2011 Cost of Data Breach Study: United Kingdom

Benchmark Research sponsored by Symantec

Independently Conducted by Ponemon Institute LLC

March 2012

Ponemon Institute© Research Report

2011 Cost of Data Breach Study: United Kingdom

Ponemon Institute, March 2012

Part 1. Introduction

Symantec Corporation and Ponemon Institute are pleased to present *2011 Cost of Data Breach Study: United Kingdom*, our fifth annual benchmark study concerning the cost of data breach incidents for UK-based companies. In this year's study, the average per capita cost of a data breach has increased from £71 to £79.

Since Ponemon Institute began studying this issue, several EU countries have enacted laws requiring the owners of personal information databases to inform affected individuals in the event of a data security breach. In an effort to reduce administrative burdens and the cost of compliance with data protection laws, including data breach notification, Viviane Reding, European Commissioner for Justice, Fundamental Rights and Citizenship, announced the European Commission's 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 across the EU.[1]

Starting in April 2010, the Information Commissioner's Office (ICO) has had the power to fine all organisations up to £500,000 for data breaches.[2] 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 loss of reputation and brand.

This year's study examines the costs incurred by 36 UK companies in 11 different industry sectors after those companies experienced the loss or theft of protected personal data and then had to notify breach victims as required by law. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. The number of breached records per incident this year ranged from approximately 3,500 records to more than 78,000 records.

Ponemon Institute conducted its first *Cost of Data Breach* study in the United States seven years ago and the United Kingdom five years ago. Since then, we have expanded the study to include Germany, France, Australia and, for the first time this year, India, Italy and Japan. The 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, rates.

The following are the most interesting findings and implications for organisations:

- **The cost of data breach continues to rise**. For the fifth consecutive year, the cost per lost or stolen record has increased. For organisations participating in this study, the average cost increased from £71 to £79. We define a record as information that identifies an individual and regulations require notification of data breach victims.

  However, the organisational cost has declined from £1.9 to million to £1.75 million. This decline suggests that organisations represented in this study have improved their performance in both preparing for and responding to a data breach. As the findings reveal, fewer records are being lost in these breaches and there is less customer churn.

[1] "European Commission Publishes New Framework on Data Protection," IAPP Daily Dashboard, January 25, 2012

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

- **More customers remain loyal following the data breach**. Fewer customers are abandoning companies that have a data breach. The average abnormal churn decreased from 3.3 percent in 2010 to 2.9 percent this year. However, certain industries, such as financial services and pharmaceutical companies, are more susceptible to customer churn, which causes their data breach costs to be higher than the average. Taking steps to keep customers loyal and repair any damage to reputation and brand can help reduce the cost of a data breach.

- **Negligence is the main cause of the data breach**. Thirty-six percent of data breaches involved negligent employees or contractors. Malicious or criminal attacks have increased slightly from 29 percent to 31 percent of data breaches experienced by organisations in this study. This type of breach is also the most costly. Accordingly, organisations need to focus on processes, policies and technologies that address threats from the malicious insider or hacker.

- **Lost business costs declined sharply from £910,000 in 2010 to £780,000 in 2011**.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. During the five years we have studied this aspect of a data breach, the highest cost for lost business was £920,000 in 2008 and the lowest was £500,000 in 2005.

- **Certain organisational factors reduce the overall cost**. If the organisation has a CISO with overall responsibility for enterprise data protection the average cost of a data breach can be reduced as much as £18 per compromised record. Outside consultants assisting with the breach response can save as much as £11 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. Data breaches caused by third parties or a lost or stolen device increased the cost by £9 and £6, respectively.

- **Detection and escalation costs stayed about the same but notification costs decreased.** Detection and escalation costs increased very slightly from approximately £370,000 in 2010 to £380,000 this year. These costs refer to activities that enable a company to detect the breach and whether it occurred in storage or in motion. Controlling these costs suggests that organisations have the appropriate processes and technologies to execute these activities.

  Notification refers to the steps taken to report the breach of protected information to appropriate personnel within a specified time period. The costs to notify victims of the breach declined in this year’s study from approximately £170,000 to £140,000. This decline could suggest that organisations are becoming more efficient in notifying data breach victims.

Cost of Data Breach FAQs

How do you collect the data?

Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a nine-month period. Recruiting organisations for the 2011 study began in January 2011 and interviews were completed in December. In each of the 36 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 36 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 the ones experienced by Sony or Epsilon?

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 158 UK organisations.

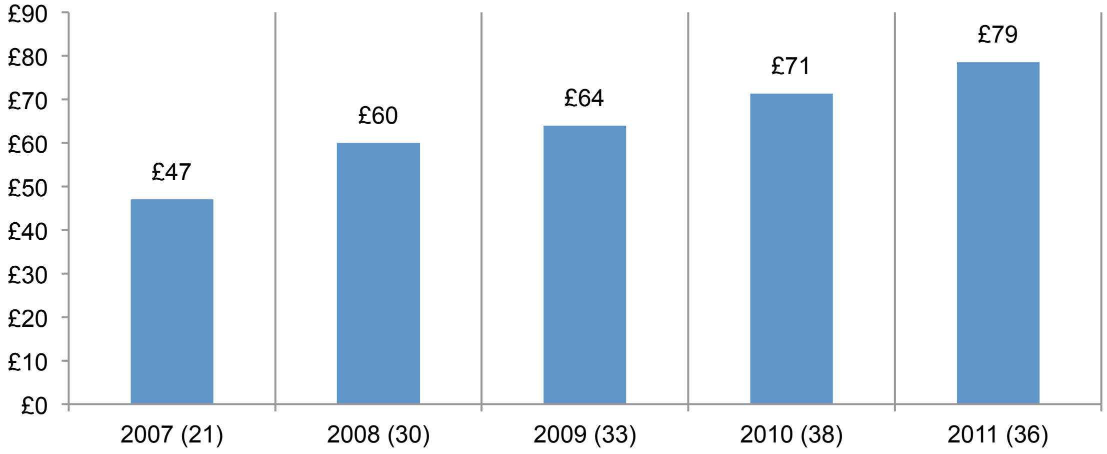
Part 2. Key Findings

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

- Cost of data breach: per record, organisational and industry
- Root causes of a data breach
- Attributes that influence the cost of data breach
- Trends in the frequency of compromised records
- Trends in customer turnover or churn
- Trends in the following costs: detection and escalation, notification, lost business, direct and indirect and post data breach
- Trends in the Security Effectiveness Score for benchmarked organisations

The cost of data breach increases. Figure 1 reports the average per capita cost of data breach.[3] As can be seen, for five consecutive years the average per capita cost has increased. According to this year's benchmark findings, data breaches cost companies an average of £79 per compromised record – of which £37 pertains to indirect costs including abnormal turnover or churn of existing and future customers. Last year's average per capita cost was £71 with an average indirect cost of £33.

