartphones, tablets, servers and USB drives containing confidential or sensitive information.
- **Consultants were engaged to help remediate the data breach**. Forty-two percent of organisations hired consultants to assist in their data breach response and remediation.

Figure 7 shows incident response plan, security posture, CISO appointment, consulting support and quick notification of the data breach results in cost savings. Third party errors and lost or stolen devices increase the per capita cost. Hence, having an incident response plan in place can reduce the average cost from £86 to £73 (decreased cost = -£13). In contrast, a third party error can increase the average cost from £86 to £103 (increased cost = +£17).

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

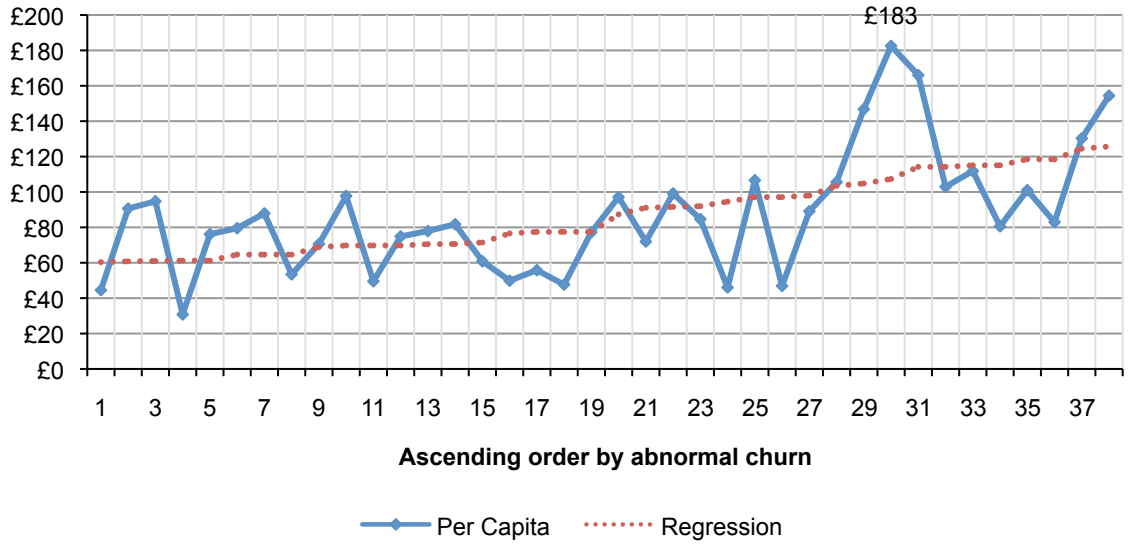
[8]The Security Effectiveness Score was developed by Ponemon Institute in its annual encryption trends survey to define the security posture of responding organisations. The SES is derived from the rating of 24 security features or practices. This method has been validated from more than 40 independent studies conducted since June 2005. The SES provides a range of +2 (most favourable) to -2 (least favourable). Hence, a result greater than zero is viewed as net favourable.

The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for 38 benchmarked companies 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 £297,173 to £9,939,403.

Figure 8. Total cost of data breach by size of lost or stolen records
Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope.

