



# 2010 Annual Study: U.K. Cost of a Data Breach

Compliance pressures, cyber attacks targeting sensitive data drive leading IT organisations to sometimes pay more than necessary

A benchmark study of 38 U.K. companies about the financial impact, customer turnover and preventive solutions related to breaches of sensitive data

March 2011

Research conducted by  
***Ponemon Institute, LLC***



2011 Symantec Corporation

Approved for redistribution by the Ponemon Institute.

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of Symantec Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications. Symantec and the Symantec Logo are registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners.

NO WARRANTY. Symantec makes this document available AS-IS, and makes no warranty as to its accuracy or use. The information in contained in this document may include inaccuracies or typographical errors, and may not reflect the most current developments, and Symantec does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Symantec reserves the right to make changes at any time without prior notice.

# Table of Contents

- EXECUTIVE SUMMARY ..... 3**
  - 2010 ANNUAL STUDY: COST OF A DATA BREACH.....4
  - SUGGESTED PREVENTIVE SOLUTIONS..... 7
  - NEXT STEPS ..... 7
- INTRODUCTION..... 8**
- STUDY OVERVIEW & METHODOLOGY.....10**
  - STUDY METHODOLOGY ..... 10
- KEY REPORT FINDINGS..... 12**
- REPORT CONCLUSIONS..... 34**
  - SUGGESTED PREVENTIVE SOLUTIONS..... 35
  - NEXT STEPS ..... 35
  - ABOUT THE PONEMON INSTITUTE ..... 36
  - ABOUT SYMANTEC CORPORATION ..... 36
- APPENDIX A – STUDY METHODOLOGY ..... 37**
  - BENCHMARK METHODS ..... 37

## Executive Summary

Symantec Corporation and the Ponemon Institute proudly present *2010 Annual Study: U.K. Cost of a Data Breach*, our fourth annual study concerning the cost of data breach incidents for U.K. companies. Ponemon Institute research indicates that data breaches continue to have serious financial consequences for organisations. This year, multiple factors apparently confirm that data breach mitigation and regulatory compliance drive companies' data breach costs – and, in some cases, may lead them to pay much more than they would otherwise.

This benchmark study examines data breach costs to organisations resulting in the loss or theft of protected personal data. As a benchmark study, *Cost of a Data Breach* differs greatly from the standard survey study, which typically requires hundreds of respondents for the findings to be statistically valid. Benchmark studies are valid because the sample is designed to represent the population studied. They intentionally limit the number of organisations participating and involve an entirely different data-gathering process.

In a survey, the unit of analysis is an individual. In this benchmark study, the unit of analysis is an organisation. Each company represents one case study. We conduct in-person and telephone interviews with many individuals in participating organisations. This process can take several months to complete. In sum, benchmark studies are far more difficult to execute and analyse than standard survey research.

The findings of this benchmark study pertain to the actual data breach experiences of 38 U.K. companies from 13 different industry sectors, all of which participated in the 2010 study. We believe the findings of this study are important because they can be generally applied to U.K. organisations that experience large data breaches (between 1,000 and 100,000 compromised records).

The Ponemon Institute conducted its first *Cost of a Data Breach* study in the United States six years ago. Since then, we have expanded the study to include the United Kingdom, Germany, France and Australia. The initial study established objective methods for quantifying specific activities that result in direct and indirect costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law. To maintain consistency from prior years, our methods for quantifying data breach costs has remained relatively constant.

Our current analysis of the actual data breach experiences of 38 U.K. companies from 13 different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response. We also analyse the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates.

Utilising activity-based costing, our methods capture information about direct expenses such as engaging forensic experts, outsourced hotline support, free credit monitoring subscriptions, and discounts for future products and services. We also capture indirect costs such as in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates.

To understand how organisations are performing, the Ponemon Institute continues to track the index of organisations' IT security effectiveness known as the Security Effectiveness Score (SES). The SES is based on respondents' self-evaluation of their IT organisation across 24 attributes and is used throughout the study to answer questions, make comparisons and identify trends. We reference SES where appropriate throughout the report.

This report reveals how much companies pay for each kind of data breach studied, based both on primary breach causes and organisations' common breach response. We also discuss any changes from previous benchmark studies and what those changes mean to organisations in an evolving data protection environment.

We base our conclusion -- that the focus on data breach mitigation and regulatory compliance profoundly affects company behaviour and may increase some data breach costs -- on key findings, including:

- Defending against malicious or criminal attacks and lack of internal preparedness and expertise appear to drive spending on data breach costs
- Malicious or criminal attacks remain the most expensive breach cause and, for the first time, are the most expensive breach type overall
- Eighty percent of breach attributes are less frequent than last year
- Lost business and ex-post response are becoming the main components of data breach costs

## 2010 Annual Study: Cost of a Data Breach

This 2010 Ponemon Institute benchmark study, sponsored by Symantec Corporation, examines the costs incurred by 38 organisations after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the fourth annual study of this issue.

Breaches included in the study ranged from 6,900 records to 72,000 records from 13 different industry sectors.

### What we learned from the 2010 results:

#### *Top Findings*

**Defending against malicious or criminal attacks and lack of internal preparedness and expertise appear to drive spending on data breach costs:** The highest costs in 2010 belonged to breach types that reflect failure to address the most prominent and dangerous data breach causes: malicious or criminal attacks and overall lack of preparedness that can lead companies to become breach victims. The opposite was also true: companies that avoided problems and had sufficient internal expertise and experience with data breaches fared better.

Costs rose the fastest for breaches involving proactive breach response and preparation and expertise that regulations demand for compliance (SES above the median, quick response and those not involving third-party mistakes, systems failures or lost or stolen devices). At the same time, costs were lowest and shrinking for breaches lacking both internal (systems failures) and external (third-party mistakes) preparation and expertise for compliance.

An interesting trend in this year's data is that eight out of ten breach attributes saw the cost difference narrow between the presence of the attribute and its absence. This means that organisations became more likely to incur certain response costs whether or not they prepared for a certain kind of breach.

**Malicious or criminal attacks remain the most expensive breach cause and, for the first time, are the most expensive breach type overall:** Of the three overarching breach categories – malicious or criminal attacks, negligence and systems failures -- malicious or criminal attacks accounted for 29 percent in 2010. That number is up 5 points from 2009. In 2010 the cost per compromised record of a data breach involving a malicious or criminal act averaged £80, up £4 (5 percent) from 2009. The high cost may reinforce the extreme danger hostile breaches pose.

**Eighty percent of breach attributes are less frequent than last year:** Out of ten data breach attributes tracked in this study, only two – malicious or criminal attacks and systems failures – became more common between 2009 and 2010. All other causes and response attributes became less frequent.

An interesting trend in this year's data was how often the lack of IT security acumen led to higher breach costs. Fifty-eight percent of respondents had an SES below the median and 68 percent lacked CISO leadership, meaning well more than half of companies could unnecessarily pay some of the highest breach costs. Even more respondents cut back on external consulting support, which provided relatively minor savings. These figures may indicate that organisations' growing experience with data breaches may lead them to believe they don't need good security postures or specialised help for breach response. We will closely watch this issue in future reports.

Systems failures became a much bigger priority this year and had the most distinctive results. More than one-third of breaches (37 percent) were due to systems failures, up 7 points from 2009, the biggest rise of any data breach attribute and making it the most common breach cause this year. More companies have data breach experience and fewer reported breaches due to negligence, lost or stolen devices and third-party mistakes.

Taken together, these figures may indicate that fear of data breaches and cyber attacks may be driving more companies to devote much more effort to IT security. Companies' increasing focus on data breach mitigation and regulatory compliance may be encouraging them to discover more systems failures behind data breaches – especially when breach response costs from systems failures are the lowest in this study and are getting cheaper. We will closely watch this issue as well.

**Lost business and ex-post response are becoming the main components of data breach costs:** Recovering customers, profits and business opportunities after data breaches posed the greatest cost hurdles for companies in 2010 – even more than data breach response itself. Lost business and detection and escalation costs rose the most, while ex-post response stayed level and notification costs fell a little. Lost business costs rose the fastest.

Lost business accounted for 48 percent of overall data breach costs, up 2 points from 2009. Ex-post response comprised 23 percent, down 3 points. Detection and escalation rose 2 points to 20 percent. Finally, notification costs remained by far the smallest cost component. It accounted for 9 percent of 2010 costs, down 1 percent from 2009.

Taken together, these figures appear to support findings from the *2010 Annual Study: U.K. Enterprise Encryption Trends* report, also conducted by the Ponemon Institute and sponsored by Symantec.<sup>1</sup> That report found that data breach mitigation and complying with data protection and privacy regulations are rapidly becoming the primary reasons organisations use encryption and other data protection technologies.

### **Overall Trends**

**For the third year in a row, data breach costs have continued to rise:** Data breaches continue to cost organisations more every year. The average organisational cost of a data breach this year increased to £1.9 million, up 13 percent from 2009 and 10 percent from 2008. Data breaches in 2010 cost an average of £71 per compromised record, up £6 (9 percent) from 2009 and up £11 (18 percent) from 2008.

Data breaches are costing more at both ends of the scale, but particularly the top. The most expensive data breach included in this year's study cost a company £6.2 million to resolve, up £2.3 million (60 percent) from last year. The least expensive data breach was £336,000, down £29,000 (8 percent) from 2009. Breach size this year ranged from 6,900 to 72,000 lost or stolen records, with larger breaches continuing to be a more serious threat than smaller ones.

**Both direct costs and indirect costs continue to rise:** This year's figures indicate that companies are continuing to spend more on both kinds of costs. In 2010, direct costs accounted on average for £38 (54 percent) of the total average cost per record, up £4 (12 percent). Indirect costs in 2010 were £33 (46 percent) of the total, up £3 (10 percent). Among specific cost activities, organisations continued to spend the most on lost customer business due to churn (up 1 point to 42 percent) and investigations and forensics (12 percent, almost unchanged since 2008).

**Customer turnover in direct response to breaches remains the main driver of data breach costs:** Abnormal churn or turnover of customers after data breaches appears to remain the dominant data breach cost factor. Regulatory compliance helps lower churn rates by boosting customer confidence in companies' IT security practices.

Average abnormal churn rates across all 38 incidents dropped a point to 3 percent. The sectors with the highest 2010 churn rate were communications, financial and services, all at 7 percent. The industries with the lowest abnormal churn rates were transportation (2 percent), consumer and retail (each at 1 percent) and public sector (less than 1 percent). Sectors with the highest 2010 average per-record costs were communications (£102), financial (£94) and pharmaceutical (£90). Those with the lowest costs were retail (£45), public sector (£50) and consumer (£51).

**Manual, policy and training-oriented options remained the most popular post-breach preventive and remediation measures:** In 2010, 43 percent of respondents implemented additional manual procedures and controls and 40 percent relied upon training and awareness programs. Frequency of implementation of all listed measures stayed about the same except strengthening perimeter controls, which jumped 8 points from 2009 to 32 percent. Even though organisations still far prefer using traditional approaches, this year's figures may indicate companies are starting to see more value in technology that can help prevent and mitigate data breaches.

### **Data Breach Types – Cause<sup>2</sup>**

**Breaches involving third-party mistakes by outsourcers are still a major worry and expense:** Data breaches from third-party mistakes decreased marginally in 2010 to 34 percent, down 2 points. The cost of such breaches fell as well, down £7 (9 percent) to £74 per record. The marked drops in both cost and rank of third-party breaches may

<sup>1</sup> *2010 Annual Study: U.K. Enterprise Encryption Trends*, The Ponemon Institute, Nov 2010

<sup>2</sup> Causes also include malicious or criminal attacks discussed in the Top Findings.

indicate that whilst the security of outsourced data remains important, those breaches became a much lower priority in 2010. Companies may be focusing more on internal breaches, as those costs rose quickly. Organisations may also feel confident enough in dealing with third-party breaches to handle them cost-effectively and put other concerns first.

**Breaches involving data on lost or stolen devices are expensive and may reflect anxiety about insecure use of mobile technologies:** The frequency of breaches concerning mobile devices holding sensitive data stayed about the same in 2010, down 1 point to 29 percent. Per-record costs rose £3 (4 percent) to £72. The relative stability of both the frequency and severity of device-oriented breaches this year may indicate that organisations feel confident in their ability to identify and mitigate such risks. The *2010 Enterprise Encryption Trends* report found that companies fear insecure use of mobile technologies as much or more than direct cyber attacks against their IT systems.

**Negligent breaches are becoming much less frequent:** The number of breaches attributed to negligence fell 11 points to 34 percent. Breach costs for negligence rose sharply as well. Breaches from negligence in 2010 averaged £66 per record, up £10 (18 percent) from 2009. Breaches from negligence in 2010 averaged £87 per record, up £2 (2 percent) from 2009. The sharp drop in breaches due to negligence may stem from increased awareness of data breaches pose and more conscientious efforts to prevent them through education and compliance.

**Breaches from systems failures are becoming more common, less expensive and quite distinctive:** As stated above, the most common breach cause this year was systems failures, up 7 points to 37 percent. Breaches from systems failures averaged £59, down £5 (8 percent). It was one of only two types that were cheaper than last year (the other being the presence of third-party mistakes). Along with CISO leadership, it was part of another unique pair that saw the cost difference widen between breaches involving it and those that did not. The results are all the more noticeable because last year breaches with systems failures and those without them cost the same, £64.

#### **Data Breach Types – Response**

**First-time breaches are one of the most expensive breach types but are becoming much less common:** A third (32 percent) of respondents faced their first data breaches. That figure has declined 10 points from 2009, one of the biggest drops of any breach type. This year, the cost per compromised record of an organisation's first data breach averaged £74 (up £6 or 9 percent). These findings may indicate that the pool of first timers is shrinking due to both an increase in compliance activities to prevent breaches and a larger pool of prior breach victims over time. As stated above, attacks are becoming more insidious and damaging, which requires greater resources to combat.

**Rapid response to data breaches became less frequent and much more expensive:** A third (32 percent) of companies notified victims within one month of discovering the data breach, down 4 points from last year. In 2010, quick responders had a per-record cost of £72, up £16 (29 percent) from the year before. This year's results show that the value of quick response changed this year for U.K. organisations. Previously, quick response led to much lower costs. This year's figures may indicate that quick response became much more expensive between 2009 and 2010. Regulatory compliance pressures may explain these factors.

**Fewer organisations than ever are engaging external consulting support to respond to breaches:** The proportion of respondents that engaged outside consultants fell 10 points this year to 26 percent. This decrease, along with the sharp drop in first-time breach victims, made breaches involving outside consultants the least frequent breach type of 2010. Breaches involving external consultants averaged £69 per record, up £9 or 15 percent. Our results suggest that many fewer companies are using external consulting support, and those that do are seeing a smaller return on their investment in the form of cost savings. We will closely watch this issue in future reports.

**Good security posture remains common and cost-effective, but not as much as last year:** Forty-two percent of respondents had a Security Effectiveness Score (SES) above the median value determined from benchmark results.<sup>3</sup> Even though that figure is down 3 points from last year, good security posture remains the most common breach response attribute. Not surprisingly, those organisations with a more favourable security posture (SES above the median) experienced a lower average cost per compromised record than those with a less favourable posture (SES

---

<sup>3</sup>The SES is a methodology developed in 2005 by the Ponemon Institute and PGP Corporation (which Symantec acquired in 2010) for PGP's annual encryption trends study. The SES measures the effectiveness of an organisation's security posture. Since its inception six years ago, this proprietary security scoring method has been used in nearly 100 studies involving information security practitioners in organisations throughout the world.

below the median). Accordingly, organisations above the median had an average cost per record in 2010 of £67, £15 (29 percent) more than last year. Having an SES above the median, however, saved less money this year than last year and rose much faster. Taken together, these figures may indicate that companies are paying more to ensure good security, perhaps to meet increasing regulatory compliance requirements.