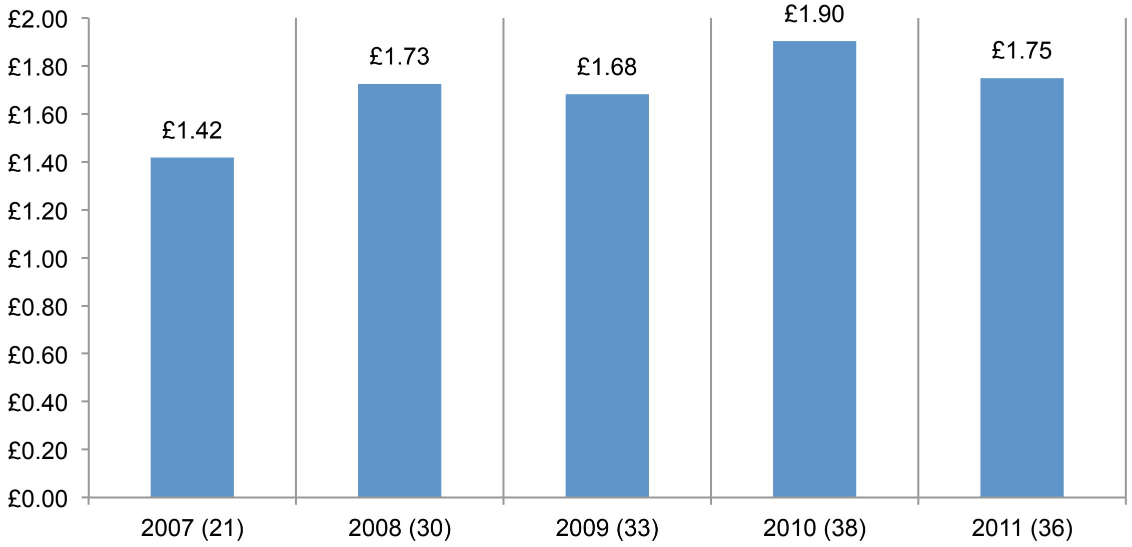
Figure 1: The average per capita cost of a data breach over five years
Bracketed number defines the benchmark sample size



[3] 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.

The total average cost of data breach over five years is shown in Figure 2. The total cost of data breach actually decreased from £1.90 million to £1.75 million – or, an eight (8) percent decline between 2010 and 2011 results.

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



Containing the size of the breach and improving responsiveness can result in lower organisational costs. Figure 3 reports four key metrics that show mixed results. Despite increasing per capita cost, the average total cost of a data breach actually decreased by 8 percent. A 12 percent decrease in abnormal churn rate suggests organisations have improved their response to data breach and they are more successful in retaining the loyalty of customers. The average data breach size has declined by 17 percent, suggesting fewer records are being lost or stolen.

Figure 3: Reasons for decline in organisational cost
Net change defined as the difference between the 2011 and 2010 results

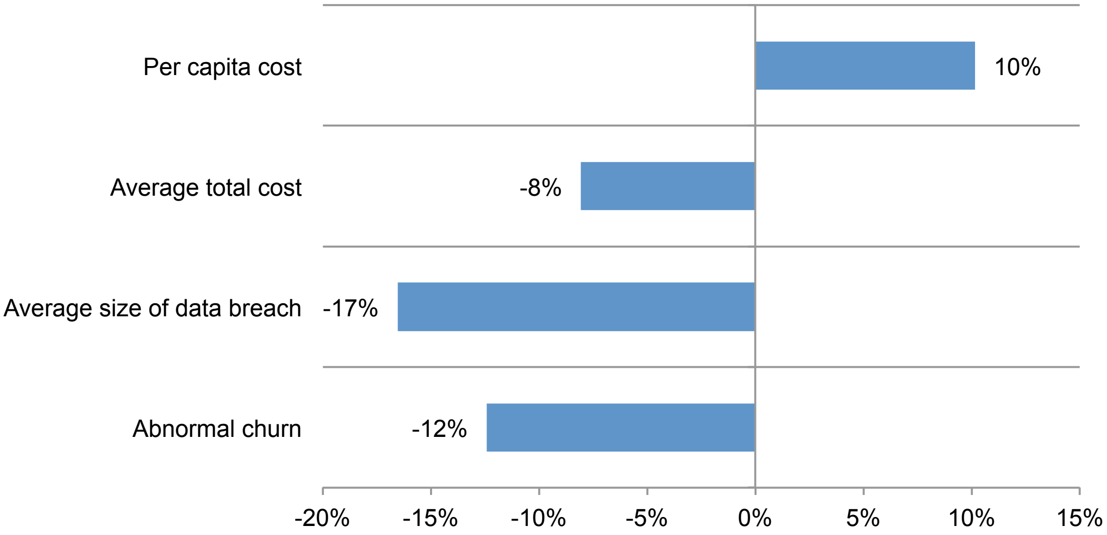
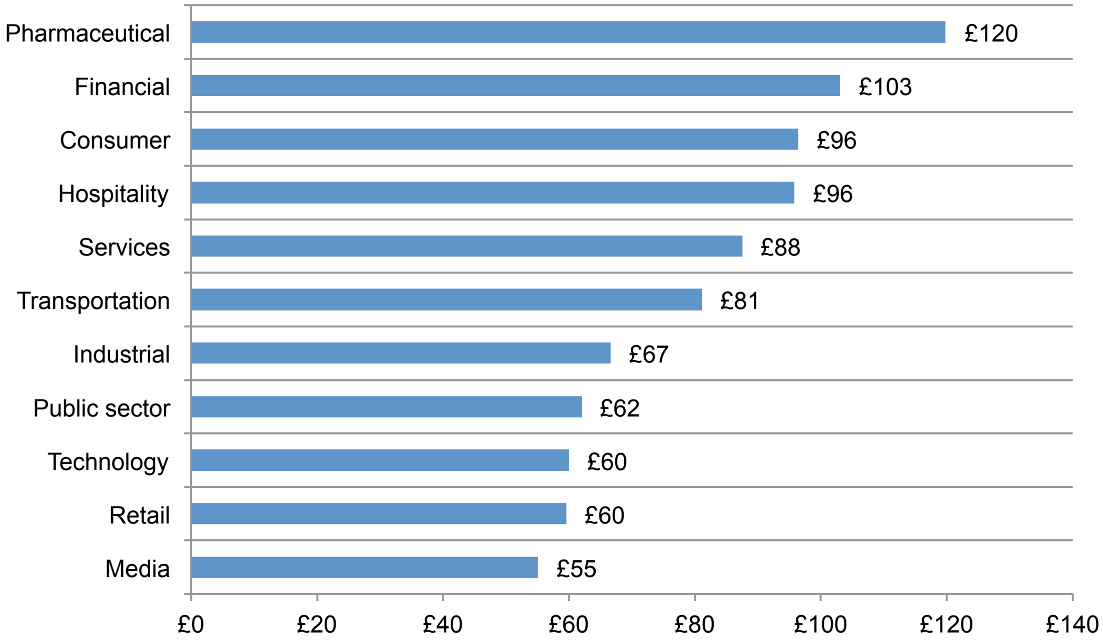


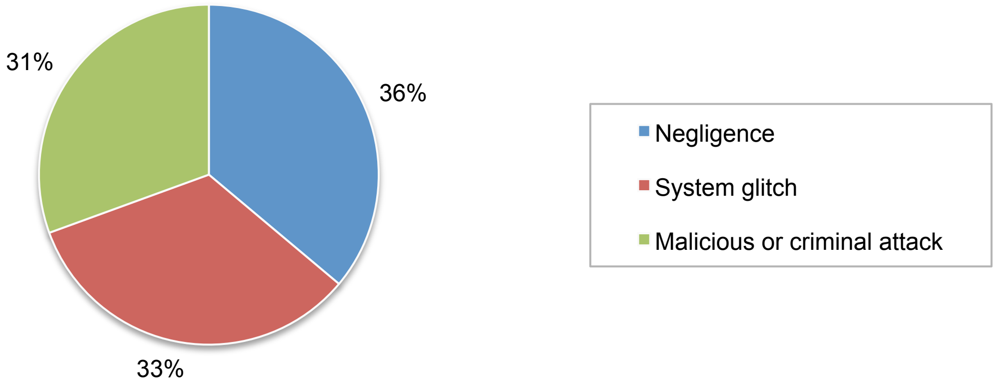
Figure 4 reports the per capita costs for the 2011 study by industry classification. While small sample size prevents us from generalising industry cost differences, the pattern of 2011 industry results is consistent with prior years. Accordingly, financial service companies tend to have a per capita cost above the mean (£103) and retail companies have a per capita cost below the mean (£60).