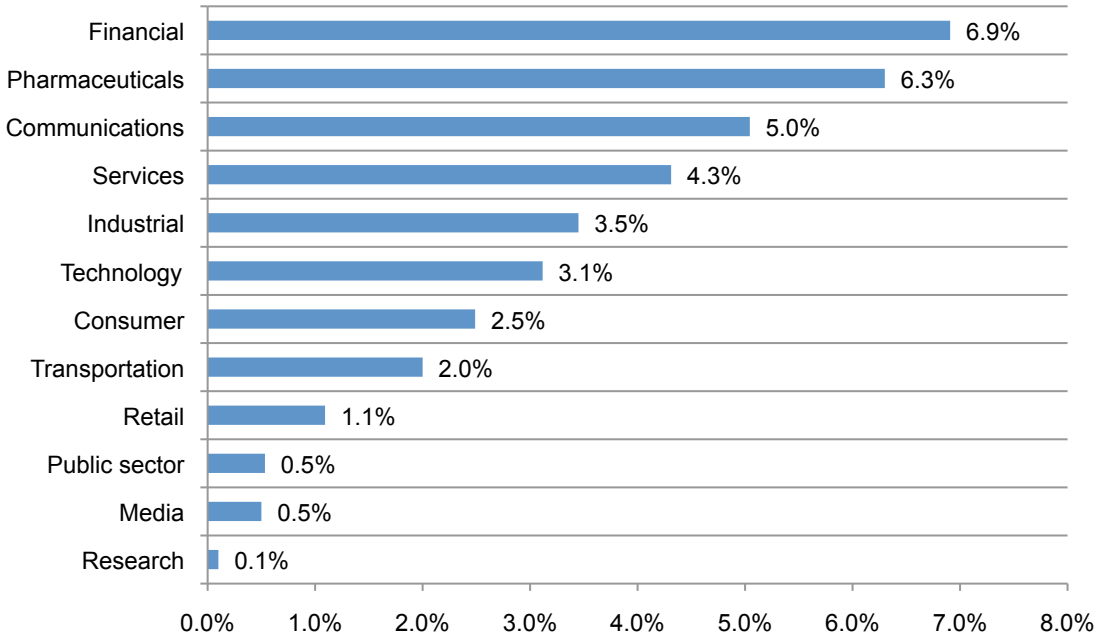
The more churn, the higher the per capita cost of data breach. Figure 9 reports the distribution of per capita data breach costs in ascending rate of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn and per capita costs are linearly related. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 9. Distribution of abnormal churn rates in ascending order by per capita costs
Regression = Intercept + {abnormal churn rate) x β, where β denotes the slope.



Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate of benchmarked organisations for the 2012 study. While small sample size prevents us from generalising the affect of industry on data breach cost, our 2011 industry results are consistent with prior years – wherein financial service organisations tend to experience relatively high abnormal churn and research and media companies experience a lower abnormal churn rate.[9]

Figure 10. Abnormal churn rates by industry classification of benchmarked companies



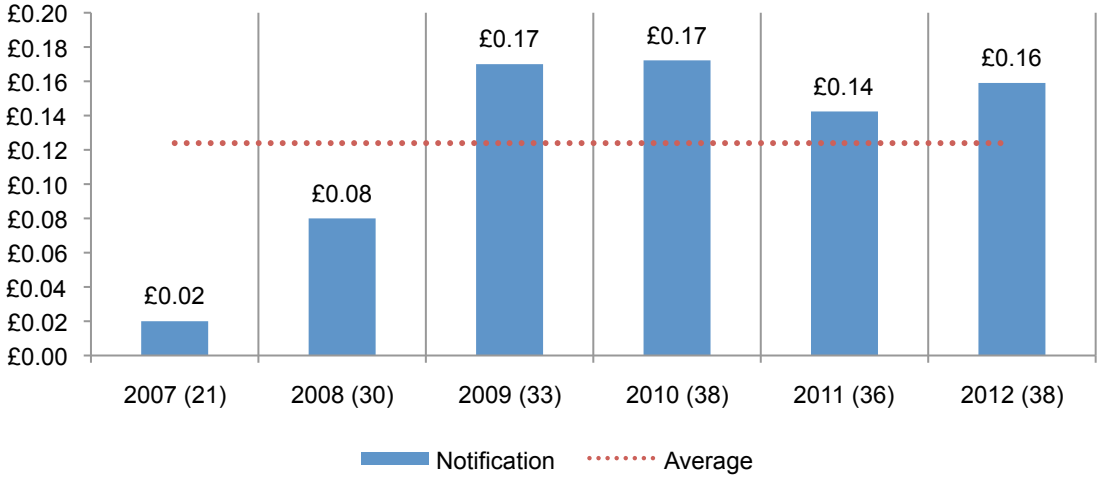
[9]Public sector organisations utilise a different churn framework given that customers of government organisations typically do not have an alternative choice.