**Despite dramatically lowering breach costs, CISO leadership is becoming much less popular:** A third (32 percent) of respondents had a CISO (or equivalent title) manage data breaches, down 7 points. Breach response involving CISO leadership averaged £63 (up £4 or 7 percent). Our results suggest that expert guidance through CISO leadership can substantially reduce data breach costs. Given these and other reasons, the sharp drop in use of CISO leadership in breach response is thus somewhat counterintuitive. We will closely watch this issue in future reports.

In conclusion, our 2010 research once again suggests that U.K. organisations by and large take their stewardship of sensitive personal data seriously and are taking greater steps to ensure its protection from breaches. Despite its limitations, the research reinforces best practices for IT security and privacy and arguments that those practices provide a positive return on investment. Our research also supports statements by leading industry and government experts who advocate proactive, automated data protection in addition to written policies, procedures and training.

## Suggested Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organisations should strongly consider a holistic approach to protecting data wherever it is – at rest, in motion and in use. While many companies may prefer manual and policy solutions, those tactics alone aren't as effective as a multi-pronged strategy including automated IT security solutions. Many kinds of automated, cost-effective enterprise data protection solutions are now available to secure data both within an organisation and among business partners. Some of the most popular and effective technologies include:

- Encryption (including whole disk encryption and for mobile devices/smartphones)
- Data loss prevention (DLP) solutions
- Identity and access management solutions
- Endpoint security solutions and other anti-malware tools

Companies should also look for centralised management of IT security solutions so they can automatically enforce IT security best practices throughout their organisations. Such capability also enables enterprises to align information protection with corporate security policies and regulatory or business-partner mandates.

## Next Steps

This fourth annual report enables organisations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report provides guidance to conduct an internal audit, create breach response cost estimates and compare technology and other costs of preventing data breaches. Whether or not they have yet had a data breach, companies should also consider the following best practices:

- Vet and evaluate the security posture of third parties before sharing confidential or sensitive information. Pick responsible vendors that can guarantee data protection through encryption and appropriate procedures and controls. Also, ensure that third parties protect data on their employees' mobile devices.
- Ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for extensive business travellers. Also, consider implementing inventory control, anti-theft devices and data loss prevention (DLP) policies, practices and technologies.
- Take as slow and thoughtful an approach to data breach response as possible, given federal and state legal requirements applicable to location, industry and circumstances of the breach. Prepare in advance as much as possible to enable quick and cost-effective response.

## Introduction

2010 marked a number of milestones in British data protection and the fight against data breaches. Both the U.K. Government and the European Commission took decisive steps to strengthen data breach notification requirements, while high-profile data breaches continued to make headlines and damage lives and businesses.

The United Kingdom has a strong tradition of IT security and remains at the forefront of deploying data protection technologies to protect critical systems and data. That is fortunate because companies have never experienced the intensity of IT implementation challenges, regulatory requirements and data security threats that they face today. The twin onslaughts of data breaches and cyber attacks have thus driven the British Government to make improving cybersecurity – and particularly protection of the nation's cyber infrastructure and sensitive data – a national priority.

As a result of these pressures and public demand, the Ministry of Justice (MOJ) in January 2010 provided its privacy watchdog, the Information Commissioner's Office (ICO), with some long-awaited and much-needed bite. In April 2010, the MOJ authorised the ICO to assess fines of up to £500,000 against individuals responsible for serious breaches of the Data Protection Act, putting the ICO on par with many of its European equivalents. The new powers aim to deter behaviour that could cause data breaches and to promote compliance with U.K. data protection legislation. Penalties vary with the sector, size and severity of the breach; the steps organisations took to prevent breaches; and affected organisations' financial resources.

The ICO levied its first two breach-related penalties in November 2010. One fined an employment services company £60,000 after the theft of an unencrypted laptop from an employee's home jeopardised the personal data of 24,000 people. The ICO's announcement emphasised lack of encryption as justifying the penalty. A chance to levy the maximum £500,000 penalty presented itself in September 2010. A cyber attack on a British law firm compromised personal information of more than 9,000 customers of the firm's clients.

In May 2010, the ICO said it had received notice of 1,000 breaches between November 2007 and May 2010 and urged organisations to improve their data protection.<sup>4</sup> Not all data protection-related news was bad. In March 2010, the ICO issued a report providing justifications for proactive business investment in privacy protections.<sup>5</sup> That October, the ICO requested comment on a draft of proposed code of practice for sharing data with third parties.<sup>6</sup>

The victory of the Conservative-Liberal Democrat coalition government in May 2010 brought to power two groups with shared interest in improving data privacy protections.<sup>7</sup> Each party proposed to extend the ICO's audit powers to cover private sector organisations.

Additionally, the European Commission in November 2010 revealed a draft version of its vision to review and modernise the European Union Data Protection legal framework to ensure comprehensive personal data protection for European citizens.<sup>8</sup> A key proposal being made is the creation of a general personal data breach notification requirement for all sectors, which would include criteria for triggering notification.

---

<sup>4</sup> Press Release, Information Commissioner's Office (ICO), 28 May 2010

[http://www.ico.gov.uk/~media/documents/pressreleases/2010/1000\\_DATA\\_BREACHES280510.ashx](http://www.ico.gov.uk/~media/documents/pressreleases/2010/1000_DATA_BREACHES280510.ashx)

<sup>5</sup> *The Privacy Dividend: the business case for investing in proactive privacy protection*, ICO, Mar 2010

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/privacy\\_dividend.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf)

<sup>6</sup> Press Release, ICO, 8 Oct 2010

[http://www.ico.gov.uk/~media/documents/pressreleases/2010/Data\\_sharing\\_consultation\\_press\\_release\\_07102010.ashx](http://www.ico.gov.uk/~media/documents/pressreleases/2010/Data_sharing_consultation_press_release_07102010.ashx)

<sup>7</sup> "Uncertainty Reigns Supreme: What Impact Will a Coalition Government Have on Data Protection Law in the UK?" Privacy and Information Security Law Blog, Hunton & Williams LLP, 13 May 2010

<http://www.huntonprivacyblog.com/2010/05/articles/european-union-1/uncertainty-reigns-supreme-what-impact-will-a-coalition-government-have-on-data-protection-law-in-the-uk/>

<sup>8</sup> *A comprehensive approach to personal data protection in the European Union*, European Commission, 4 Nov 2010  
[www.huntonfiles.com/files/webupload/PrivacyLaw\\_com\\_2010\\_609\\_en/pdf](http://www.huntonfiles.com/files/webupload/PrivacyLaw_com_2010_609_en/pdf)

At the time of this study, the Financial Services Authority requires financial and public sector organisations to provide notification to customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts. Although the specific conditions for notification vary by industry, organisations may not be required to notify when:

- The breached data is protected by at least 128-bit encryption
- The breached data elements are not considered “protected”
- The breach was stopped before information was wrongfully acquired
- Other special circumstances (such as national security or law enforcement investigations) exist

Other Ponemon Institute research has revealed that more U.K. companies are focusing on preventing cyber attacks and data breaches overall and especially those that affect sensitive data. The *2010 Annual Study: U.K. Enterprise Encryption Trends* report found that for the first time, 100 percent of respondents said they considered loss or theft of confidential or sensitive data as either a severe or very severe threat to fulfilling their objectives. Another first was that nearly 9 out of 10 respondents (88 percent) said it was likely or very likely they would suffer cyber attacks in the next 12 to 24 months. Still another first was that even more respondents (92 percent) considered cyber attacks a severe or very severe threat to their ability to successfully carry out their missions.<sup>9</sup>

All these discussions about data breach prevention and notification are taking place while broader economic and technological trends are making data protection – and its absence during a breach – even more relevant. The stumbling global economy has forced many companies to reduce costs and improve efficiencies, leading to increased use of outsourcers, mobile technologies and application delivery models such as cloud computing. A major side effect of moving so much data from in-house IT networks is that organisations must take more responsibility for protecting their data wherever it is, especially when that data is in third-party hands.

The Ponemon Institute and Symantec Corporation are pleased to offer the fourth annual survey that quantifies the actual costs incurred by 38 organisations compelled to notify individuals of data privacy breaches. This study provides detailed information from responses to questions organisations face when responding to data breaches:

- What are the potential legal costs, as well as costs of lost customers and brand damage?
- What are industry-average costs resulting from a breach, including the detection, investigation, notification, and possible services offered to affected individuals?
- What are the key trends?
- What measures are taken following a breach that could have been implemented to avert it?

This report reveals how much companies pay for each kind of data breach studied, based both on primary breach causes and organisations’ common breach response. We also discuss any changes from previous benchmark studies and what those changes mean to organisations in an evolving data protection environment.

---

<sup>9</sup> *2010 Annual Study: U.K. Enterprise Encryption Trends*, The Ponemon Institute, Nov 2010

## Study Overview & Methodology

The Ponemon Institute's annual *Cost of a Data Breach* benchmark study, begun in 2005, examines the costs organisations incur when responding to data breach incidents resulting in the loss or theft of protected personal data.

This benchmark study examines data breach costs resulting in the loss or theft of protected personal data. As a benchmark study, *Cost of a Data Breach* differs greatly from the standard survey study, which typically requires hundreds of respondents for the findings to be statistically valid. Benchmark studies are valid because the sample is designed to represent the population studied. They intentionally limit the number of organisations participating and involve an entirely different data-gathering process.

In a survey, the unit of analysis is an individual. In this benchmark study, the unit of analysis is an organisation. Each company represents one case study. We conduct in-person and telephone interviews with many individuals in participating organisations. This process can take several months to complete. In sum, benchmark studies are far more difficult to execute and analyse than standard survey research.

The findings of this benchmark study pertain to the actual data breach experiences of 38 U.K. companies from 13 different industry sectors, all of which participated in the 2010 study. We believe the findings of this study are important because they can be generally applied to U.K. organisations that experience large data breaches (between 1,000 and 100,000 compromised records).

- Fieldwork for this research commenced in April 2010 and continued until the end of December 2010.
- Thirty-eight companies known to have experienced a breach sometime in 2010 agreed to participate in the study. The breaches involved the loss or theft of personal customer, consumer or student data and required notification according to U.K. laws. Study results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from actual incidents.
- All organisations voluntarily agreed to participate with the promise of complete confidentiality and anonymity.
- The reported number of individual records breached ranged from 6,900 records to 72,000 records from companies in 13 different industry sectors.
- The 2010 study shows that 34 percent of breaches occurred due to third parties, down 2 points from 2009. A third-party breach is defined as a case where a third party (such as professional services, outsourcers, vendors, business partners) possessed and was responsible for protecting the data. In comparison, an in-house breach is defined as a case where the organisation itself was responsible.

## Study Methodology

Our study addresses core process-related activities that drive a range of expenditures associated with companies' data breach detection and response. 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.
- Ex-post response: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimise potential harm. Redress activities also include ex-post 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 a breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our research shows that the negative publicity associated with a data breach incident can often damage companies' reputations and may lead to abnormal turnover, or churn, rates and a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we used a shadow costing method that relies on the 'lifetime value' of an average customer as defined for each participating organisation.

- Turnover intentions 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.
- Diminished new 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.

It is important to note, however, that the loss of non-customer data, such as employee records, may not impact an organisation's churn or turnover rates directly.

## Key Report Findings

### Overall Findings

**For the third year in a row, data breach costs have continued to rise:** Data breaches continue to cost organisations more every year. The average organisational cost of a data breach this year increased to £1.9 million, up 13 percent from 2009 and 10 percent from 2008. Data breaches in 2010 cost an average of £71 per compromised record, up £6 (9 percent) from 2009 and up £11 (18 percent) from 2008.

Data breaches are costing more at the top end of the scale and less at the bottom. The most expensive data breach included in this year's study cost a company £6.2 million to resolve, up £2.3 million (60 percent) from last year. The least expensive data breach was £336,000, down £29,000 (8 percent) from 2009.

Breach size this year ranged from 6,900 to 72,000 lost or stolen records. As in prior years, data breach cost appears to be directly proportional to the number of records compromised. Therefore, larger breaches continue to be a more serious cause for concern than smaller breaches.