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 36 organisations. Thirty-six percent of incidents involved a negligent employee or contractor, 33 percent involved system glitches, including a combination of both IT and business process failures, and 31 percent experienced a malicious or criminal attack.[4]

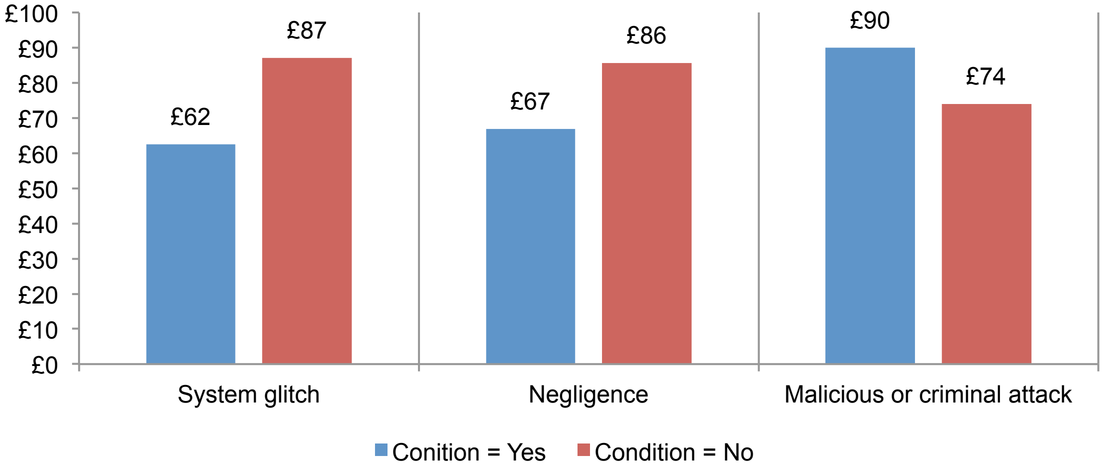
Figure 5. Distribution of the benchmark sample by root cause of the data breach



[4] Malicious and criminal attacks increased slightly from 29 percent in our 2010 study.

Malicious attacks are most costly. Hackers or criminal insiders (employees, contractors and other third parties) typically cause the data breach as determined by the post data breach investigation. Figure 6 reports per capita cost of data breach for three conditions or root causes of the breach incident. Again, the pattern of results in 2011 is consistent with prior years' research; wherein the most costly breaches typically involve malicious acts against the company rather than negligence or system glitches. Accordingly, companies that experience malicious or criminal attacks have a per capita cost above the mean (£90) and companies experiencing system glitches have a per capita cost below the mean (£62).

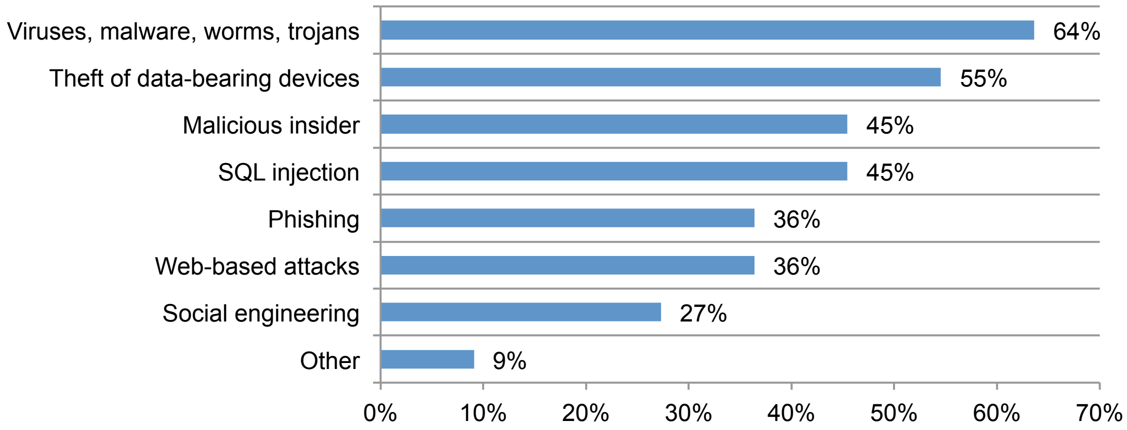
Figure 6. Per capita cost for three root causes of the data breach



Criminal attacks are mainly electronic agents. In this year's report, we analysed the findings from the 18 organisations that report their data breach was caused by a malicious insider or hacker as previously described. Figure 7 summarises the types of criminal attacks experienced. Please note that a given company might have experienced three or more of these attacks.

As can be seen, 64 percent of the subsample experienced electronic agents such as viruses, malware, worms and trojans. Fifty-five percent experienced theft of data-bearing devices. Forty-five percent experienced malicious insiders such as rogue employees or contractors and SQL injection (45 percent). Other major conditions include phishing (including spear phishing) and web-based (36 percent) attacks.

Figure 7. Analysis of malicious or criminal attacks experienced by 11 companies
More than one attack type may exist for each company



Six positive and negative attributes can influence the cost of a data breach. Over the years of conducting this research, we have identified six attributes that can influence the cost of a data breach. The percent of organisations in this study that have these attributes is shown in Figure 8.

- **CISO (or equivalent title) has overall responsibility for enterprise data protection**. Forty-two percent of participating organisations have centralised the management of data protection with the appointment of a C-level security professional.
- **Organisations notified data breach victims quickly.** Another 33 percent say their organisations quickly notified appropriate parties within 30 days from initial discovery.
- **Data was lost or stolen due to third-party botches**. Thirty-three percent of organisations say their data breach involved one or more third parties – including outsourcers, cloud providers and business partners.
- **The data breach involved lost or stolen devices**. A significant percentage of organisations (31 percent) say their breach incident involved one or more lost or stolen data-bearing devices – which included laptops, smartphones, tablets and servers.
- **Consultants are engaged to help remediate the data breach**. Twenty-eight percent say they engaged a consultant to assist in the data breach response or remediation.
- **It is the first time the organisation had a data breach**. Most of the organisations in this year’s study have experienced more than one data breach. Only 28 percent say the incident was their first data breach involving 1,000+ records.

Figure 8. Defining attributes for the benchmark sample

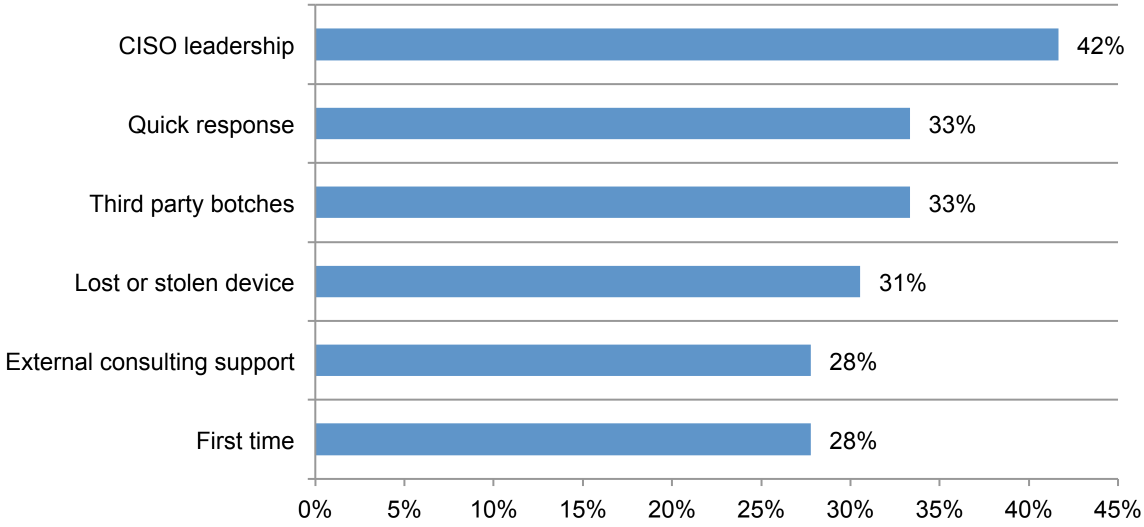


Figure 9 summarises the per capita costs for six normatively important conditions or attributes about the benchmark sample. As previously mentioned, these attributes were selected based on learned experiences from previous cost benchmark studies. Per capita costs are above the mean for third party botches and those experiencing a lost or stolen device. Per capita costs are below the mean for organisations engaging external consultants and having an information security leader (CISO) with enterprise-wide responsibility for data protection.