Detection and escalation costs are higher this year. Figure 11 shows the distribution of costs associated with detection and escalation of the data breach event. 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, average detection and escalation costs increased from £.38 million to £.45 million in the present year study.

Figure 11. Detection and escalation costs over six years
£000,000 omitted (sample size in brackets)

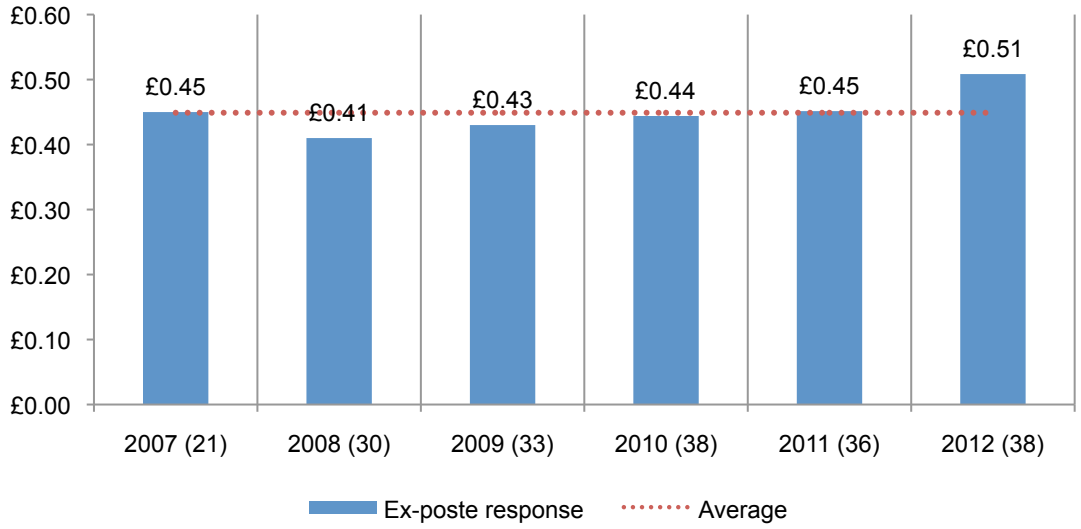
Notification costs rises slightly. Figure 12 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification cost was £.16 million. This represents an increase from £.14 million in 2011.

Figure 12. Notification costs over six years
£000,000 omitted (sample size in brackets)



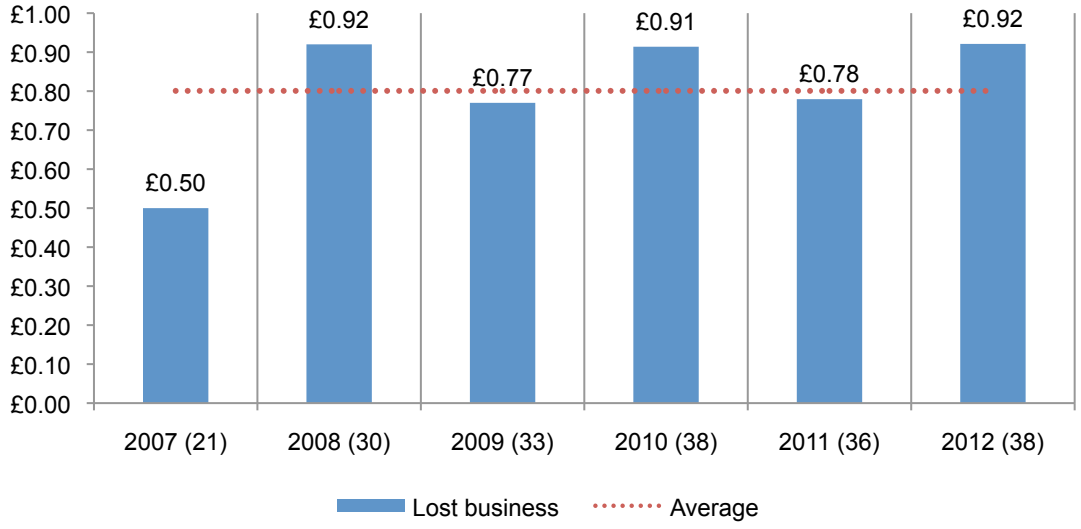
Post data breach costs increase. Figure 13 shows the distribution of costs associated with ex-poste (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-poste response costs increased from £.45 million to a six-year high of £.51 million in this year's study.