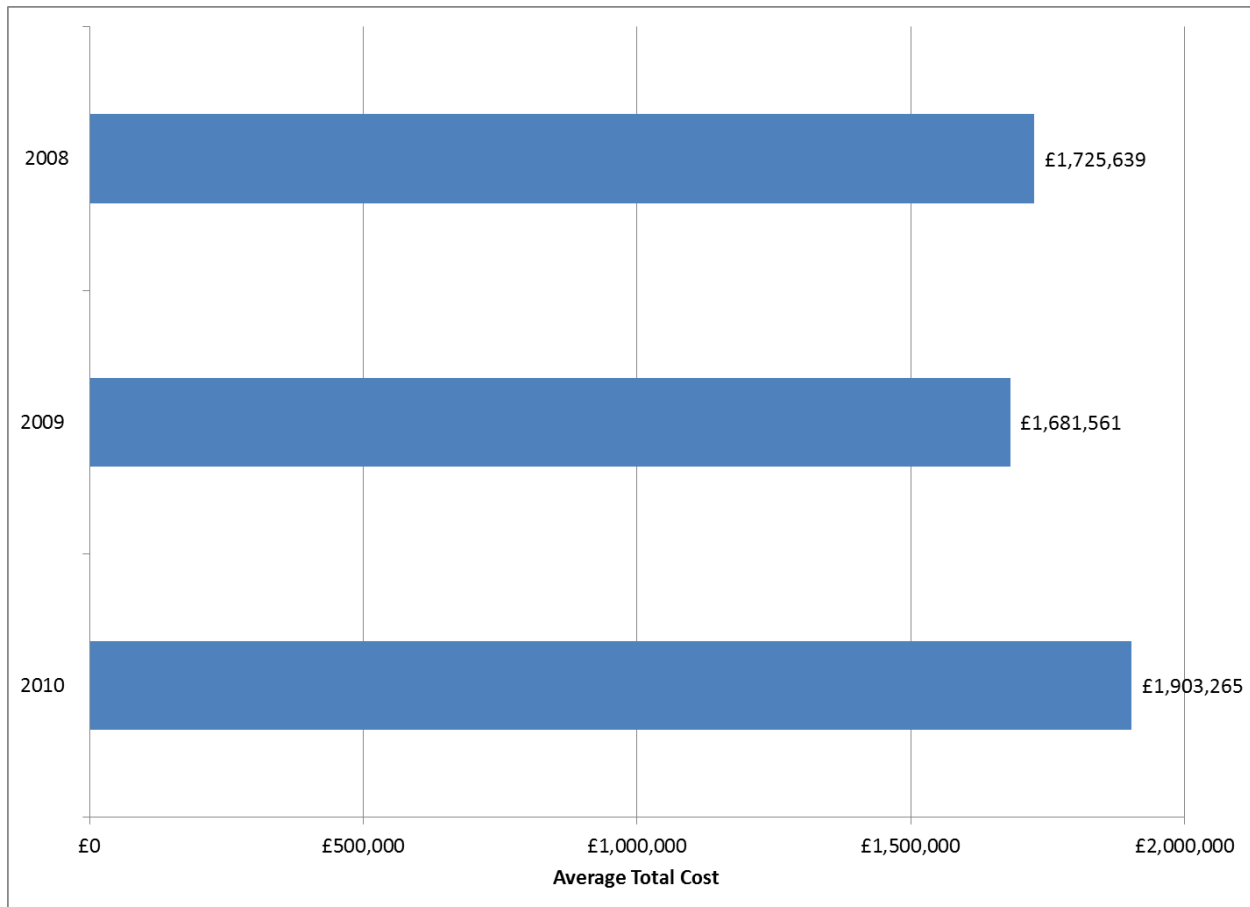


Figure 1: Average organisational cost of a data breach, 2008-10

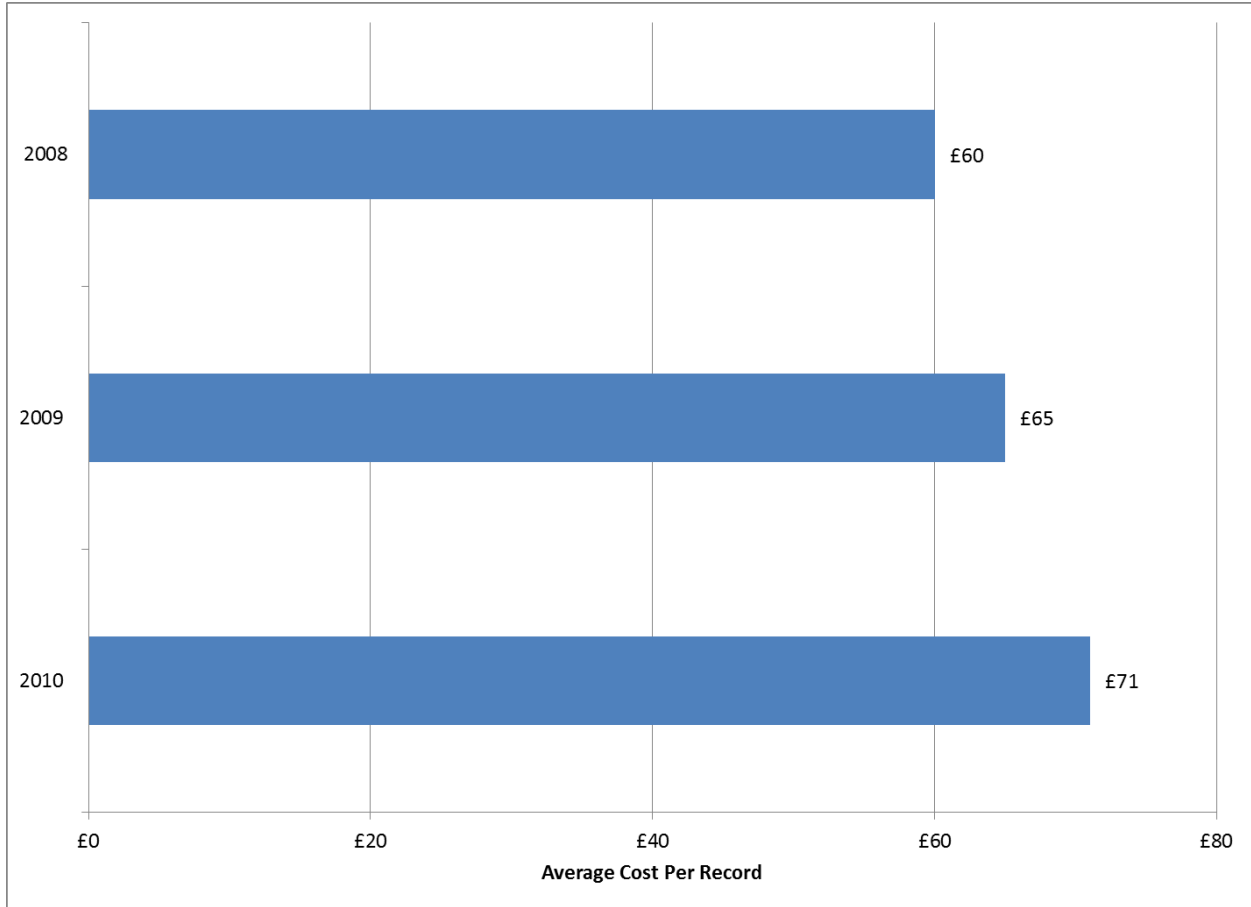


Figure 2: Average cost per record of a data breach, 2008-10

**Defending against malicious or criminal attacks and lack of internal preparedness and expertise appear to drive spending on data breach costs:** The highest costs in 2010 belonged to breach types that reflect failure to address the most prominent and dangerous data breach causes: malicious or criminal attacks and overall lack of preparedness that can lead companies to become breach victims. The opposite was also true: companies that avoided problems and had sufficient internal expertise and experience with data breaches fared better.

Costs rose the fastest for breaches involving proactive breach response and preparation and expertise that regulations demand for compliance (SES above the median, quick response and those not involving third-party mistakes, systems failures or lost or stolen devices). At the same time, costs were lowest and shrinking for breaches lacking both internal (systems failures) and external (third-party mistakes) preparation and expertise for compliance.

An interesting trend in this year's data is that eight out of ten breach attributes saw the cost difference narrow between the presence of the attribute and its absence. This means that organisations became more likely to incur certain response costs whether or not they prepared for a certain kind of breach. The exceptions were CISO leadership and systems failures, the presence of which saved companies £12 and £19 per record, respectively.

Whilst CISO leadership provides expertise that better enables cost-effective data breach response, the presence of system failures points to technical problems that can be relatively easy to mend (compared to preventing malicious or criminal attacks, etc.). The much higher cost of breaches not involving systems failures may indicate rising costs overall for breach response and especially those aimed at thwarting malicious or criminal attacks.

Breach Type	Cost 2010	Cost 2009	Rank 2010	Rank 2009
Malicious or criminal attack YES	£80	£76	1	2
System failure NO	£78	£64	2	10
SES above median NO	£77	£74	3	3
CISO leadership NO	£75	£67	4	8
First timer YES	£74	£68	5	7
Negligence NO	£74	£71	6	4
Third party mistake YES	£74	£81	7	1
Quick response YES	£72	£56	8	17
External consulting support NO	£72	£66	9	9
Lost or stolen device YES	£72	£69	10	5
Lost or stolen device NO	£71	£82	11	12
Quick response NO	£71	£69	12	6
Third party mistake NO	£70	£55	13	19
First timer NO	£70	£61	14	13
External consulting support YES	£69	£60	15	14
Malicious or criminal attack NO	£68	£60	16	15
SES above median YES	£67	£52	17	20
Negligence YES	£66	£56	18	18
CISO leadership YES	£63	£59	19	16
System failure YES	£59	£64	20	11

**Table 1: Breach costs and rankings by breach type, 2009-10**

**Note:** Data breach types are categorised by whether the breach involved a specific attribute (e.g. First timer YES) or all other breach types not involving that attribute (e.g. First timer NO).

In this year’s rankings, eight breach types rose, nine fell and three (negligent breaches and breaches not involving external consulting support or companies above the SES median) stayed the same. Of the 20 ranks, 18 had higher costs per record in 2010 than in 2009 and only two had lower costs – those involving third-party mistakes and systems failures.

Two of the three most expensive breach types remained the same from 2009 – malicious or criminal attacks rose one slot to first place, while breaches involving companies below the SES median stayed in third place. Interestingly, breaches not involving systems failures leaped eight slots to second place. Last year’s most expensive breach type, those involving third-party mistakes, fell six ranks to seventh place.

Looking at breach costs by rank alone and independent of breach type, the highest average per record costs companies experienced decreased by £1 (1 percent), from £81 to £80. The least expensive breaches rose £7 to £59. Interestingly, the most expensive ranks saw the smallest rises in cost, while the bottom 10 ranks saw increases between 11 and 20 percent. Of the 20 ranks, 19 saw increases, with only the top-ranked cost seeing a slight decline.

Relative Data Breach Type Rank	2010 Cost Per Record	2009 Cost Per Record
1	£80	£81
2	£78	£76
3	£77	£74
4	£75	£71
5	£74	£69
6	£74	£69
7	£74	£68
8	£72	£67
9	£72	£66
10	£72	£64
11	£71	£64
12	£71	£62
13	£70	£61
14	£70	£60
15	£69	£60
16	£68	£59
17	£67	£56
18	£66	£56
19	£63	£55
20	£59	£52

**Table 2: Breach cost comparison by relative ranking, 2009-10**

**Eighty percent of breach attributes are less frequent than last year:** Out of ten data breach attributes tracked in this study, only two – malicious or criminal attacks and systems failures – became more common between 2009 and 2010. All other causes and response attributes became less frequent. Overall, fewer organisations have above-average security postures and fewer are using either internal or external counsel to bolster their efforts.

Among data breach causes, systems failures became the most common at 37 percent, up 7 points, the biggest rise of any data breach attribute. It replaced negligence, which dropped 11 points, the most of any data breach attribute, to 34 percent. Lost or stolen devices and third-party mistakes each fell slightly. Malicious or criminal attacks rose 5 points to 29 percent.

Among data breach response behaviours, having an SES above the median remained the most common breach response attribute and most common attribute overall. It dropped 3 points to 45 percent. The number of first-time breach victims fell fast, by 10 points to 32 percent. Fewer companies responded quickly to breaches, down 4 points to 32 percent. Fewer companies are relying on internal or external expert counsel to handle breaches. CISO leadership fell 7 points to 32 percent, whilst external consulting support fell 10 points to 26 percent, becoming the least common attribute of all.

Data Breach Attribute	Frequency 2010	Frequency 2009
SES above median	42%	45%
System failure	37%	30%
Negligence	34%	45%
Third-party mistake	34%	36%
First timer	32%	42%
CISO leadership	32%	39%
Quick response	32%	36%
Lost or stolen device	29%	30%
Malicious or criminal attack	29%	24%
External consulting support	26%	36%

**Table 3: Frequency of data breach attributes, 2009-10**

An interesting trend in this year's data was how often the lack of IT security acumen led to higher breach costs. Fifty-eight percent of respondents had an SES below the median and 68 percent lacked CISO leadership, meaning well more than half of companies could unnecessarily pay some of the highest breach costs.

A related observation is that notably fewer companies are putting CISOs in charge of data breach response, despite evidence that such leadership provides increasingly impressive cost savings. Even more respondents cut back on external consulting support, which provided relatively minor savings. These figures may indicate that organisations' growing experience with data breaches may lead them to believe they don't need specialised help for breach response. We will closely watch this issue in future reports.

Systems failures became a much bigger priority this year and had the most distinctive results. It was one of only two types that were cheaper than last year (the other being the presence of third-party mistakes). Along with CISO leadership, it was part of another unique pair that saw the cost difference widen between breaches involving it and those that did not. The results are all the more noticeable because last year breaches with systems failures and those without them cost the same, £64.

The systems failures findings are even more interesting when taken in context of the frequency of other breach types. More companies have data breach experience and fewer reported breaches due to negligence, lost or stolen devices and third-party mistakes. Taken together, these figures may indicate that fear of data breaches and cyber attacks may be driving more companies to devote much more effort to IT security. Companies' increasing focus on data breach mitigation and regulatory compliance may be encouraging them to discover more systems failures behind data breaches – especially when breach response costs from systems failures are the lowest in this study and are getting cheaper. We will closely watch this issue in future reports as well.

These figures correspond with findings from the *2010 Annual Study: U.K. Enterprise Encryption Trends* report, also conducted by the Ponemon Institute and sponsored by Symantec.<sup>10</sup> Namely, the report found that for the first time, 100 percent of respondents said they considered loss or theft of confidential or sensitive data as a severe threat. Other firsts included that nearly 9 out of 10 respondents (88 percent) expecting cyber attacks in the next 12 to 24 months and even more (92 percent) considered cyber attacks a severe threat.

The *2010 Enterprise Encryption Trends* report also found that 71 percent of organisations surveyed had had at least one data breach, the same as in 2009. A worrying trend, however, was that fewer respondents are experiencing no data breaches. These figures reinforce the rising recognition that malicious attackers can get at critical data, particularly unprotected data. That fear made other data protection issues lower priorities.

Moreover, the *2010 Enterprise Encryption Trends* report found that data breach mitigation and complying with data protection and privacy regulations are rapidly becoming the primary reasons organisations use encryption (and, by extension, other data protection technologies). For the first time, 40 percent of respondents stated that data breach mitigation was their main reason. That figure is up 30 points from 2007. Regulatory compliance saw nearly as strong growth: 39 percent in 2010, up 22 percent since 2007. These figures illustrate a growing acceptance that data breaches are a worsening threat and regulations are important means to combat them.

Key regulations driving encryption use remained the same from 2009 and 2010, including Payment Card Industry (PCI) requirements and the European Union Privacy Directive. PCI requirements were the most influential at 55 percent, up 5 points from 2009. The largest gain from 2009 by far was for the U.K. Information Commissioner's Office (ICO) requirements, up 15 points from 24 percent to 39 percent.

---

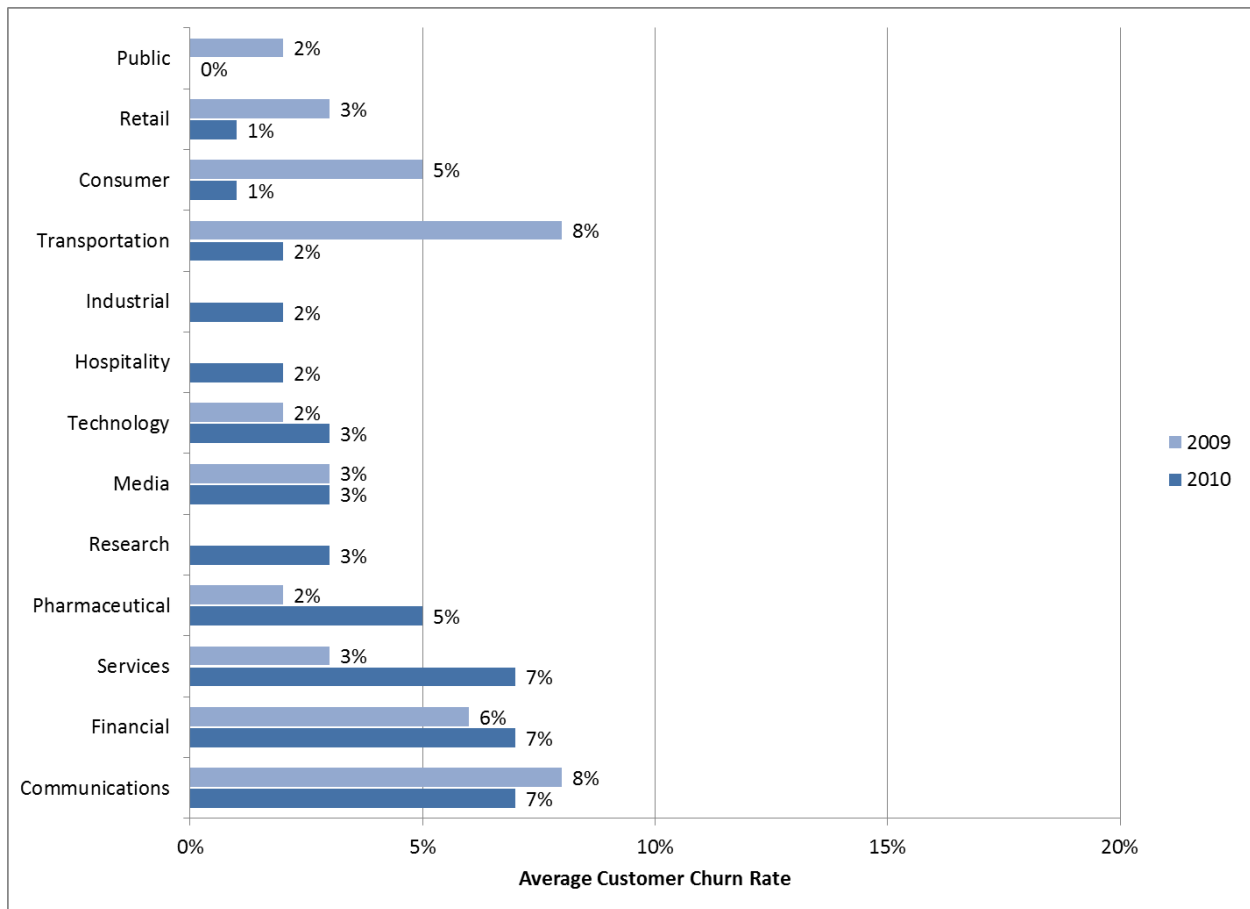
<sup>10</sup> *2010 Annual Study: U.K. Enterprise Encryption Trends*, The Ponemon Institute, Nov 2010

**Customer turnover in direct response to breaches remains the main driver of data breach costs:** For the second straight year, abnormal churn or turnover of customers after data breaches appears to be the dominant factor in data breach cost. Regulatory compliance contributes to lower churn rates by boosting customer confidence in organisations' IT security practices.