Figure 9. Per capita cost for six attributes or conditions

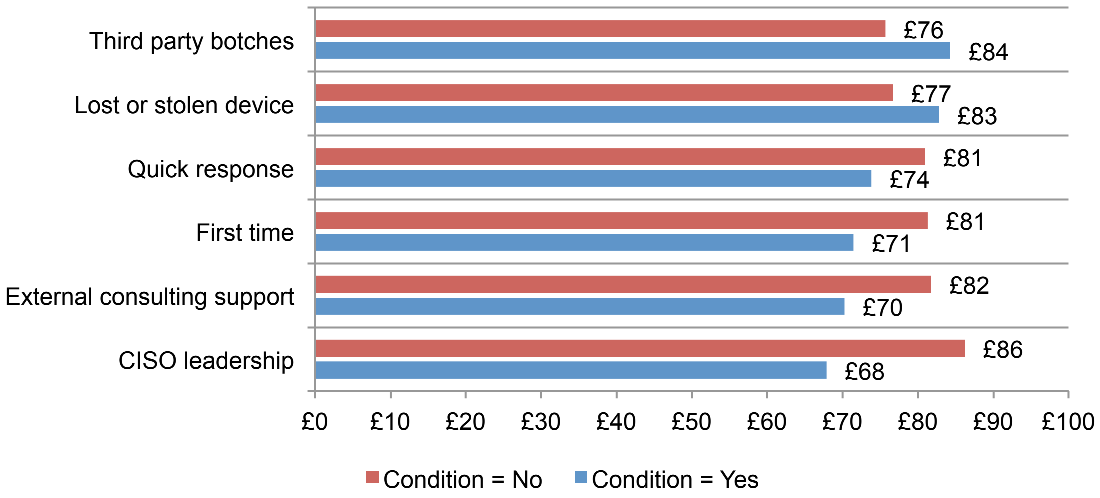


Figure 10 summarises the per capita cost differences for seven normatively important conditions or attributes about the benchmark sample.   In this analysis, a negative difference means that the attribute or condition moderates (lessens) the data breach costs. A positive difference has the opposite meaning.

As can be seen, organisations that employ a CISO with enterprise-wide responsibility for data protection experience an £18 cost saving per compromised record. Organisations engaging an external consultant benefit from a £11 cost saving. In contrast to organisations in other countries, UK organisations that say the reported data breach is their first serious incident have a lower per capita cost (£10) than more experienced companies. Finally, organisations that respond quickly to the data breach incident appear to have a lower per capita cost (£7).

Figure 10. Per capita cost differences for six attributes or conditions

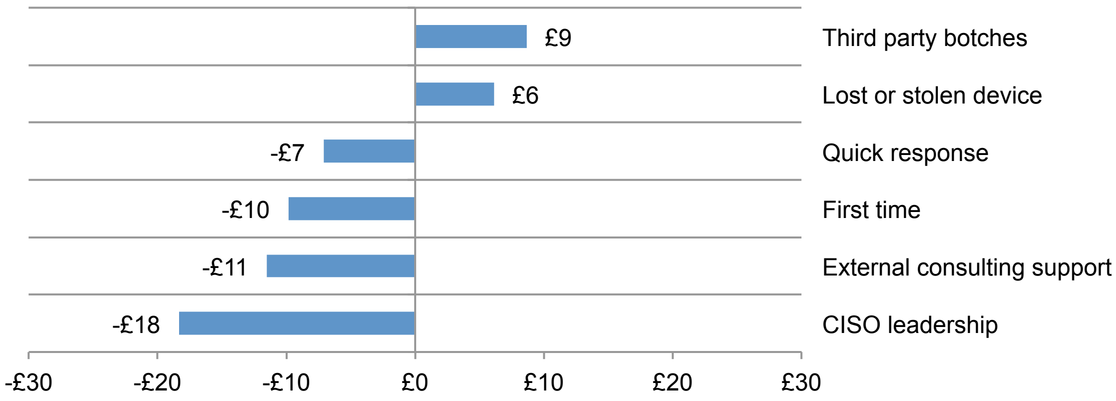
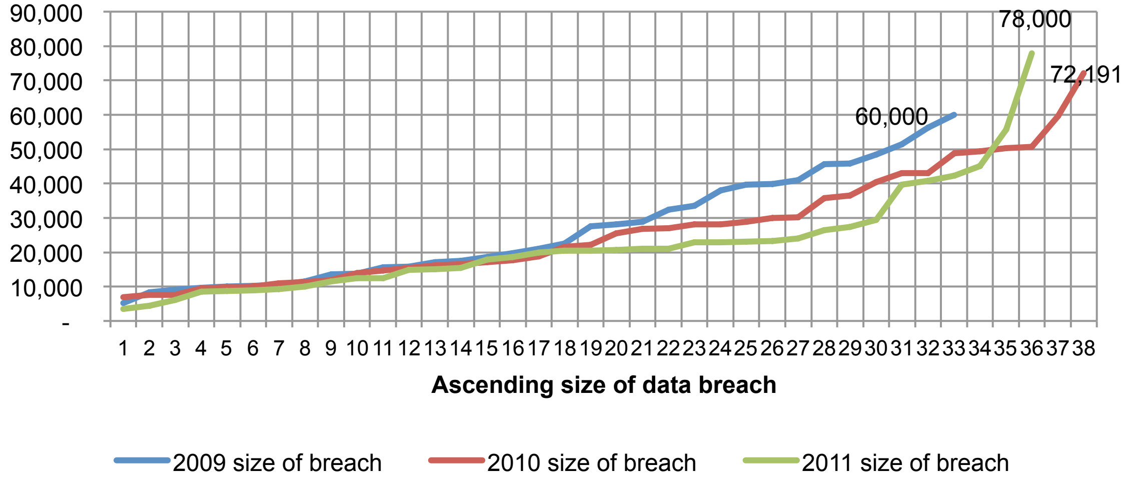


Figure 11 shows, in ascending order, the number of lost or stolen records involved in data breach incidents included in studies conducted over the past three years. According to the figure, the number of compromised records has remained consistent since 2009. The benchmark samples do not contain data breach incidents involving millions of compromised records. In our experience, these so-called "mega breaches" are rare events and including them would skew results. The largest data breach incident in this year's study involved 78,000 records.

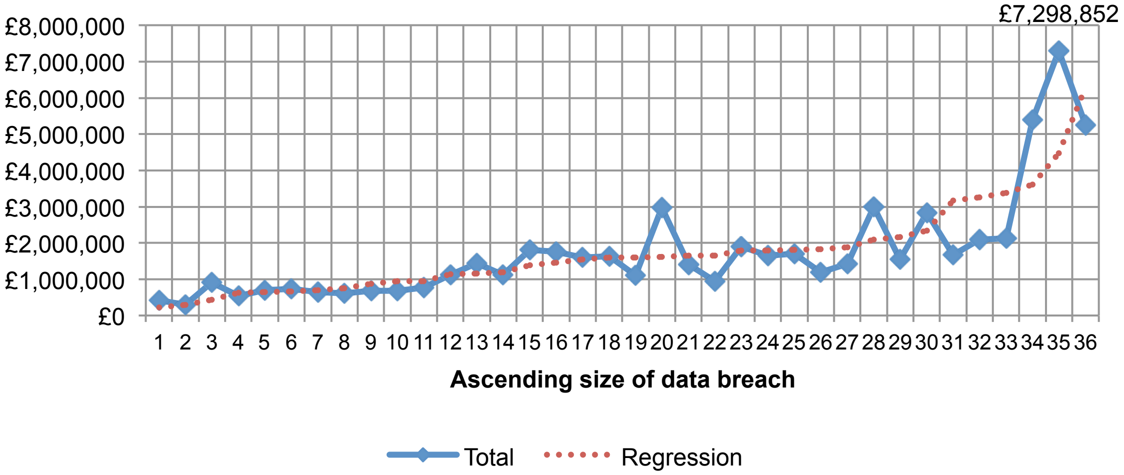
Figure 11. Ascending frequency of compromised records over three years



The more records lost, the higher the cost of the data breach. Figure 12 shows the relationship between the total cost of a data breach and the size of the incident for 36 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 £299,053 to £7,298,852.