Figure 13. Average ex-poste response costs over six years
£000,000 omitted (sample size in brackets)



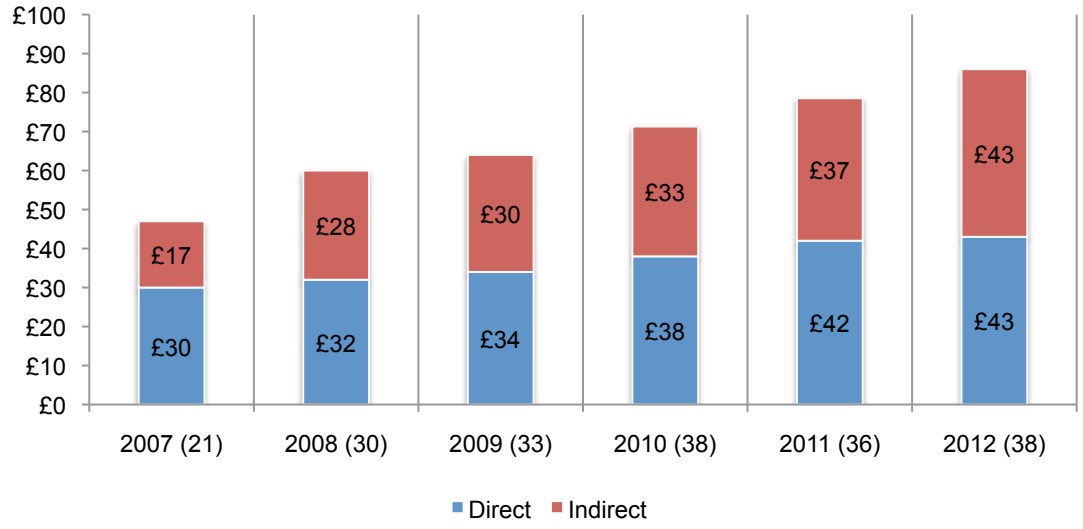
Lost business costs declined sharply. Figure 14 reports lost business costs associated with data breach incidents over six years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As shown, lost business costs increased from £.78 million in 2011 to £.92 million in 2012.

Figure 14. Average lost business costs over six years
£000,000 omitted (sample size in brackets)



Both direct and indirect costs increased. Figure 15 reports the direct and indirect cost components of data breach on a per capita basis. In essence, the cost of data breach per compromised record increased by more than £7 – from £79 in 2011 to £86 in 2012. Approximately £6 of this increase pertains to indirect cost. In the present study, indirect cost represents 50 percent of total per capita cost.

Figure 15. Direct and indirect per capita data breach cost over six years
Sample size in brackets



Preventative measures taken after the breach

In addition to measuring specific cost activities relating to the leakage of personal information, we report in Table 1 the preventive measures implemented by companies after the data breach. The most popular measures and controls implemented after the data breach are: additional training and awareness activities (41 percent), expanded use of encryption (38 percent) and manual control practices (36 percent). In this year's study, the use of security certifications or audit increased 5 percent. However, adoption of identity and access management solutions declined 7 percent.

Table 1. Preventive measures and controls implemented after the data breach	2009	2010	2011	2012
Training and awareness programs	38%	40%	39%	41%
Expanded use of encryption	33%	33%	35%	38%
Manual control practices	41%	43%	40%	36%
Data loss prevention (DLP) solutions	31%	29%	33%	31%
Security certification or audit	19%	21%	25%	30%
Strengthening of perimeter controls	24%	32%	31%	27%
Endpoint security solutions	27%	25%	23%	26%
Identity and access management solutions	25%	26%	30%	23%
Security intelligence solutions	15%	16%	19%	18%

*Please note that a company may be implementing more than one preventive measure.