The sectors with the highest 2010 churn rate were communications, financial and services, all at 7 percent. The industries with the lowest abnormal churn rates were transportation (2 percent), consumer and retail (each at 1 percent) and public sector (less than 1 percent).

Average abnormal churn rates across all 38 incidents dropped a point to 3 percent. Of the ten industry sectors represented in both the 2009 and 2010 reports, abnormal churn rates of five decreased, one stayed the same and four increased.

Sectors with the highest 2010 average per-record costs were communications (£102), financial (£94) and pharmaceutical (£90). Those with the lowest costs were retail (£45), public sector (£50) and consumer (£51). Of the ten industry sectors represented in both the 2009 and 2010 reports, six paid more in 2010 and four paid less.



**Figure 3: Abnormal churn rates following data breaches by industry classification, 2009-10**

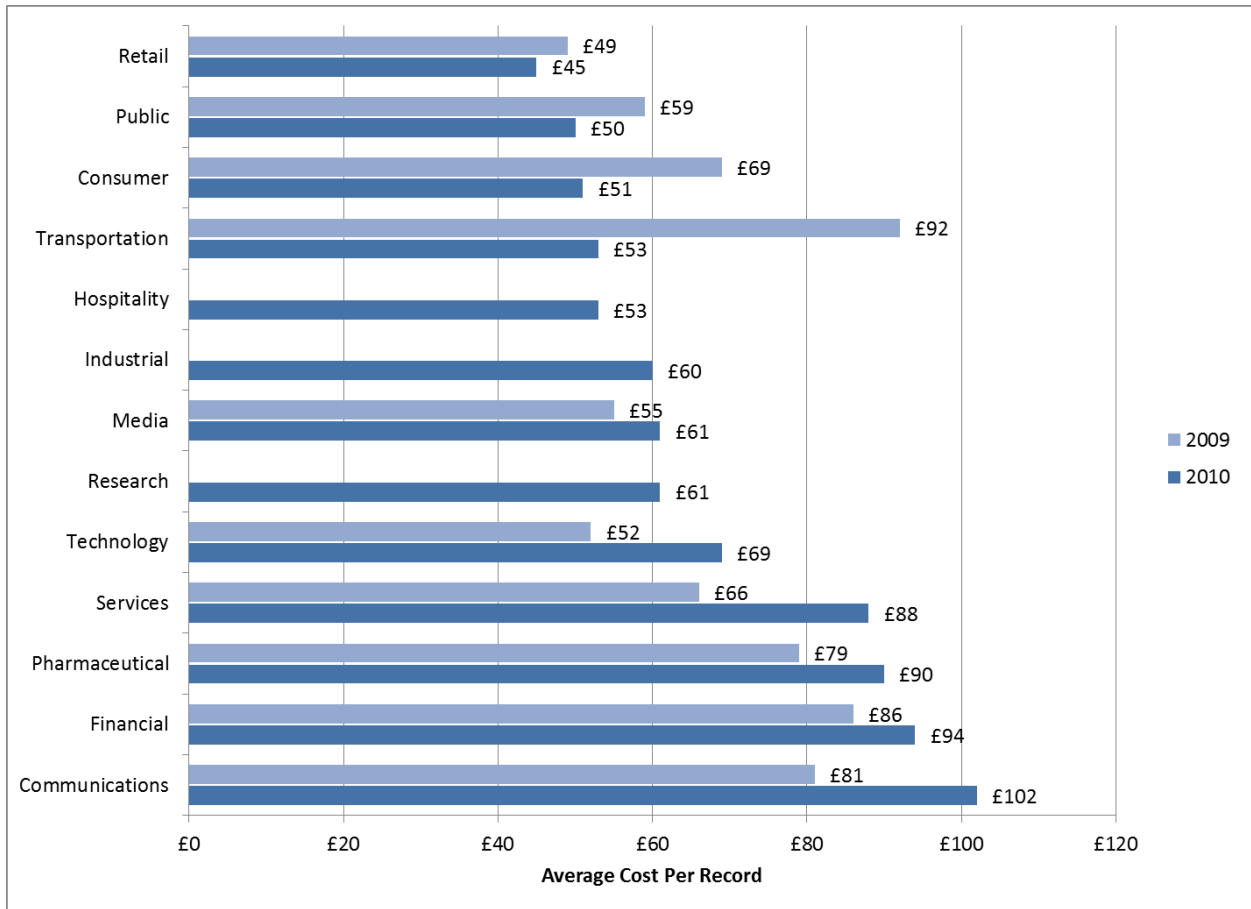


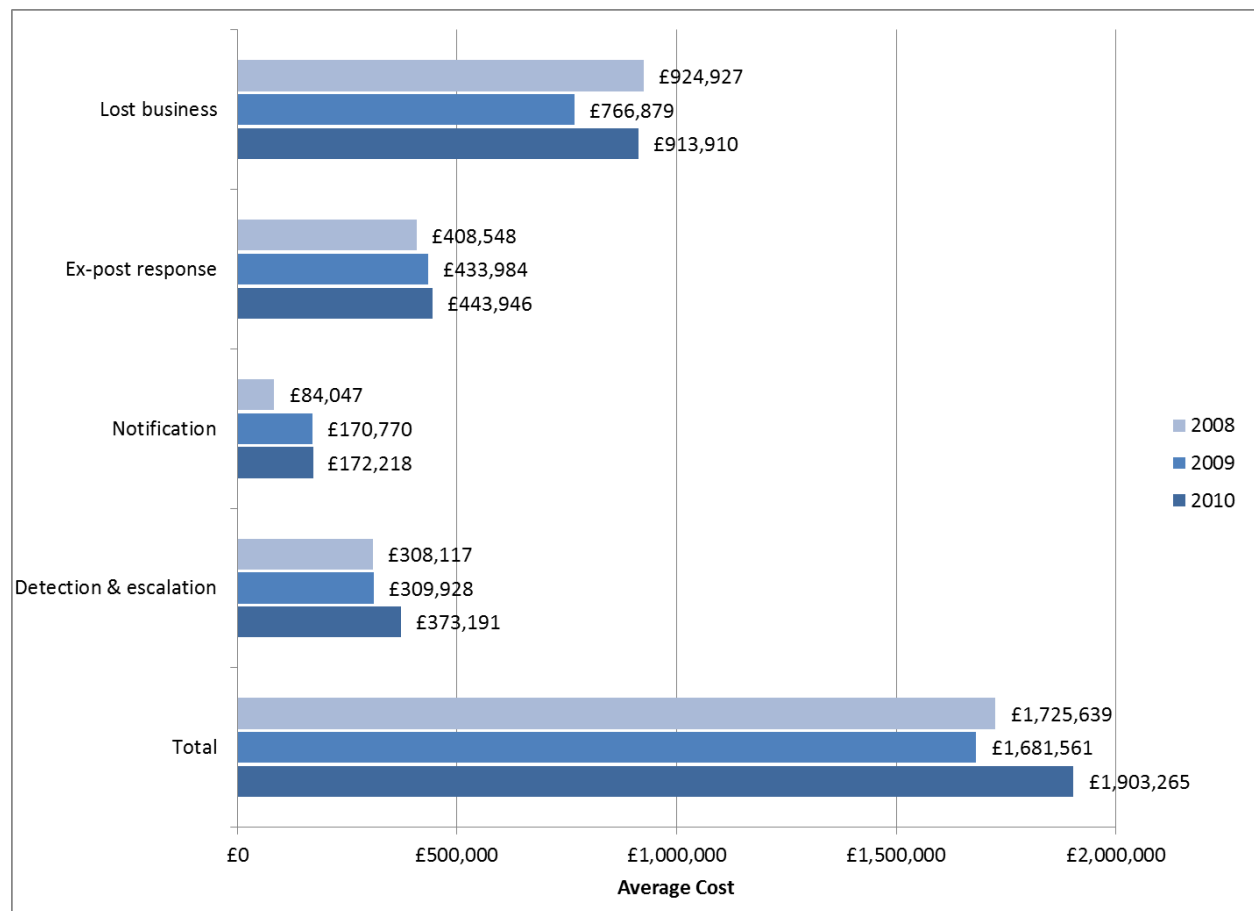
Figure 4: Cost per record of data breaches by industry classification, 2009-10

**Lost business and ex-post response are becoming the main components of data breach costs:** Recovering customers, profits and business opportunities after data breaches posed the greatest cost hurdles for companies in 2010 – even more than data breach response itself. Lost business and detection and escalation costs rose the most, while ex-post response stayed level and notification costs fell a little.

Lost business accounted for 48 percent of overall data breach costs, up 2 points from 2009. Ex-post response comprised 23 percent, down 3 points. Detection and escalation rose 2 points to 20 percent. Finally, notification costs remained by far the smallest cost component. It accounted for 9 percent of 2010 costs, down 1 percent from 2009.

Lost business further solidified its title as the most expensive cost activity for organisations and represented the majority of the growth in data breach costs in 2010. Companies in 2010 on average paid £914,000 per breach, up £144,000 (19 percent) from 2009. Lost business costs accounted for £34 (48 percent) of total per-record costs this year. That amount is £5 (17 percent) more than in 2009, when lost business costs were £29 (45 percent) of the total. Per-record costs rose the most and fastest of any activity category.

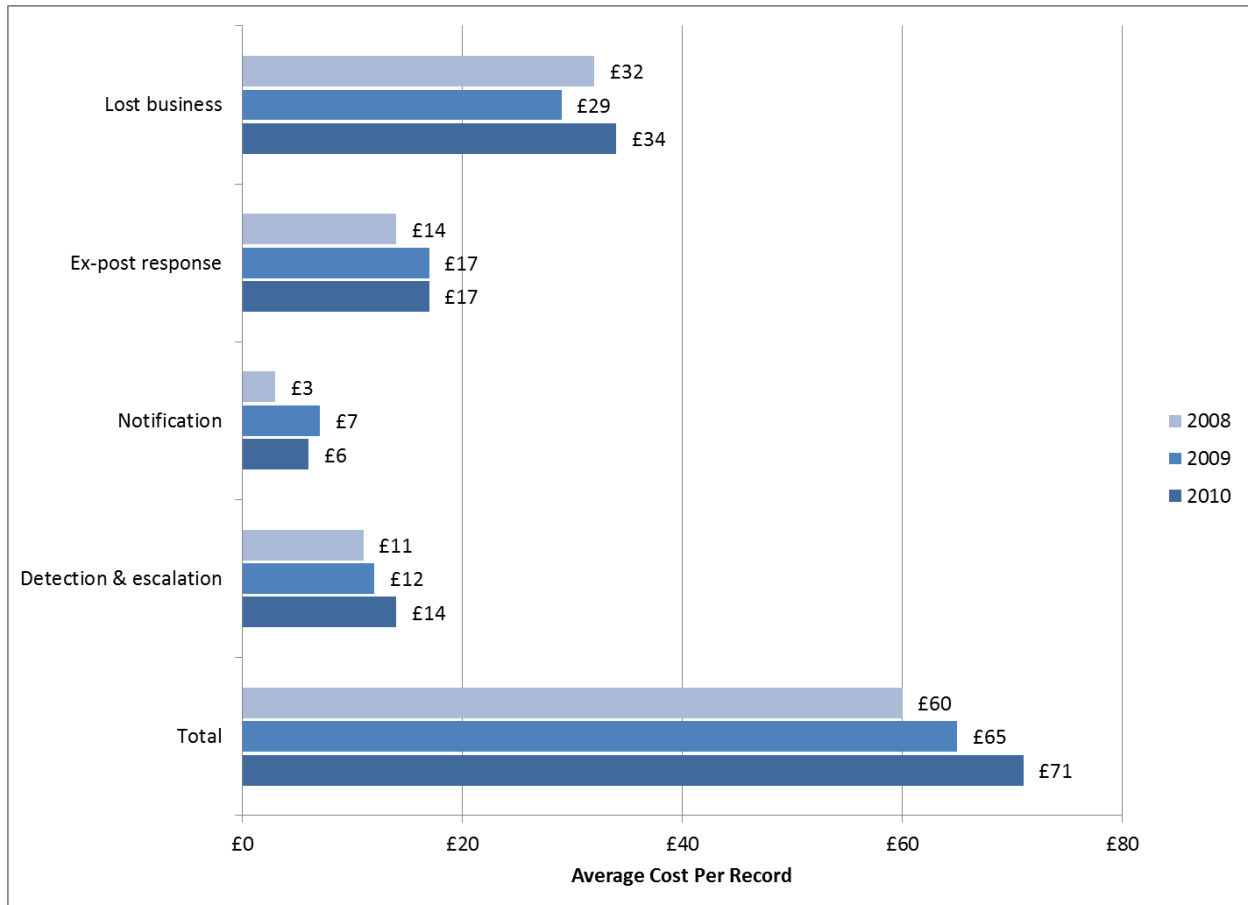
High costs for lost business mean consumers are concerned about how well organisations safeguard personal data. They also mean that companies know the damage breaches can do and are willing to pay more to fix that damage.



**Figure 5: Average data breach cost by cost activity, 2008-10**

Ex-post response remained in second place but changed little from last year. Companies in 2010 on average paid £444,000 per breach, up £14,000 (3 percent) from 2009. Ex-post response accounted for £17 of total per-record costs, the same amount as last year but accounting for less of the total – down 2 points to 24 percent.

For detection and escalation, companies on average paid £373,000, up £63,000 (20 percent). Detection and escalation costs accounted for £14 (20 percent) of total per-record costs this year. That amount is £2 (17 percent) more than in 2009, when detection and escalation costs were £12 (27 percent) of the total. This greatly increased effort to find the sources of breaches and start the response process may indicate greater attention to regulatory compliance activities.



**Figure 6: Average cost per record by cost activity, 2008-10**

Notification costs continued to be the least significant portion of data breach costs. Even so, organisations devoted slightly fewer resources to notifying data breach victims. Companies on average paid £172,000 per breach for notification costs, up only £2,200 (1 percent) from 2009. Notification costs accounted for £6 (8 percent) of total per-record costs this year. That amount is £1 (14 percent) less than in 2009, when notification costs were £7 (11 percent) of the total.

Taken together, these figures appear to correspond with findings from the *2010 Enterprise Encryption Trends* report, which found that data breach mitigation and complying with data protection and privacy regulations are rapidly becoming the primary reasons organisations use encryption (and, by extension, other data protection technologies). When considered along with the big drop in first-time breach victims this year, the figures for ex-post response and notification may indicate experience with data breaches may help keep costs down.