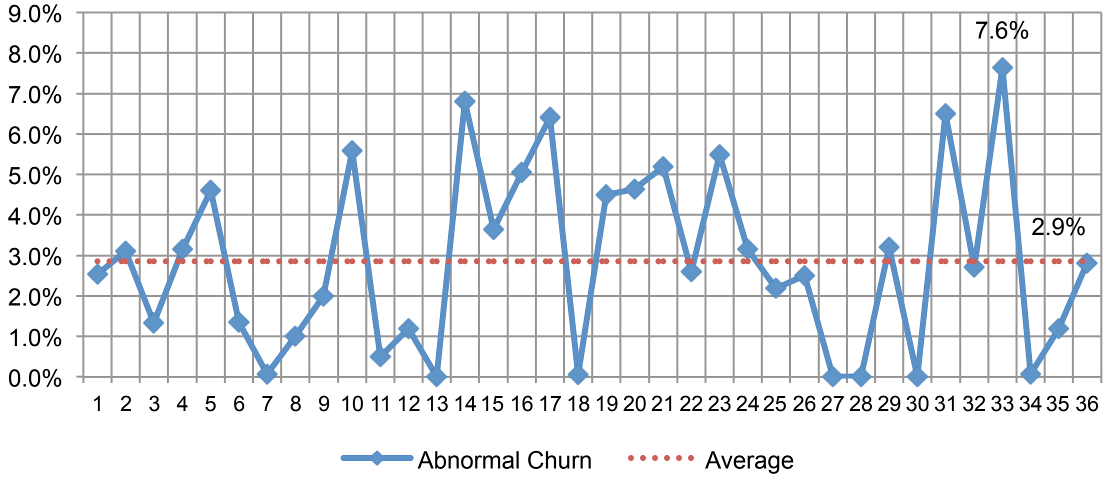
Figure 12. Total cost of data breach by size of lost or stolen records

Regression = Intercept + {Size of Breach Event} x β, where β denotes the slope.



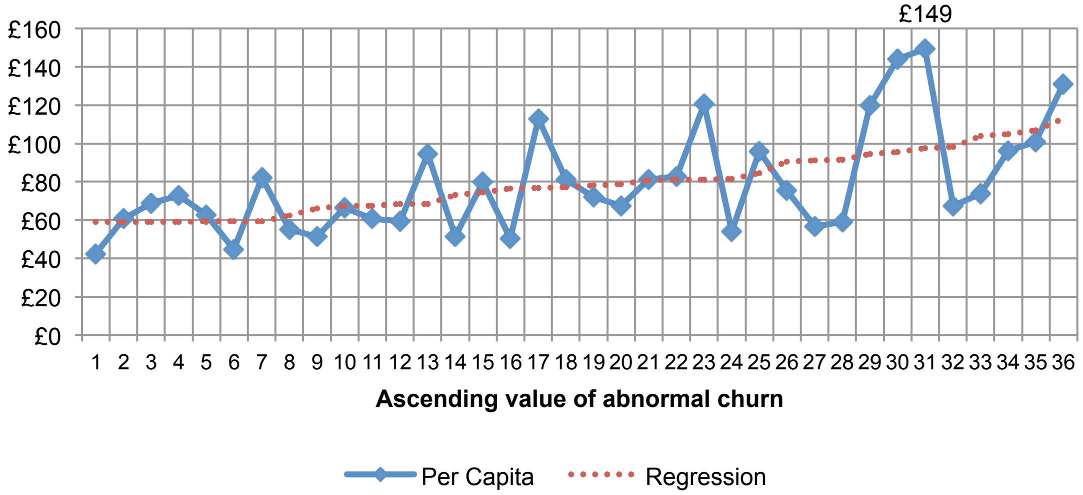
More customers remain loyal to organisations following a data breach. Figure 13 shows the abnormal churn rates for each one of the 36 organisations included in this research. As shown, the churn rate distribution is varied, with a range of 0 (no abnormal churn) to 7.6 percent. It is important to note that the average abnormal churn decreased from 3.3 percent in the 2010 study to 2.9 percent this year.

Figure 13. Distribution of abnormal churn rates for 36 benchmark companies



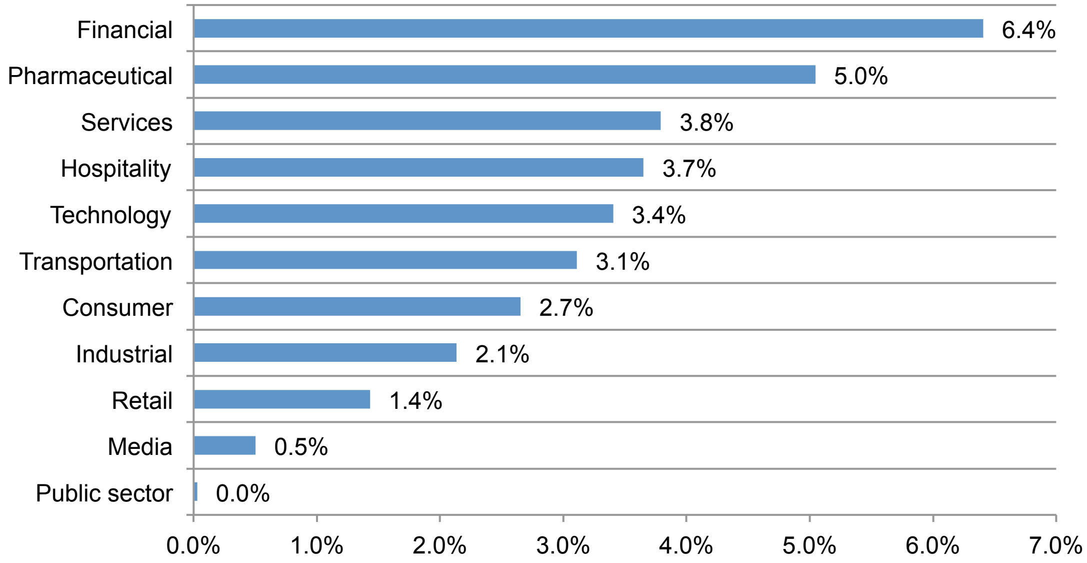
The more churn, the higher the cost of a data breach. Figure 14 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, which suggests that abnormal churn is linearly related to cost. This pattern of results is consistent with benchmark studies completed in prior years.

Figure 14. Distribution of per capita costs in ascending value of abnormal churn rates
Regression = Intercept + {Abnormal Churn} x β, where β denotes the slope.