Cost changes of data breach categories over time

Table 2 reports 11 cost categories on a percentage basis over six years. As can be seen, most cost categories appear to be relatively stable since 2007. However, lost customer business increased from 36 percent to 42 percent and investigation and forensic costs increased from 12 percent in 2011 to 14 percent in 2012. Audit and consulting services have decreased from 14 percent to eight percent.

Table 2. Cost changes over five years	2007	2008	2009	2010	2011	2012
Investigation and forensics	12%	12%	13%	12%	12%	14%
Audit and consulting services	14%	10%	9%	8%	9%	8%
Outbound contact costs	13%	9%	10%	11%	12%	10%
Inbound contact costs	10%	7%	7%	8%	10%	8%
Public relations and communications costs	1%	3%	5%	6%	5%	3%
Legal services – defence	3%	3%	2%	1%	0%	2%
Legal services – compliance	1%	2%	3%	2%	2%	3%
Free or discounted services	4%	2%	2%	3%	2%	2%
Credit monitoring services	0%	1%	0%	0%	0%	0%
Lost customer business	36%	44%	41%	42%	41%	42%
Customer acquisition cost	6%	8%	8%	7%	7%	8%

Part 3. Concluding observations and description about participating companies

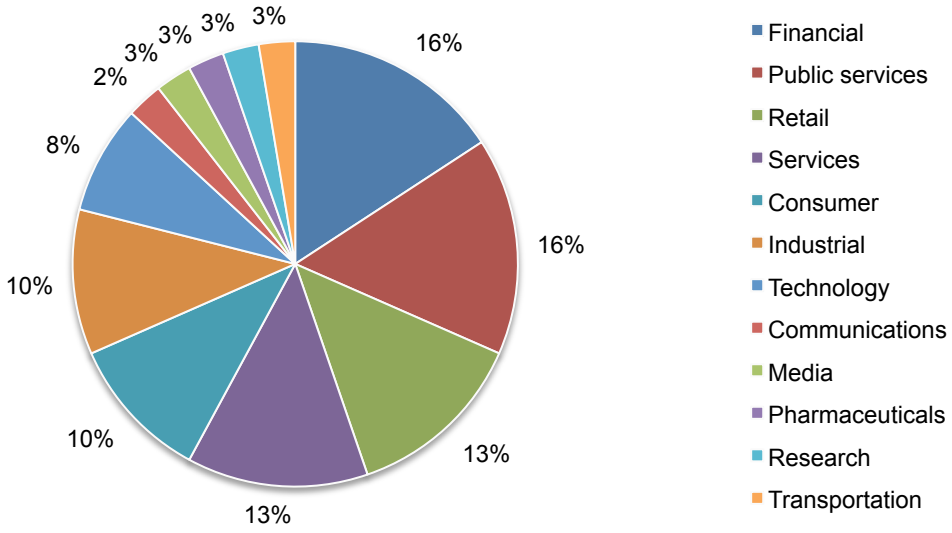
Companies in this year's study reported that their data breaches were larger in scale and resulted in a higher rate of churn. We conclude that companies can substantially reduce the cost of data breach by improving incident response planning, enhancing the company's security posture, establishing accountability (through the appointment of a CISO) and engaging consultants to assist during and after the data breach incident.

We hope this study helps to understand what the potential costs of a data breach could be based on certain characteristics and how best to allocate resources to the prevention, detection and resolution of a data breach. Specifically the study reveals the severe financial consequences from malicious or criminal acts. These data breaches can prove to be the most costly.

In this report, we compare the results of the present study to those from prior years. It is important to note that 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 attempt to recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach.

Figure 16 shows the distribution of benchmark organisations by their primary industry classification. In this year's study, 12 industries are represented. Financial services, public sector (government), retail and services companies represent the four largest segments.[10]

Figure 16. Distribution of the benchmark sample by industry segment



[10]Retail organisations are companies that sell directly to consumers. This includes both conventional store sales and online sales.