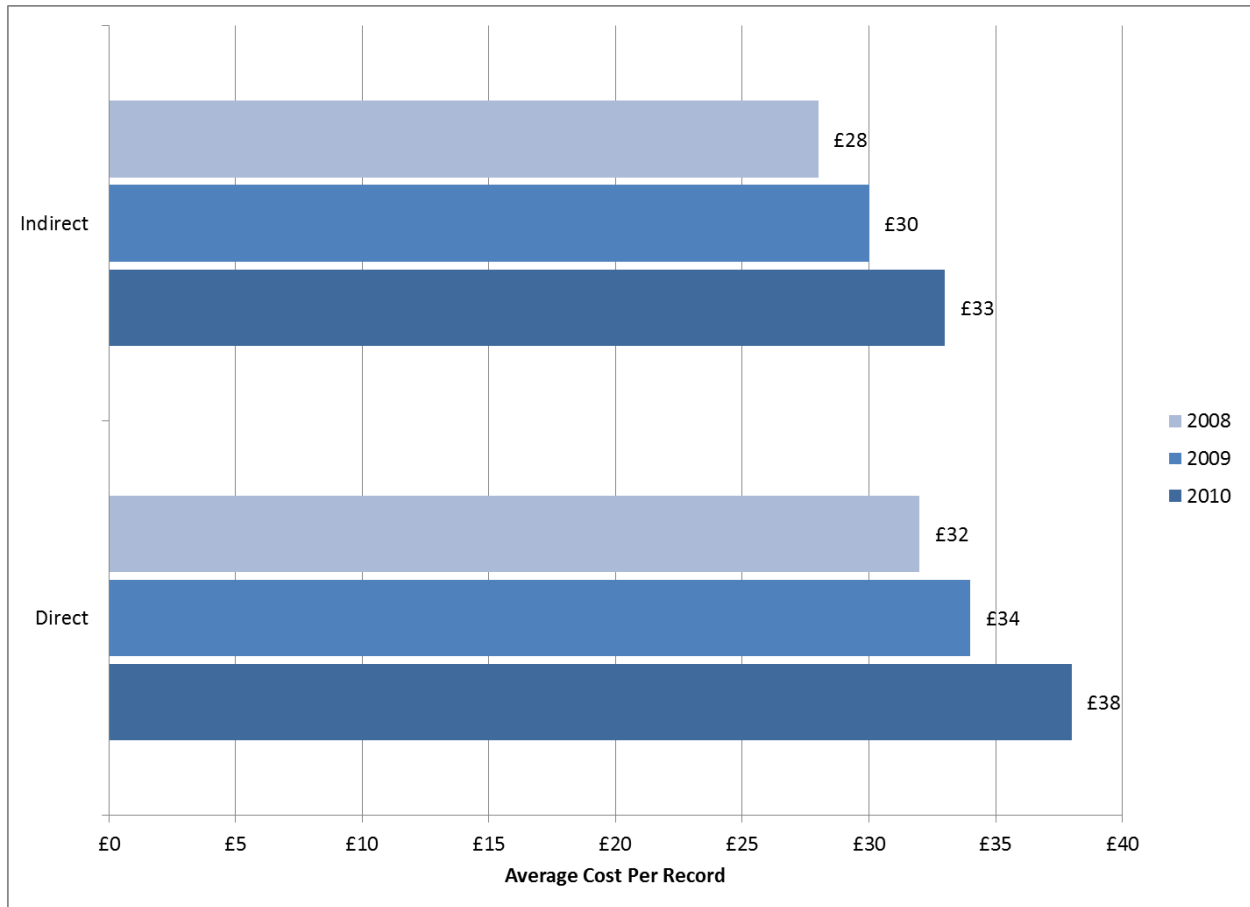
Additionally, the relatively stable costs for ex-post response and notification may also indicate that companies generally have high confidence in their capabilities. The *2010 Enterprise Encryption Trends* report found that in general, the security posture of companies is improving. Overall SES scores overall have consistently risen between 15 and 31 percent a year over the past three years. Preventing or curtailing major data breaches involving sensitive or confidential data saw much larger improvements, up more than 120 percent two of the past three years. These figures indicate that organisations are becoming more confident in discovering, mitigating and stopping breaches.

**Both direct costs and indirect costs continue to rise:** Direct costs represent measurable accounting line items organisations have for specific data breach response activities. Indirect costs include lost customer business due to churn and customer acquisition costs. This year's figures indicate that companies are continuing to spend more on both kinds of costs.

In 2010, direct costs accounted on average for £38 (54 percent) of the total average cost per record, up £4 (12 percent) than in 2009, when direct costs were £34 (52 percent) of the total. Indirect costs in 2010 were £33 (46 percent) of the total, up £3 (10 percent) from 2009. Direct breach cost activities were £5 (13 percent) more this year than indirect costs, up £1 (25 percent) from last year. In 2009, direct costs were £4 (12 percent) more.

Among specific cost activities, organisations continued to spend the most on investigations and forensics (12 percent, almost unchanged since 2008). Lost customer business due to churn formed an even greater proportion of total costs, up 1 point to 42 percent this year.

Similar to the previous finding, these figures may reflect how data breach mitigation and regulatory compliance affect data breach costs.



**Figure 7: Cost per record of direct and indirect costs, 2008-10**

Cost Activity	2010	2009	2008
Lost customer business due to churn	42%	41%	45%
Investigations & forensics	12%	13%	12%
Outbound contact costs	11%	10%	9%
Audit and consulting services	8%	9%	10%
Inbound contact costs	8%	7%	7%
Customer acquisition costs	7%	8%	9%
Public relations/communications	6%	5%	3%
Free or discounted services	3%	2%	2%
Legal services - compliance	2%	3%	2%
Legal services - defense	1%	2%	3%
Credit monitoring services	0%	0%	1%
<b>Total</b>	<b>100%</b>	<b>102%</b>	<b>103%</b>

**Table 4: Percent of breach costs by specific cost activity, 2008-10**

Note: Some totals do not add up to 100 percent because of rounding.

**Manual, policy and training-oriented options remained the most popular post-breach preventive and remediation measures:** After data breaches, organisations often consider a number of possible remedies to protect confidential and sensitive data as part of an enterprise data protection strategy. Most U.K. organisations have traditionally preferred manual- and policy-based solutions over technological solutions as post-breach remediation measures.

In 2010, 43 percent of respondents implemented additional manual procedures and controls and 40 percent relied upon training and awareness programs. Frequency of implementation of all listed measures stayed about the same except strengthening perimeter controls, which jumped 8 points from 2009 to 32 percent. Since 2008, manual procedures and controls have fallen 6 points, data loss prevention (DLP) and security event management solutions have each risen 8 points and endpoint security solutions (including laptop anti-theft) have risen 11 percent.

Even though organisations still far prefer using traditional approaches, this year's figures may indicate companies are starting to see more value in technology that can help prevent and mitigate data breaches. A combination of IT security and economic worries may have helped drive companies to embrace their faith in technology in general, but especially to known and trusted solutions such as perimeter controls. Additionally, the *2010 Enterprise Encryption Trends* study also found that more organisations see encryption – and, by extension, data protection – as a tool to protect customer confidence in organisations' privacy or data security commitments.

These figures correspond with similar questions about technology use in the *2010 Enterprise Encryption Trends* report. That study found that perimeter controls were the most popular security technology that received specific budget allocations. A notable increase in respondents said mobile device encryption was very important or important – 64 percent, up 13 points from 2009. That figure supports this study's finding that endpoint security solutions (including laptop anti-theft) have seen strong growth. It also reinforces the overall IT security trend of malicious attackers going after vulnerable data on mobile devices.

Preventive Measure	2010	2009	2008
Additional manual procedures and controls	43%	41%	49%
Training and awareness programs	40%	38%	42%
Expanded use of encryption	33%	33%	31%
Strengthening of perimeter controls	32%	24%	29%
Data loss prevention (DLP) solutions	29%	31%	21%
Identity and access management solutions	26%	25%	29%
Endpoint security solutions (including laptop anti-theft)	25%	27%	14%
Security certification or audit	21%	19%	13%
Security event management systems	16%	15%	8%

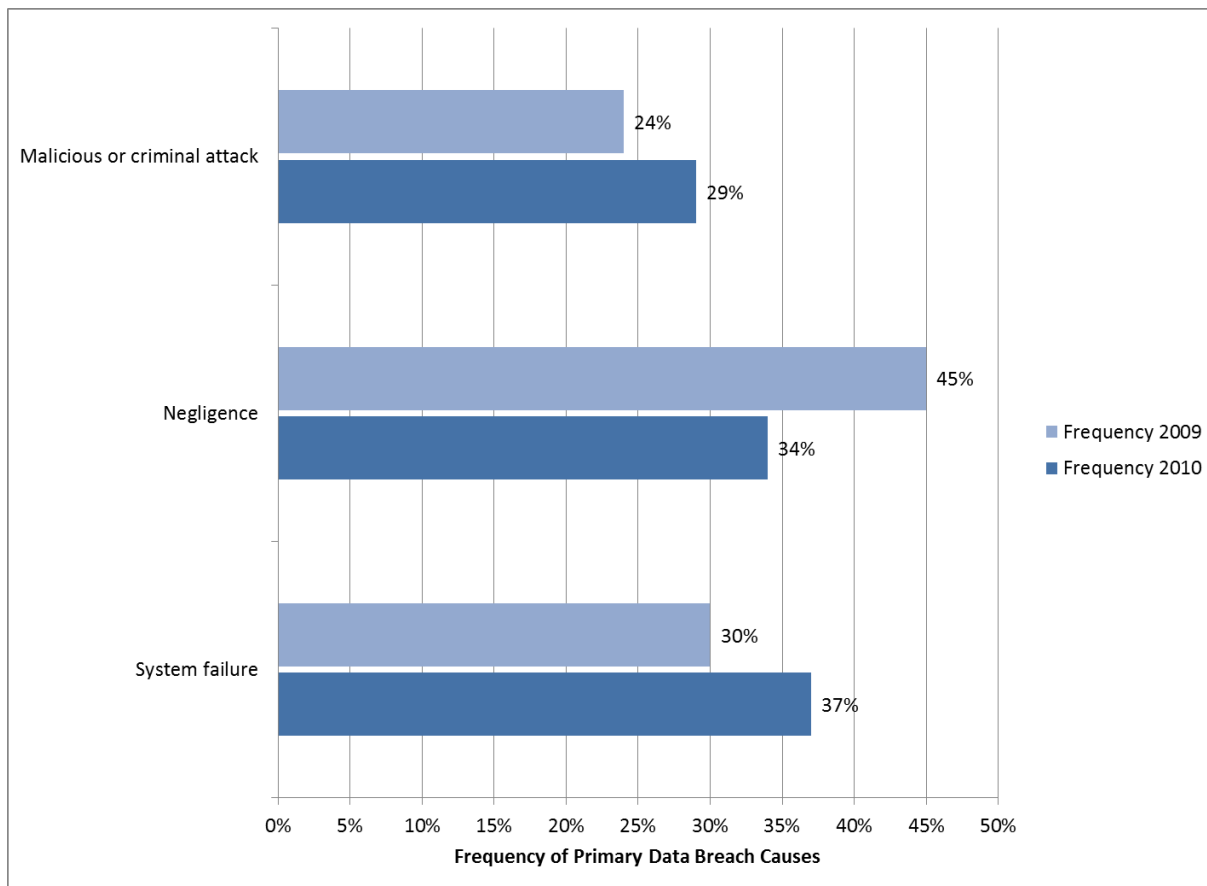
**Table 5: Preventive measures implemented as a result of a data breach, 2008-10**

## Findings by Breach Type – Cause

**Malicious or criminal attacks remain the most expensive breach cause and, for the first time, are the most expensive breach type overall:** Of the three overarching breach categories – malicious or criminal attacks, negligence and systems failures<sup>11</sup> -- malicious or criminal attacks accounted for 29 percent in 2010. That number is up 5 points from 2009.

Meanwhile, the number of breaches attributed to negligence fell 11 points to 34 percent. More than one-third of breaches (37 percent) were due to systems failures, up 7 points from 2009.

The growth in malicious or criminal attacks is consistent with an escalating cyber security threat environment. Growing complexity of data systems and strictness of compliance requirements may pose additional challenges to preventing and mitigating internal breaches from systems failures. The sharp drop in breaches due to negligence may stem from increased awareness of the dangers data breaches pose and more conscientious efforts to prevent them.



**Figure 8: Frequency of primary data breach causes, 2009-10**

Our research shows data breaches involving malicious or criminal acts continued to be much more expensive than incidents resulting from either negligence or systems failures – and that cost is ticking upward. Accordingly, in 2010 the cost per compromised record of a data breach involving a malicious or criminal act averaged £80, up £4 (5 percent) from 2009. In contrast, breaches not involving malicious actors cost 15 percent less and averaged only £68

<sup>11</sup> Third-party mistakes and the loss or theft of data bearing devices are also main causes of data breaches. For the purposes of this particular survey question, the reasons they occur fall under these three categories.

per record, up £8 (13 percent) from last year. Breaches involving malicious or criminal attacks cost £12 (18 percent) more this year than internal breaches, down £4 (25 percent) from last year. In 2009, malicious breaches cost £16 (27 percent) more.

Malicious breaches ranked first in costliness in this year's study, up one slot from last year. Non-malicious breaches ranked 16<sup>th</sup>, also up one slot.

At the same time, breach costs for negligence rose sharply as well. Breaches from negligence in 2010 averaged £66 per record, up £10 (18 percent) from 2009. Breaches not involving negligence cost £74 per record, up £3 (4 percent) from last year. Negligent breaches cost £8 (11 percent) less this year than non-negligent breaches, £7 (47 percent) less than last year, when negligent breaches cost £15 (21 percent) more.

Breaches from systems failures averaged £59, down £5 (8 percent). Breaches not involving systems failures cost £78, up £14 (22 percent). Breaches without systems failures cost £19 (32 percent) more this year than those with them, £19 (190 percent) more than last year. In 2009, breaches both from systems failures and not from systems failures averaged £64. More than any other breach type this year, breaches from system failures had unique characteristics (see pages 14-17 above).

Negligent breaches ranked 18<sup>th</sup> in cost, the same as in 2009. Non-negligent breaches ranked sixth, down two slots. Breaches from systems failures ranked 20<sup>th</sup>, down nine slots. Breaches not involving systems failures ranked second, rising eight slots.

Interestingly, for both systems failures and negligence, breaches not involving them once again cost more than those that did. This similarity may indicate that both companies and their customers take malicious breaches seriously and expect companies to spend appropriately to respond to them. Additionally, companies may be changing how they respond to breaches by looking at the type of breach they're experiencing to determine what actions to take.