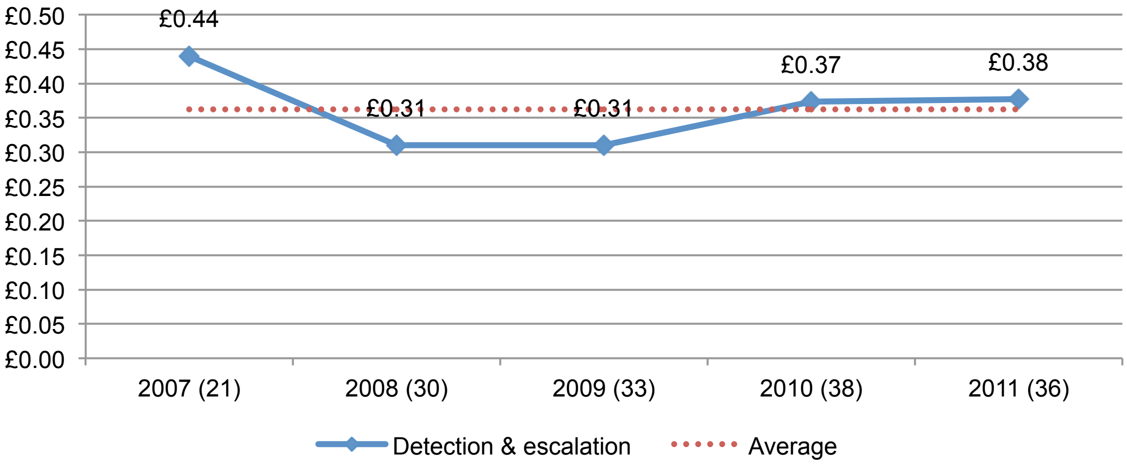
Certain industries are more vulnerable to churn. Figure 15 reports the abnormal churn rate of benchmarked organisations for the 2011 study. While small sample size prevents us from generalising the affect of industry on data breach cost, our 2011 industry results are consistent with prior years – wherein financial service organisations tend to experience relatively high abnormal churn and retail companies tend to experience a relatively low abnormal churn.[5]

Figure 15. Abnormal churn rates by industry classification of benchmarked companies



Detection and escalation costs are slightly higher this year. Figure 16 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 cost increased slightly from £373,191 in 2010 to £376,773 in the present study. The highest value was £440,000 in 2007.

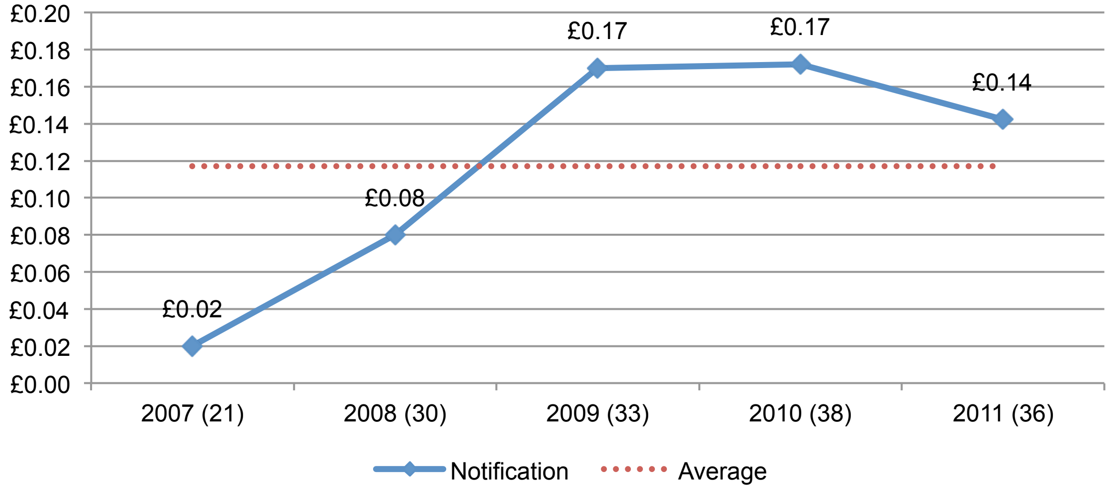
Figure 16. Average detection and escalation costs over five years
£000,000 omitted (sample size in brackets)



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

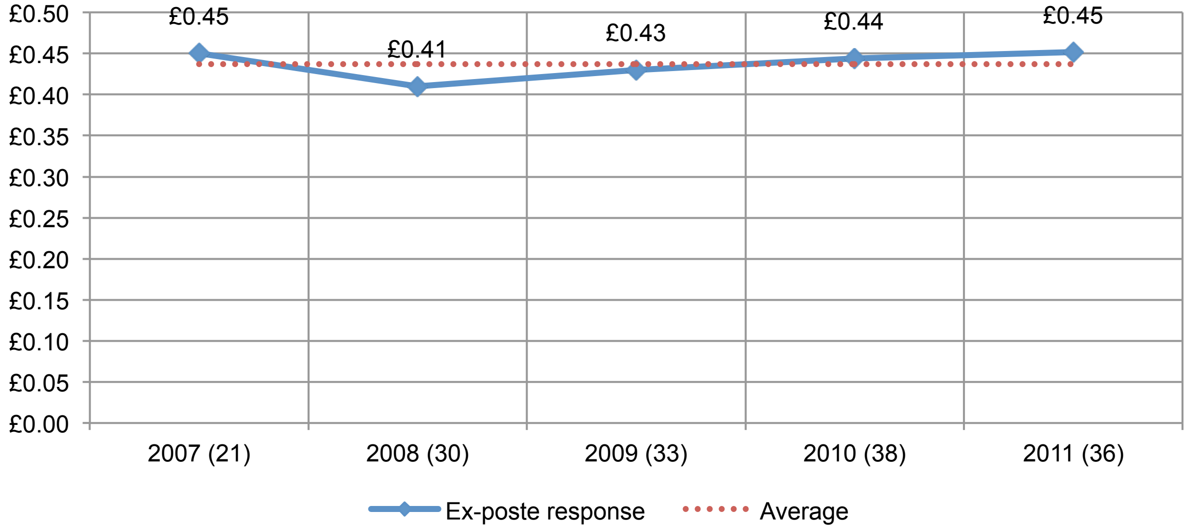
Notification costs decrease. Figure 17 reports the distribution of costs associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, secondary contacts to mail or email bounce-backs and inbound communication set-up. This year's average notification is £142,399. This represents a decrease from £172,218 in 2010, which is the highest cost of notification over five years.

Figure 17. Average notification costs over five years
£000,000 omitted (sample size in brackets)



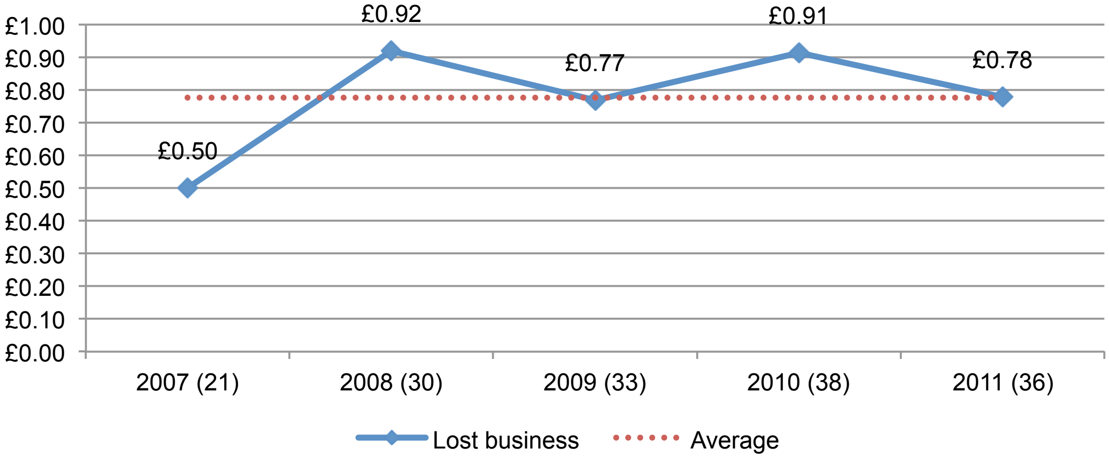
Post data breach costs increase. Figure 18 shows the distribution of costs associated with ex-poste (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-poste response cost increased from £443,946 in 2010 to a five-year high of £451,446 in this year's study.