Part 4. How we calculate the cost of a data breach

Our study addresses core process-related activities that drive a range of expenditures associated with an organisation's data breach detection, response, containment and remediation. The four cost centres 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.
- Ex-poste response: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimise potential harms. Redress activities also include ex-poste response such as 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 organisation.

- 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.[11]
- Diminished customer acquisition: The estimated number of target customers who will not have a relationship with the organisation 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 organisation's churn or turnover.[12] 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).

All participating organisations experienced one or more data breach incidents sometime over 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

[11] In several instances, turnover is partial, wherein breach victims still continued their relationship with the breached organisation, 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.

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

of customer or consumer [13]information. It also required these practitioners to estimate opportunity costs associated with program activities.

Estimated data breach cost components were captured on a rating form. In most cases, the researcher conducted follow-up interviews to obtain additional facts, including estimated abnormal churn rates that resulted from the company's most recent breach event involving 1,000 or more compromised records.[14]

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, labour and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

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

LL	_____|_____	UL

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

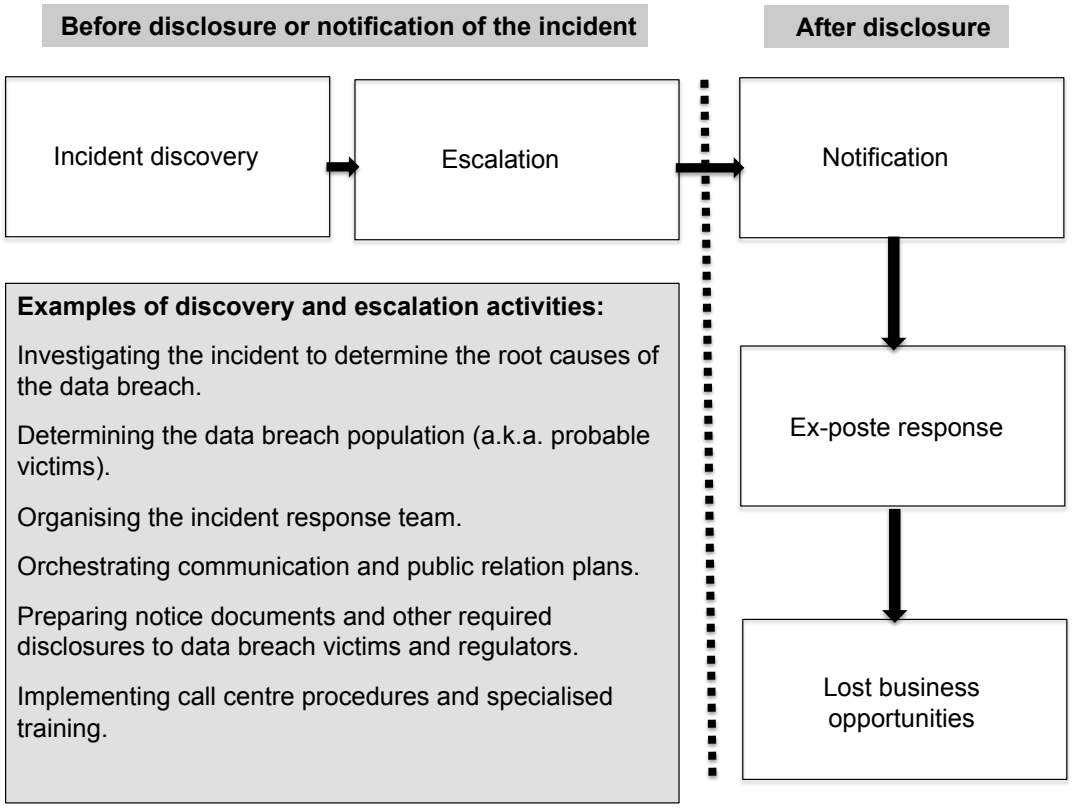
The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information. We believed that a study focused on business process – and not data protection or privacy compliance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

[13]We define a consumer as a potential customer of the organisation that had the breach. This includes marketing or target marketing data that contains personal information about the individual whose record is lost or stolen.