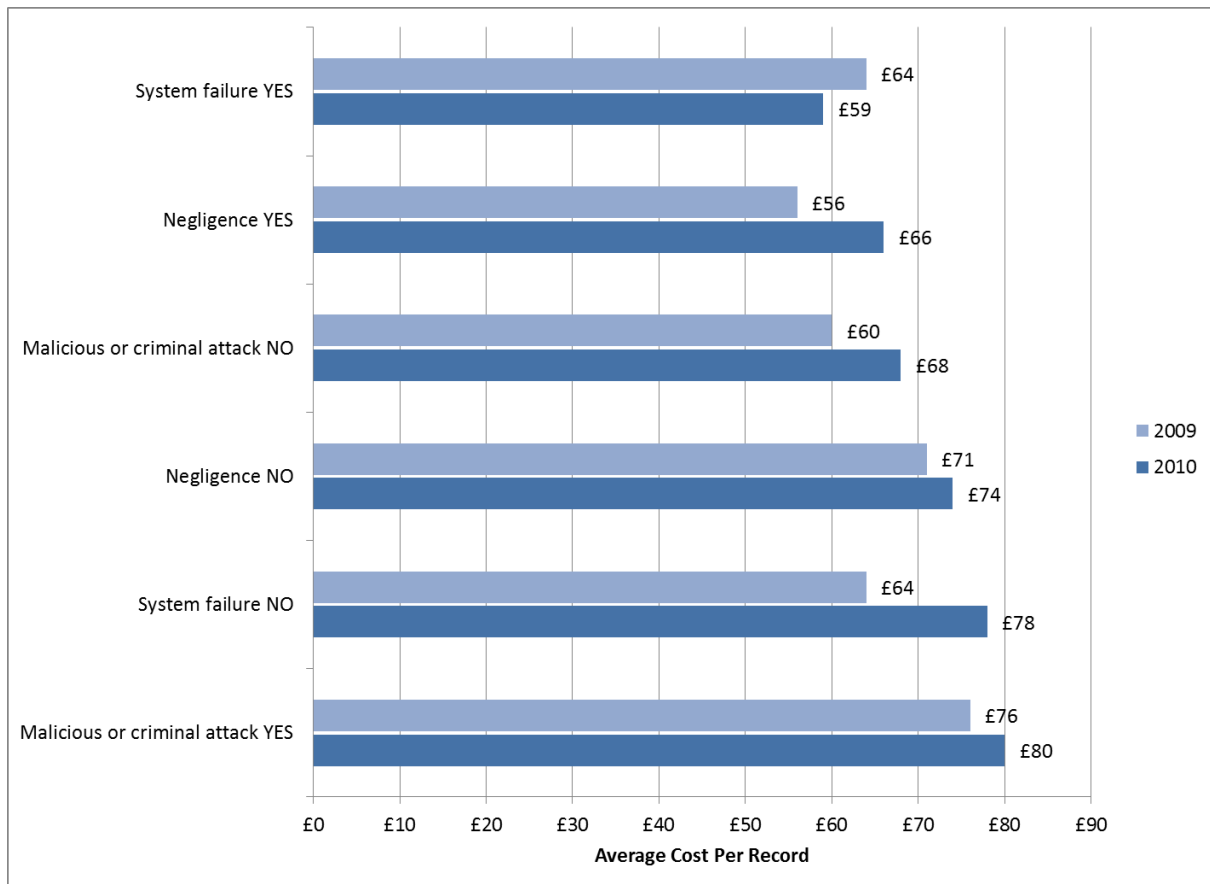


Figure 9: Cost per record of data breaches by primary cause, 2009-10

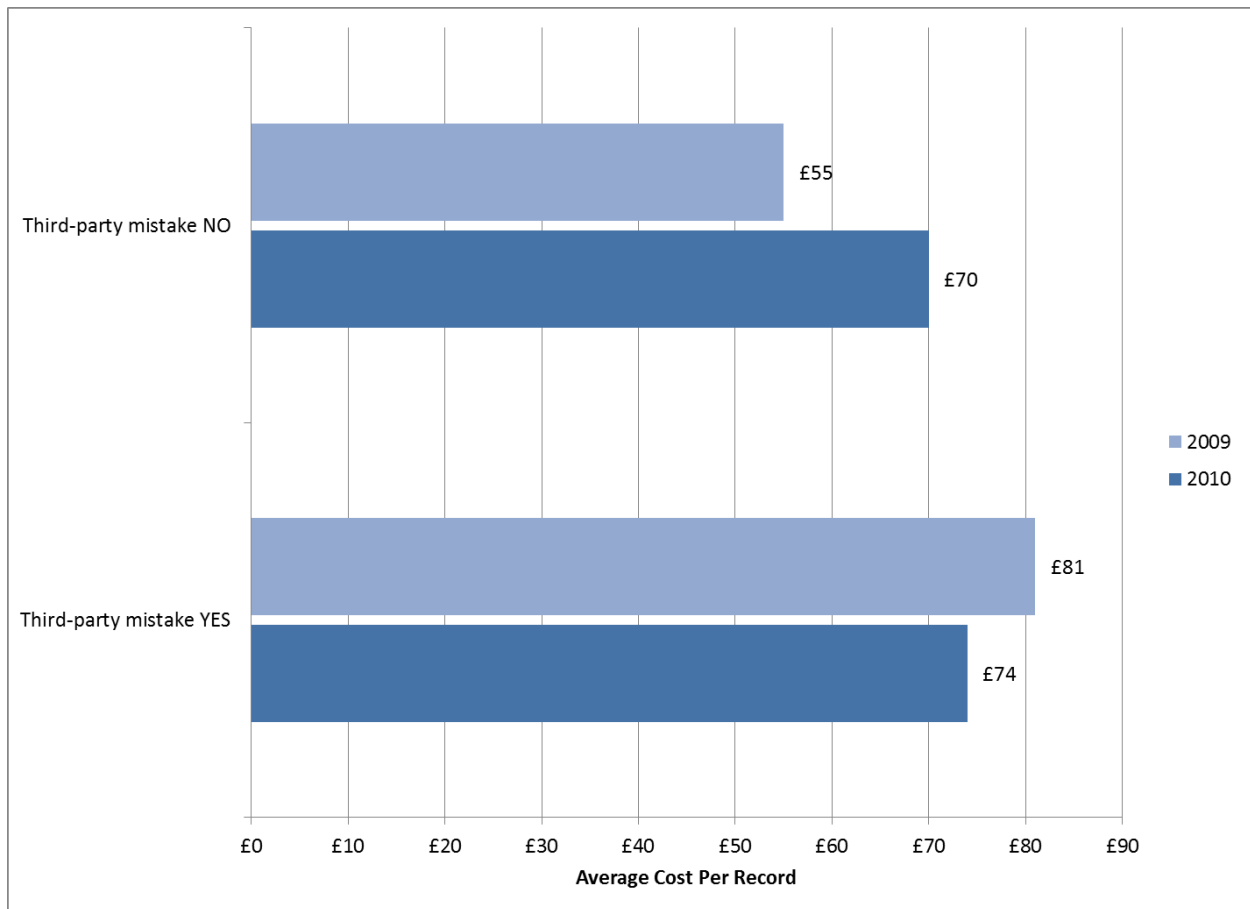
**Breaches involving third-party mistakes by outsourcers are still a major worry and expense:** Third-party outsourcers or consultants often analyse or process large volumes of customer-related data. Data breaches can involve outsourced data, especially when the third party is offshore. Third-party mistakes decreased marginally in 2010 to 34 percent, down 2 points.

The cost of such breaches fell as well, down £7 (9 percent) to £74 per record. The cost of breaches not involving third parties, however, shot up £15 (27 percent) to £70. Breaches involving third parties cost £4 (6 percent) more this year than internal breaches, down £22 (85 percent) from 2009. In 2009, third-party breaches cost £26 (47 percent) more. Third-party mistakes were one of only two of the 20 data breach types to see lower costs this year.

Breaches from third-party mistakes ranked seventh in costliness this year, down six slots from first place last year. Breaches not caused by third-party mistakes ranked 13<sup>th</sup>, up six slots from last year.

The marked drops in both cost and rank of third-party breaches may indicate that whilst the security of outsourced data remains important, those breaches became a much lower priority in 2010 compared to other data breach sources. Companies may be focusing more on internal breaches, as those costs rose quickly.

Organisations may also feel confident enough in dealing with third-party breaches to handle them cost-effectively and put other breach concerns first. The *2010 Enterprise Encryption Trends* report found that 55 percent of organisations felt confident or very confident in their ability to protect outsourced data. At the same time, their confidence in doing those tasks grew spectacularly from 2007 to 2010. Widespread concerns about the security of cloud computing could help explain this giant leap in confidence, as companies successfully race to safeguard data shared with third parties.



**Figure 10: Cost per record of breaches due to third-party mistakes, 2009-10**

**Breaches involving data on lost or stolen devices are expensive and may reflect anxiety about insecure use of mobile technologies:** The frequency of data breaches concerning mobile devices holding sensitive data stayed roughly the same in 2010, falling 1 point to 29 percent.

Per-record costs rose £3 (4 percent) to £72 per record for such breaches; breaches not involving lost or stolen devices increased even more, up £9 (15 percent) to £71. Breaches involving lost or stolen devices cost £1 (1 percent) more this year than those that did not, £6 (86 percent) less than last year. In 2009, loss- and theft-related breaches cost £7 (11 percent) more.

Breaches involving lost or stolen devices ranked tenth for costliness, up five slots from 2009. Breaches not involving such devices ranked 11<sup>th</sup>, up one slot.

Our research suggests that device-oriented breaches consistently cost more than many other breach types. That is not the case this year, however, as this study found the cost to be a hair more than average. The relative stability of both the frequency and severity of device-oriented breaches this year may indicate that organisations feel confident in their ability to identify and mitigate such risks.

The *2010 Enterprise Encryption Trends* report found that organisations feared the insecure use of mobile technologies as much or more than direct cyber attacks against their IT systems. The likelihood of insecure mobile devices connecting to company networks or enterprise systems rose 9 points to 84 percent, while the severity of such incidents leaped up 11 points to 88 percent. The survey found a notable increase in respondents saying mobile device encryption was very important or important – 64 percent, up 13 points from 2009. These and other figures reinforce the rising recognition that malicious attackers can get at critical data. They also reflect cyber attackers’ ongoing shift to target unprotected data, as well as mobile users’ growing need for better tools to secure data.

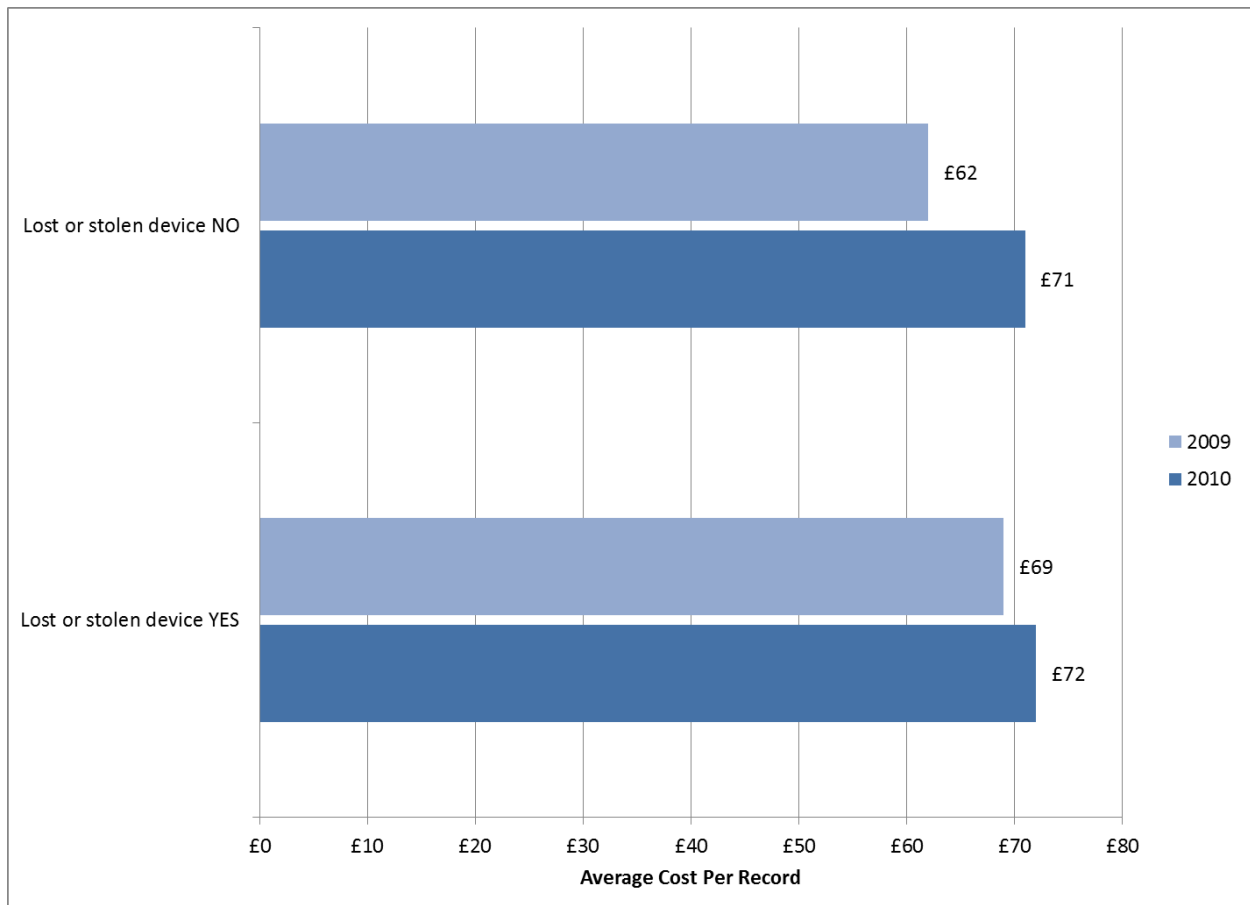


Figure 11: Cost per record of data breaches involving lost or stolen devices, 2009-10

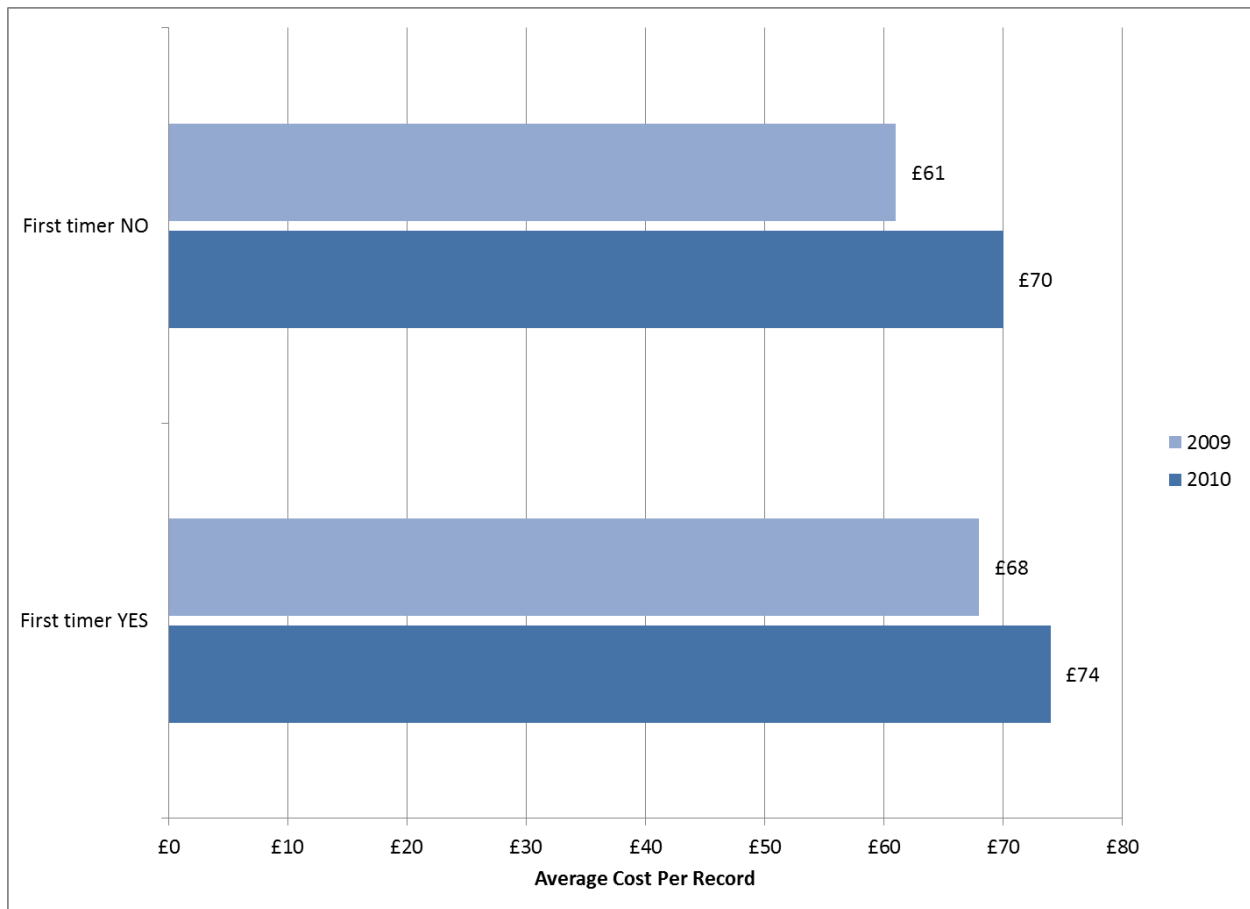
## Findings by Breach Type – Response

**First-time breaches are one of the most expensive breach types but are becoming much less common:** A third (32 percent) of respondents in 2010 faced their first data breaches involving the loss or theft of more than 1,000 records containing personal information. That figure has declined 10 points from 2009, one of the biggest drops of any breach type.