Figure 18. Average ex-poste response costs over five years
£000,000 omitted (sample size in brackets)



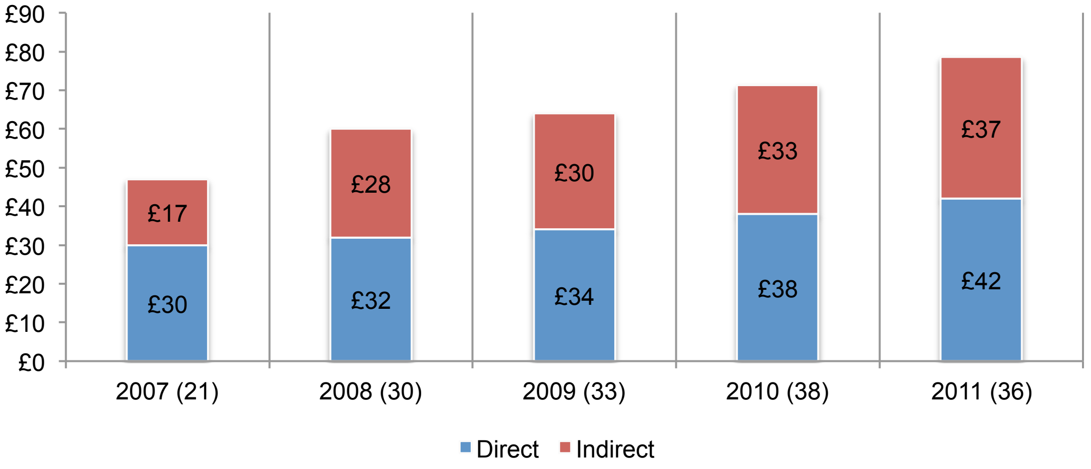
Lost business costs declined sharply. Figure 19 reports lost business costs associated with data breach incidents over five years. Such costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs sharply decreased from £913,910 in 2010 to £779,414 in 2011. The highest lost business cost over five years is £920,000, which occurred in 2008.

Figure 19. Average lost business costs over five years
£000,000 omitted (sample size in brackets)



Both direct and indirect costs increased. Figure 20 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 £71 in 2010 to £79 in 2011. Approximately, £4 of this increase pertains to direct cost. In the present study, indirect cost represents 47 percent of total per capita cost, which is identical to the 2010 indirect cost percentage.

Figure 20. Direct and indirect per capita data breach cost over five years
Sample size in brackets



Organisations with a positive security posture are more successful in reducing the impact of a data breach. We measured the security posture of each participating company using the Security Effectiveness Score (SES) as part of the benchmarking process. [6] Figure 21 reports the SES Index for 36 organisations. The SES range of possible scores is +2 (most favoruable) to -2 (least favourable). Compiled results for the present benchmark sample vary from a high of +1.34 to a low of -1.63, with a mean value at +0.20.

Figure 21. Distribution of Security Effectiveness Scores for 36 benchmark companies

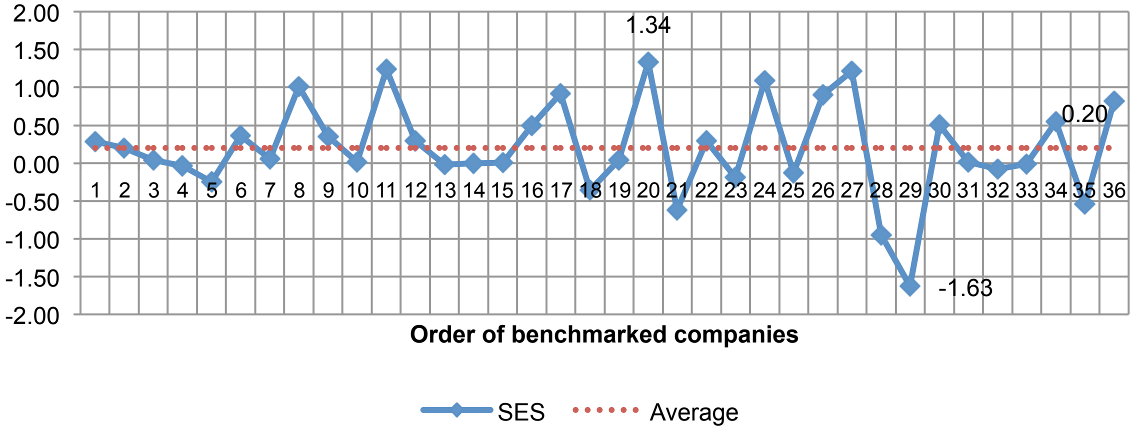
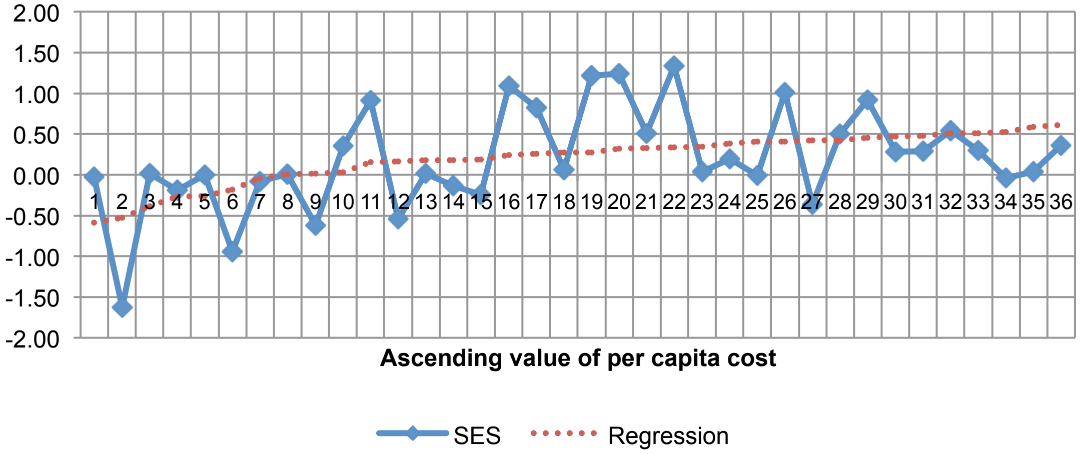


Figure 22 reports the distribution of per capita data breach cost in ascending value of abnormal churn. The regression line is upward sloping, suggesting that the Security Effectiveness Score (SES) for each organisation is inversely related to their per capita data breach cost. In other words, a strong security posture appears to moderate data breach costs.

Figure 22. Security Effectiveness Score (SES) in ascending value of per capita cost
Regression = Intercept + {Per Capita Cost} x β, where β denotes the slope.



[6] 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 practises. 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 favorable.

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 top preventive measures and controls implemented after the data breach are: manual procedures and controls (40 percent), additional training and awareness activities (39 percent), expanded use of encryption (35 percent) and data loss prevention solutions (33 percent).

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

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

Table 2 provides the percentage changes for 11 cost categories over five years. As can be seen, most cost categories appear to be relatively stable over time. However, public relation and communication costs have steadily increased from one percent in 2007 to five percent in 2011. In contrast, audit and consulting services have decreased from 14 percent in 2007 to nine percent in 2011.