[14]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 breaches, which we define as an incident involving millions of lost or stolen records, to avoid skewing overall sample findings.

Figure 17 illustrates the activity-based costing schema used in our benchmark study. The cost centres we examine sequentially are: incident discovery, escalation, notification, ex-poste response and lost business.

Figure 17: Schema of the data breach process



Within each cost centre, the research instrument required subjects to estimate a cost range to capture estimates of direct cost, indirect cost and opportunity cost, defined as follows:

- *Direct cost* – the direct expense outlay to accomplish a given activity.
- *Indirect cost* – the amount of time, effort and other organisational 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).

To maintain 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.

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

Part 5. Limitations

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

- Non-statistical results: Our study draws upon a representative, non-statistical sample of UK-based 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. Thirty-eight 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 organisational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined. Further, our study focuses on customer or consumer information rather than the plethora of other business records that may be lost or stolen.

- 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.

Appendix 1: Cost for 38 Data Breach Case Studies

Cases	Size of breach	Detection & escalation*	Notification*	Ex-poste response*	Lost business*	Total*
1	27,657	366,521	79,640	1,214,401	1,943,226	3,603,788
2	12,436	120,203	39,012	179,674	326,150	665,039
3	43,449	536,522	33,556	876,903	591,223	2,038,204
4	45,936	341,958	161,213	1,971,572	2,374,552	4,849,295
5	64,382	2,429,211	197,081	1,627,271	5,685,840	9,939,403
6	33,749	677,001	52,457	287,857	1,989,254	3,006,569
7	5,198	132,615	288,748	120,592	320,955	862,910
8	3,534	38,008	37,380	12,015	289,297	376,700
9	9,150	114,461	386,282	132,508	12,548	645,799
10	19,486	211,503	162,230	256,194	342,075	972,002
11	38,552	501,799	358,810	855,213	2,079	1,717,901
12	45,569	483,330	18,349	512,841	1,082,974	2,097,494
13	34,274	560,153	32,899	384,821	1,865,327	2,843,200
14	15,355	288,986	129,991	405,289	698,160	1,522,426
15	12,372	283,468	504,143	139,206	8,321	935,138
16	19,209	794,628	314,789	772,997	937,209	2,819,623
17	9,976	153,406	267,964	202,081	321,413	944,864
18	26,690	121,518	117,537	826,063	257,594	1,322,712
19	26,667	722,834	40,337	595,874	263,556	1,622,601
20	14,876	348,411	462,708	105,547	388,565	1,305,231
21	3,813	95,188	61,020	45,894	95,071	297,173
22	59,000	1,432,111	160,702	1,502,622	3,500,401	6,595,836
23	13,127	409,232	510,583	117,924	6,600	1,044,339
24	29,885	805,078	94,077	986,479	1,190,165	3,075,799
25	18,714	528,239	132,710	167,328	216,000	1,044,277
26	7,824	177,408	254,836	242,795	12,494	687,533
27	9,887	257,253	55,245	344,936	95,205	752,639
28	15,025	129,404	32,536	143,755	1,211,937	1,517,632
29	70,360	1,241,135	71,790	480,833	3,643,832	5,437,590
30	11,402	296,734	143,215	1,164,775	476,396	2,081,120
31	22,809	331,331	17,316	217,971	1,364,282	1,930,900
32	21,100	1,165,769	98,729	351,551	109,247	1,725,296
33	23,929	205,470	11,413	427,703	495,929	1,140,515
34	17,639	122,265	41,563	210,965	895,039	1,269,832
35	7,060	114,228	336,946	77,196	111,439	639,809
36	26,223	303,199	115,957	386,770	2,035	807,961
37	19,570	277,641	146,459	672,968	802,804	1,899,872
38	19,780	147,526	73,107	300,070	1,073,570	1,594,273

* Measured in GBP (£)

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

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

Ponemon Institute 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 organisations.

As a member of the **Council of American Survey Research Organisations (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.