This year, the cost per compromised record of an organisation’s first data breach averaged £74 (up £6 or 9 percent). Subsequent breaches averaged £70 (up £9 or 15 percent). First-time breaches cost £4 (6 percent) more this year than subsequent breaches, £3 (43 percent) less than last year. In 2009, first timers paid £7 (11 percent) more.

Breaches involving first timers ranked fifth in costliness, up two slots from last year. Breaches involving organisations that have already experienced breaches ranked 14th, down a slot from last year.

These findings may indicate that the pool of first timers is shrinking due to both an increase in compliance activities to prevent breaches and a larger pool of prior breach victims over time. As stated above, attacks are becoming more insidious and damaging, which requires greater resources to combat. Fortunately, experience with data breaches may help companies become more efficient at managing costs over time.



**Figure 12: Cost per record of first time and subsequent data breaches, 2009-10**

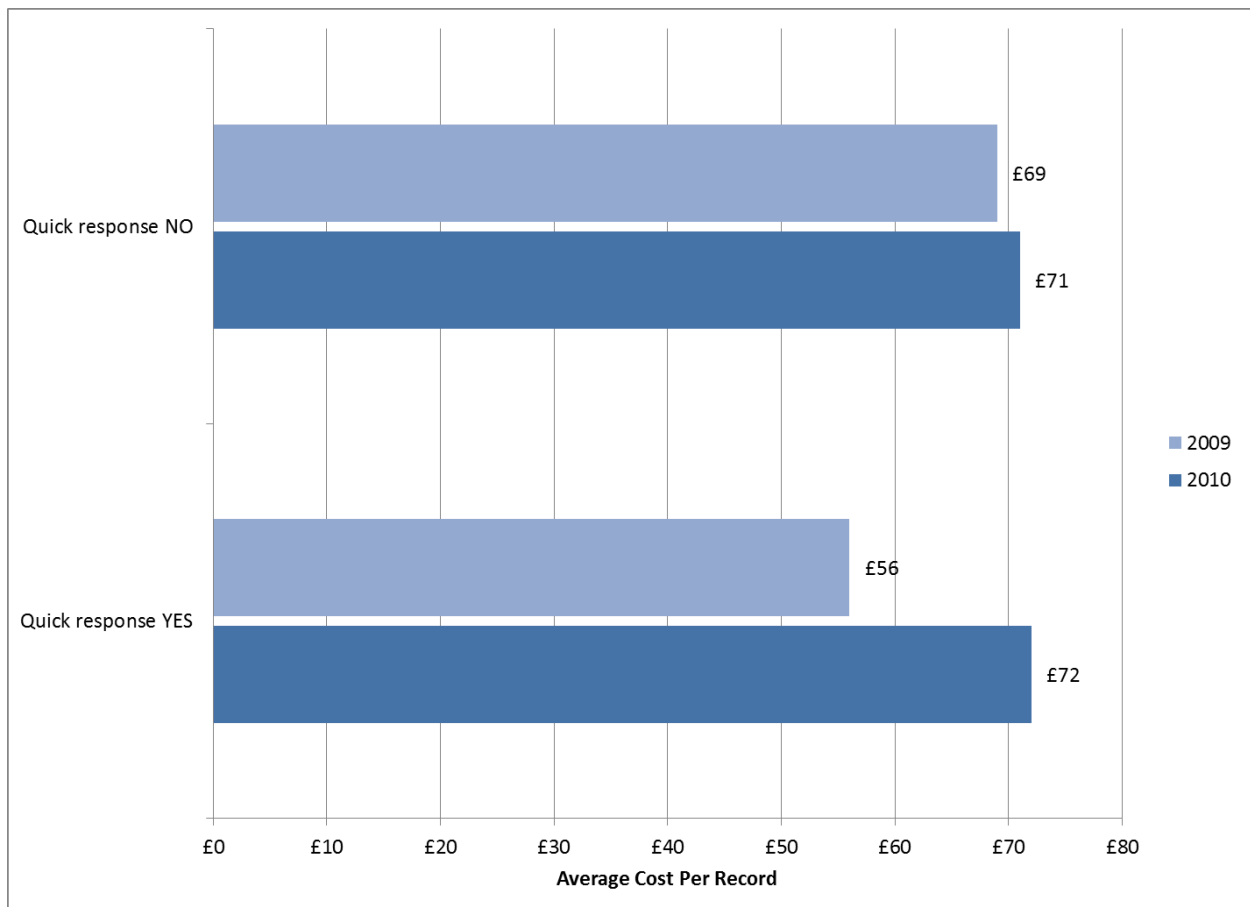
**Rapid response to data breaches became less frequent and much more expensive:** A third (32 percent) of companies notified victims within one month of discovering the data breach, down 4 points from last year.

"Quick responders" paid more per record than companies that moved more slowly. In 2010, quick responders had a per-record cost of £72, up £16 (29 percent) from the year before. Companies that took longer paid £71 per record, up only £2 (3 percent) from 2009. Breaches for companies that moved quickly cost £1 (1 percent) more this year than slower responders, £14 (108 percent) more than last year. In 2009, faster companies paid £13 (19 percent) less.

Quick responders' data breach costs ranked eighth this year, up nine slots. Slower responders' breach costs ranked 12<sup>th</sup>, down six slots.

This year's results show that the value of quick response changed this year for U.K. organisations. Previously, quick response led to much lower costs. This year's figures may indicate that quick response became much more expensive between 2009 and 2010, with fewer organisations choosing to act quickly.

Regulatory compliance pressures may explain these factors. The Information Commissioner's Office (ICO) received new enforcement powers in 2010, which may lead organisations to take compliance more seriously to avoid heavy fines. Additionally, Payment Card Industry (PCI) regulations became mandatory in 2009, with the results of organisations' compliance efforts first appearing in this year's study results.



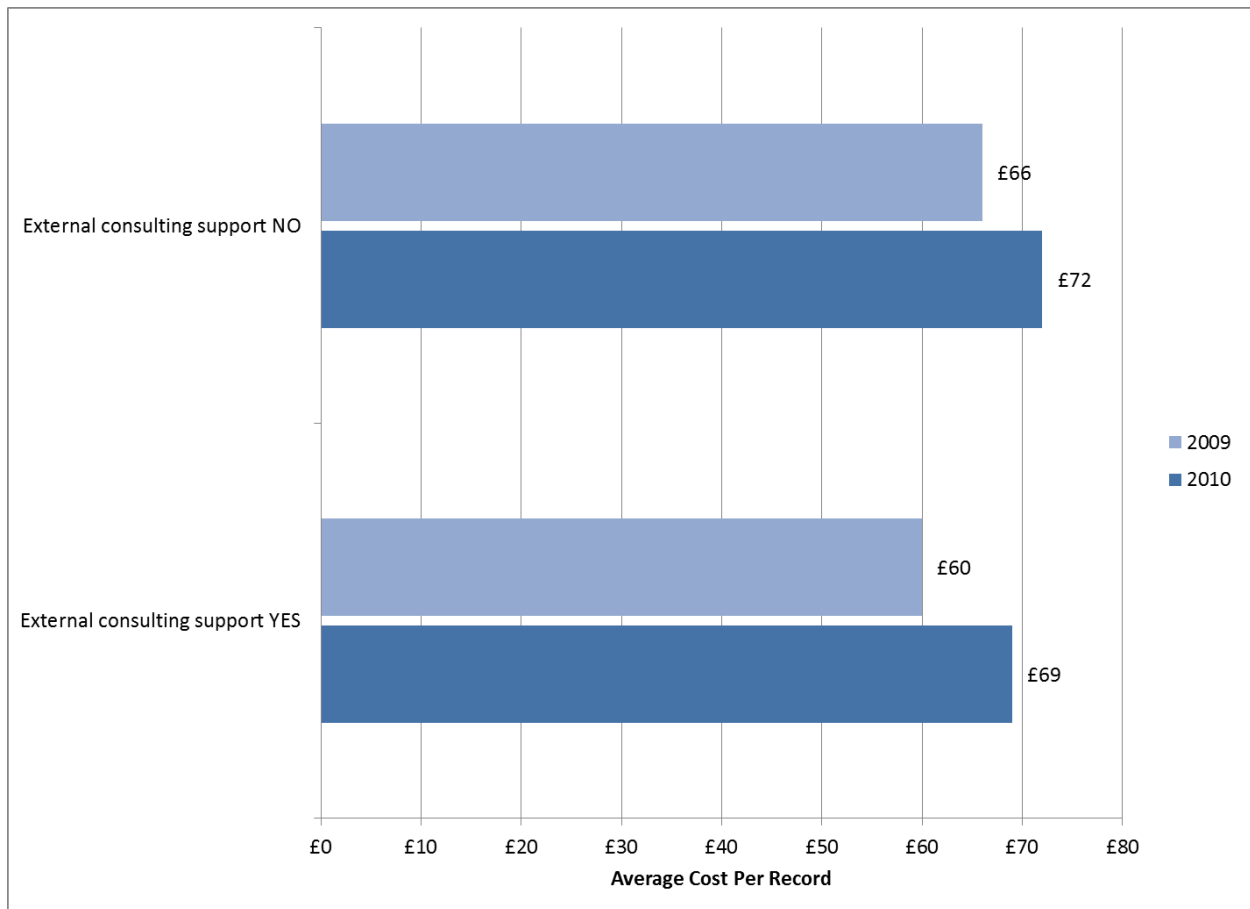
**Figure 13: Cost per record of data breaches for quick responders, 2009-10**

**Fewer organisations than ever are engaging external consulting support to respond to breaches:** The proportion of respondents that engaged outside consultants fell 10 points this year to 26 percent. This decrease, along with the sharp drop in first-time breach victims, made breaches involving outside consultants the least frequent breach type of 2010.

Breaches involving external consultants averaged £69 per record, up £9 or 15 percent. Breaches without them averaged £72 per record, up £6 or 9 percent. Breaches with external consulting support cost £3 (4 percent) less than breaches without such guidance, decreasing £3 (50 percent) from last year. In 2009, breach with external consulting support cost £6 (9 percent) less.

Data breach costs for organisations using external consulting support ranked 15<sup>th</sup>, up one slot from 2009. Costs for organisations that relied on internal resources alone ranked ninth, the same as last year.

Our results suggest that many fewer companies are using external consulting support, and those that do are seeing a smaller return on their investment in the form of cost savings. These figures may indicate that organisations' growing experience with data breaches may lead them to believe they don't need specialised help for breach response. We will closely watch this issue in future reports.



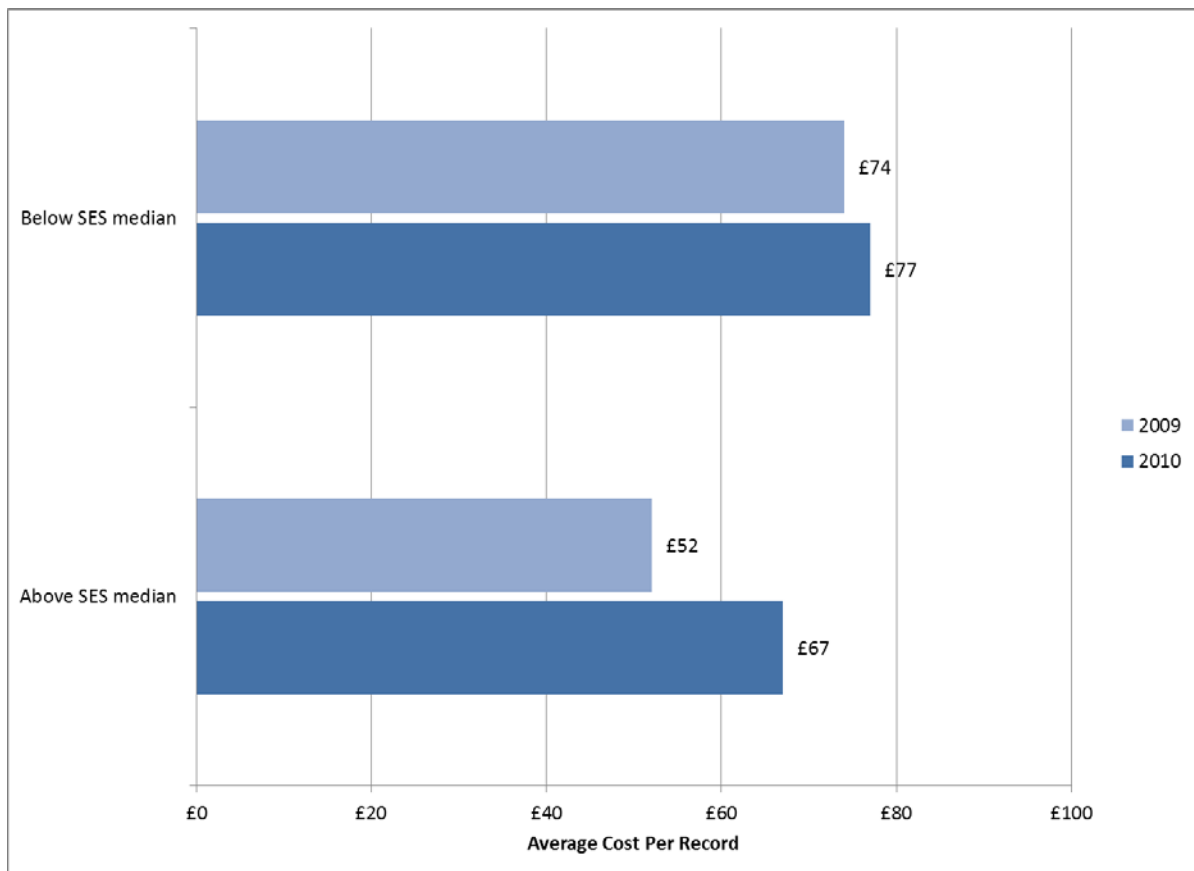
**Figure 14: Cost per record of data breaches when outside consultants are involved with response, 2009-10**

**Good security posture remains common and cost-effective, but not as much as last year:** Forty-two percent of respondents had a Security Effectiveness Score (SES) above the median value determined from benchmark results.<sup>12</sup> Even though that figure is down 3 points from last year, good security posture remains the most common breach response attribute.

Not surprisingly, those organisations with a more favourable security posture (SES above the median) experienced a lower average cost per compromised record than those with a less favourable posture (SES below the median). Accordingly, organisations above the median had an average cost per record in 2010 of £67, £15 (29 percent) more than last year. Companies below the median paid £77, £3 (4 percent) more than last year. Breaches for companies above the median cost £10 (13 percent) less this year than for those below, a £12 (55 percent) drop from last year. In 2009, better-prepared companies paid £22 (12 percent) less.

Data breach costs for companies above the SES median ranked 17<sup>th</sup>, down three slots from last place in 2009. Costs for companies below the median ranked third, the same as last year.

Our results suggest that organisations continue to be serious about preventing data breaches by upholding good IT security postures. Following best practices that enable an SES above the median, however, saved less money this year than last year. Additionally, costs for companies above the median rose much more than for those below the median. Taken together, these figures may indicate that companies are paying more to ensure good security, perhaps to meet increasing regulatory compliance requirements.