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

Part 3. Concluding observations and description about participating companies

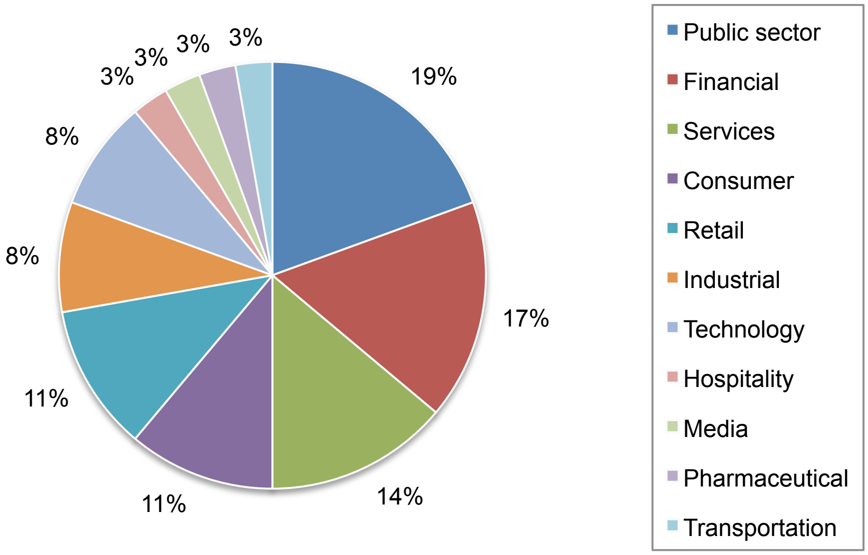
For the first time, companies participating in our annual study report that their data breaches were smaller in scale and resulted in a lower rate of churn. We conclude that companies' investment in improving their data protection practises is paying off. The most profitable investments as evidenced by the lower cost of a data breach are: the appointment of a CISO with enterprise-wide responsibility and the engagement of external consultants.

The study also reveals the severe financial consequences from malicious or criminal acts. These data breaches can prove to be the most costly. We hope this study is helpful to understanding 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.

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.

Pie Chart 1 shows the distribution of benchmark organisations by their primary industry classification. In this year's study, 11 industries are represented. Public sector (government), financial services, and services companies represent the three largest segments.[7]

Figure 23. Distribution of the benchmark sample by industry segment



[7] 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.[8]
- 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.[9] 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

[8] 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.

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

of customer or consumer [10]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.[11]

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.

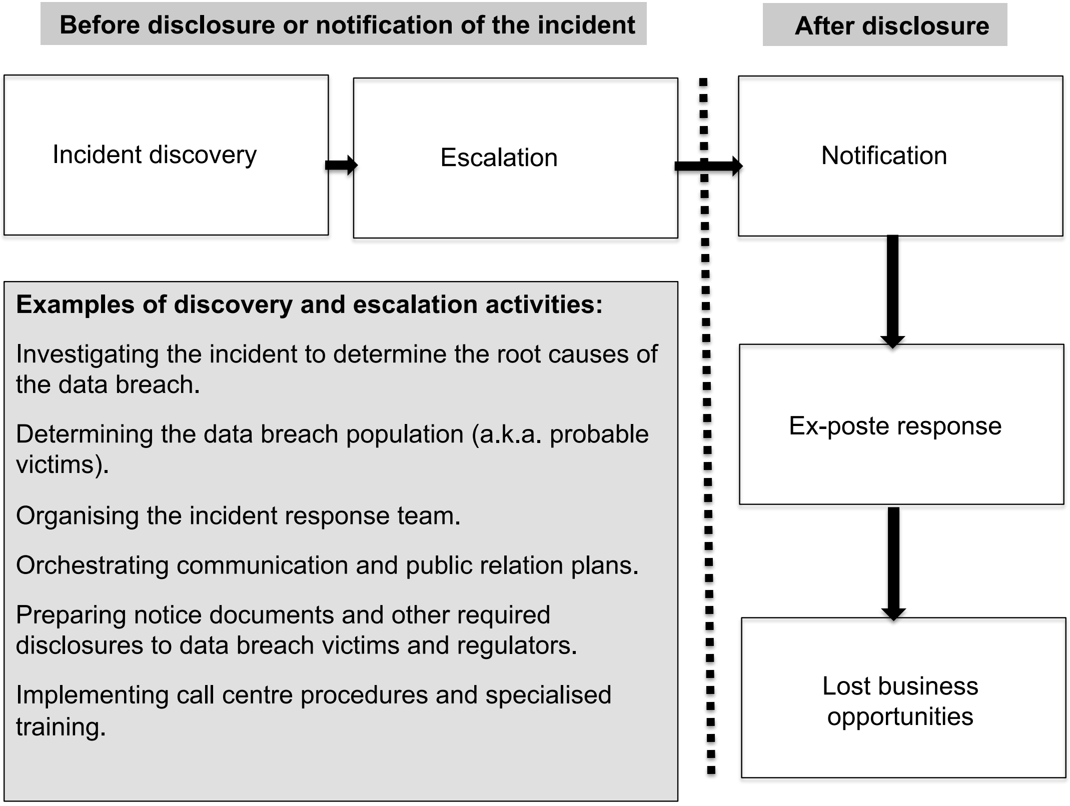
The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information. We believed that a study focused on business process – and not data protection or privacy compliance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

[10] 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.

[11] 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 1 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 24: Schema of the data breach process


Before disclosure or notification of the incident
After disclosure
Incident discovery
Escalation
Notification
Ex-poste response
Lost business opportunities

Examples of discovery and escalation activities:

Investigating the incident to determine the root causes of the data breach.

Determining the data breach population (a.k.a. probable victims).

Organising the incident response team.

Orchestrating communication and public relation plans.

Preparing notice documents and other required disclosures to data breach victims and regulators.

Implementing call centre procedures and specialised training.

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.

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-six 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.

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.

Appendix 1: Cost for 36 Data Breach Case Studies

Cases	Size of breach	Detection & escalation*	Notification*	Ex-poste response*	Lost business*	Abnormal Churn
1	3,500	34,633	35,765	10,948	340,710	5.5%
2	11,532	159,981	52,387	273,564	200,917	5.2%
3	9,300	147,502	233,898	247,951	9,478	7.6%
4	6,147	101,509	270,854	106,677	438,208	3.2%
5	12,500	104,841	285,710	205,479	164,895	5.0%
6	9,000	154,060	354,855	205,383	25,672	2.5%
7	8,544	103,564	339,211	84,154	9,394	6.8%
8	8,666	224,303	60,917	328,446	89,076	6.5%
9	10,000	118,007	335,500	140,857	11,332	3.7%
10	23,954	115,539	143,303	888,085	271,770	1.4%
11	12,500	135,294	45,807	216,102	291,654	3.2%
12	4,500	93,342	55,143	49,517	101,051	0.1%
13	17,923	129,994	26,053	154,092	1,495,378	3.1%
14	21,000	63,658	80,000	280,991	987,982	2.6%
15	20,490	558,366	127,999	155,487	265,642	2.2%
16	23,067	134,653	74,362	380,143	1,109,313	4.5%
17	22,850	240,462	133,577	697,166	824,362	6.4%
18	19,834	134,038	46,444	216,894	1,209,272	0.0%
19	21,000	363,327	130,339	443,294	2,188	2.7%
20	15,500	502,612	467,246	152,295	5,596	0.0%
21	29,498	526,264	28,749	384,435	1,894,059	2.8%
22	14,850	243,773	170,915	334,822	369,708	5.6%
23	23,299	240,128	9,133	406,339	541,056	1.2%
24	20,482	1,043,347	88,392	373,305	131,841	0.1%
25	22,896	337,538	20,050	233,621	1,063,002	1.2%
26	26,450	569,072	52,445	251,112	2,114,391	0.0%
27	40,750	496,224	27,972	870,002	700,765	1.3%
28	27,300	712,415	42,078	576,509	218,728	4.6%
29	78,000	1,135,373	85,066	520,631	3,515,764	0.0%
30	42,259	441,037	16,299	531,353	1,144,797	4.6%
31	18,635	406,670	183,887	471,426	699,789	0.5%
32	20,602	696,629	325,288	938,591	1,006,468	3.2%
33	39,600	420,823	379,014	869,388	2,265	1.0%
34	55,700	1,989,255	158,400	1,496,875	3,654,322	2.0%
35	45,000	382,308	133,049	2,359,216	2,517,208	2.5%
36	15,000	303,273	106,246	396,915	630,844	0.1%

* Measured in GBP (£)