**Figure 15: Cost per record of data breaches for companies by SES security posture, 2009-10**

<sup>12</sup>The SES is a methodology developed in 2005 by the Ponemon Institute and PGP Corporation (which Symantec acquired in 2010) for PGP's annual encryption trends study. The SES measures the effectiveness of an organisation's security posture. Since its inception six years ago, this proprietary security scoring method has been used in nearly 100 studies involving information security practitioners in organisations throughout the world.

**Despite dramatically lowering breach costs, CISO leadership is becoming much less popular:** A third (32 percent) of respondents had a CISO (or equivalent title) manage data breaches, down 7 points from 2009.

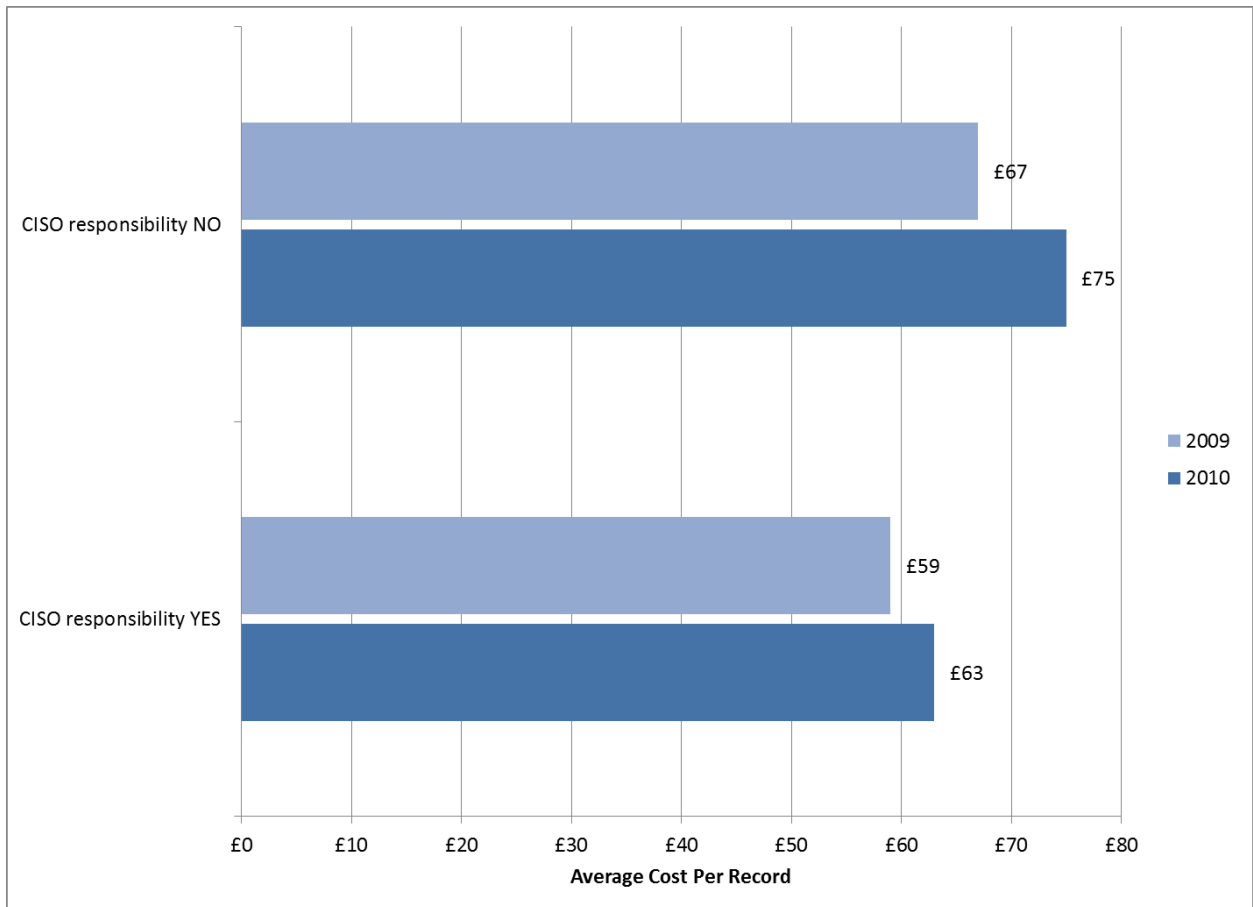
Breach response involving CISO leadership averaged £63 (up £4 or 7 percent) while breaches without it averaged £75 (up £8 or 12 percent). CISO-led breach response cost £12 (16 percent) less this year than breaches without such guidance, falling £4 (50 percent) from last year. In 2009, breach response involving CISO leadership cost £8 (12 percent) less.

Data breach costs for organisations with CISO leadership ranked 19<sup>th</sup>, down three ranks. Costs for organisations without CISO leadership ranked fourth, up four slots from 2009.

Our results suggest that expert guidance through CISO leadership can substantially reduce overall data breach costs. While specialised expertise still helps keep breach costs down, those investment costs are rising as organisations race to keep pace with escalating data protection threats. Increased compliance demands on organisations may also be raising CISO-related costs.

More than other senior company IT officials typically involved in crisis management activities surrounding data breach response, CISOs play a strategic role in ensuring security and privacy measures are effectively implemented. This strategic emphasis complements the high priority U.K. organisations put on regulatory compliance and data breach mitigation.

Taken together, all these factors make the sharp drop in use of CISO leadership in breach response somewhat counterintuitive. We will closely watch this issue in future reports.



**Figure 16: Cost per record of a data breach when CISOs lead breach response, 2009-10**

## Report Conclusions

Taken together, this year's results suggest that data breaches remain a persistent threat with which the wide majority of companies already have unfortunate experience. The data security threat landscape continues to worsen and data breach costs continue to rise, particularly on the upper end of the scale. Organisations are responding by locking down their IT systems to prevent breaches and taking proactive steps to act quickly and competently when breaches occur. Despite these positive steps, they still face increasing challenges from their own people, equipment and outsourcing partners.

This year, multiple factors apparently confirm that data breach mitigation and regulatory compliance drive companies' data breach costs – and, in some cases, may lead them to pay much more than they would otherwise. We base our conclusion on key findings, including:

- Defending against malicious or criminal attacks and lack of internal preparedness and expertise appear to drive spending on data breach costs
- Malicious or criminal attacks remain the most expensive breach cause and, for the first time, are the most expensive breach type overall
- Eighty percent of breach attributes are less frequent than last year
- Lost business and ex-post response are becoming the main components of data breach costs

Costs rose the fastest for breaches involving proactive breach response and preparation and expertise that regulations demand for compliance (SES above the median, quick response and those not involving third-party mistakes, systems failures or lost or stolen devices). At the same time, costs were lowest and shrinking for breaches lacking both internal (systems failures) and external (third-party mistakes) preparation and expertise for compliance.

Systems failures became a much bigger priority this year and had the most distinctive results. These results are even more interesting when taken in context of the frequency of other breach types. More companies have data breach experience and fewer reported breaches due to negligence, lost or stolen devices and third-party mistakes.

Taken together, these figures may indicate that fear of data breaches and cyber attacks may be driving more companies to devote much more effort to IT security. Companies' increasing focus on data breach mitigation and regulatory compliance may be encouraging them to discover more systems failures behind data breaches – especially when breach response costs from systems failures are the lowest in this study and are getting cheaper. We will closely watch this issue in future.

These trends appear to correspond with findings from the *2010 Annual Study: U.K. Enterprise Encryption Trends* report, also conducted by the Ponemon Institute and sponsored by Symantec. That report found that two major factors dramatically shifted organisations' reasons for deploying encryption and other data protection technologies in 2010 – the escalation in frequency and severity of cyber attacks designed to steal sensitive or confidential data, and the increasing strictness of data protection and privacy regulations aimed to prevent those data breaches. In past years, concerns about mitigating data breaches and protecting data itself drove encryption implementation. For the first time, companies now focus on thwarting pre-breach attacks and avoiding post-breach legal noncompliance penalties.

Data breaches are becoming a fact of life, which may be causing fewer people to end or diminish their relationships with breached organisations. More products and services become available to meet the demand, bringing down costs, and increasing mandates and regulations may push more organisations to clean up after the fact. Time will tell whether the data breach notification legislation and other government action that occurred in 2010 will create the desired long-term reductions of the incidence and severity of data breaches for U.K. organisations.

In conclusion, our 2010 research once again suggests that U.K. organisations by and large take their stewardship of sensitive personal data seriously and are taking greater steps to ensure its protection from breaches by implementing encryption technologies. Despite its limitations, the research reinforces best practices for encryption and arguments that those practices provide a positive return on investment. This insight is especially important as more organisations deploy more mobile devices and new technologies such as cloud computing and virtualisation that, even as they offer tremendous functionality and cost savings, create new challenges for data protection.

## Suggested Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organisations should strongly consider a holistic approach to protecting data wherever it is – at rest, in motion and in use. While many companies may prefer manual and policy approaches, those means by themselves work better as part of a multi-pronged approach with automated IT security solutions. Many automated, cost-effective enterprise data protection solutions are now available to secure data both within an organisation and among business partners. Some of the most popular and effective technologies include:

- Encryption (including whole disk encryption and for mobile devices/smartphones)
- Data loss prevention (DLP) solutions
- Identity and access management solutions
- Endpoint security solutions and other anti-malware tools

Companies should also look for centralised management of IT security solutions that automatically enforce IT security best practices company-wide. Such capability enables enterprises to align information protection with corporate security policies and regulatory or business-partner mandates. It also enables organisations to implement technology with minimal or no user disruption, encouraging user compliance and acceptance.

## Next Steps

This fourth annual report enables organisations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report provides guidance to conduct an internal audit, create breach response cost estimates and compare technology and other costs of preventing data breaches. Whether or not they have yet had a data breach, companies should also consider the following best practices:

- Vet and evaluate the security posture of third parties before sharing confidential or sensitive information. Pick responsible vendors that can guarantee data protection through encryption and appropriate procedures and controls. Also, ensure that third parties protect data on their employees' mobile devices.
- Ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for extensive business travelers. Also, consider implementing inventory control, anti-theft devices and data loss prevention (DLP) policies, practices and technologies.
- Take as slow and thoughtful an approach to data breach response as possible, given federal and state legal requirements applicable to location, industry and circumstances of the breach. Prepare in advance as much as possible to enable quick and cost-effective response.
- Improve IT security posture by upgrading technology and procedures to reflect current best practices and the preventive solutions discussed above.
- Develop and practice a crisis management plan that clearly defines roles, duties, procedures and timelines.
- Establish an organisational structure that allows the CISO or other security/privacy leaders to take charge and ensure the detection and notification process is handled appropriately. When in doubt about legal requirements or the technical aspects of responding to data breaches, seek the counsel of external consultants and legal and technology experts to help ensure improved results.
- To minimise customer turnover (churn), develop a proactive communications outreach plan that clearly defines the issue and root cause of the breach incident. Whenever feasible, take steps that minimise potential harm to data breach victims. For instance, consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.
- Finally, perform a post-mortem a few months after the incident to objectively evaluate the adequacy and effectiveness of the overall response. At this point, it may make good sense to consider buying insurance products to defray future data breach costs.

## About the Ponemon Institute

The 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.

## About Symantec Corporation

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at [www.symantec.com](http://www.symantec.com).

## Appendix A – Study Methodology

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

- **Non-statistical sample:** The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of U.K. organisations experiencing a breach involving the loss or theft of customer or consumer data in 2010.

For consistency purposes, our study does not include data breaches resulting from missing or stolen employee records. In addition, we deliberately excluded data breaches considered to be catastrophic (as defined by an event involving the loss or theft of more than 150,000 records). Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the judgmental nature of our company recruitment process.

- **Non-response:** The current findings are based on a small representative sample of completed benchmark studies. All participating organisations were known to have experienced a breach involving the lost or theft of customer or consumer data sometime in 2010. Thirty-eight U.K. companies completed all parts of the benchmark study. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the data breach process, as well as the underlying costs associated with information loss.
- **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. Industry classification relies on self-reported results.
- **Unmeasured factors:** To keep the study 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 estimated at this time.
- **Estimated cost results:** The quality of study research is based on the integrity of confidential responses received from companies. While reliability checks were incorporated into the benchmark study process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique rather than the company's detailed actual cost data could create significant bias in presented results.

### Benchmark Methods

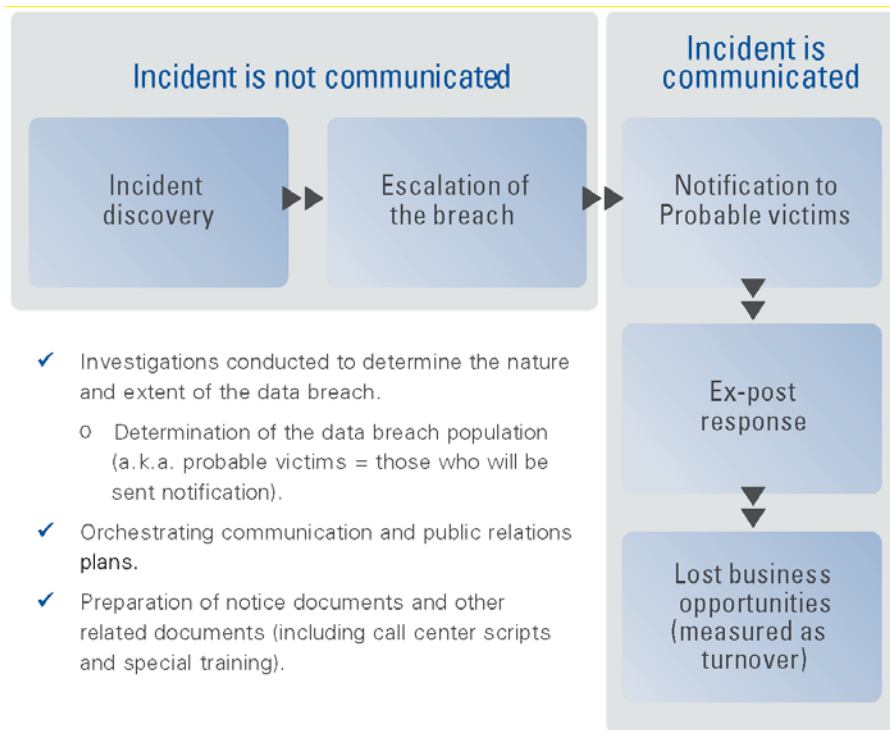
The benchmark study instrument was designed to collect descriptive information about the costs incurred either directly or indirectly concerning the breach event. Typically, the point-person for each study was privacy, data protection or compliance professionals responsible for managing the data breach incident. The study required these practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a structured study form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal churn rates that resulted from the breach event.

The study design relied upon a shadow costing method used in applied economic research. This method doesn't require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.

Within each category, cost estimation was a two-stage process. First, the study required individuals to provide direct cost estimates for each privacy cost category by checking a range variable. A range variable was used rather than a point estimate to preserve confidentiality (to ensure a higher response rate). Second, the study required participants to provide a second estimate for both indirect cost and opportunity cost, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct cost within a given category.

The size and scope of study items was limited to known cost categories that cut across different industry sectors. We believed that a study focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. We also used a paper instrument, rather than electronic study, to provide greater assurances of confidentiality.

The diagram below illustrates the activity-based costing schema used in the current benchmark study. The study examined the above-mentioned cost centers. The arrows suggest that these cost centers are sequentially aligned, starting with incident discovery and proceeding to escalation, notification, ex-post response, and culminating in lost business. The cost driver of ex-post response and lost business opportunities is public disclosure or notice of the event.



**Figure 17: Visual representation of benchmark cost categories**