



2007 Annual Study: U.K. Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventive Solutions

A study summarising the actual costs incurred by 21 U.K. organisations that lost confidential information resulting in a publicised data breach.

Benchmark research conducted by
Ponemon Institute, LLC



February 2008



© 2008 PGP Corporation and 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 PGP Corporation and Symantec Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.

Table of Contents

EXECUTIVE SUMMARY	2
DATA BREACH NOTIFICATION REQUIREMENTS	2
2007 ANNUAL STUDY: U.K. COST OF A DATA BREACH	2
CONCLUSIONS	3
PREVENTATIVE SOLUTIONS	4
NEXT STEPS	4
INTRODUCTION	5
STUDY OVERVIEW & METHODOLOGY	6
STUDY METHODOLOGY	6
KEY REPORT FINDINGS	8
REPORT CONCLUSIONS	14
PREVENTATIVE SOLUTIONS	14
NEXT STEPS	15
PGP® SOLUTIONS	15
SYMANTEC SOLUTIONS	16
APPENDIX A – SURVEY METHODOLOGY	19
BENCHMARK METHODS	20

Executive Summary

Data Breach Notification Requirements

In 2007, the U.K. saw the rise of widely publicised data breaches. Growing media attention, dissatisfaction of consumers, and action by regulatory authorities to enforce penalties under existing law, created a de facto requirement for informing the public of a data breach.

The fine of almost £1 million imposed by the Financial Services Agency (FSA) for the loss of a laptop in early 2007 first brought the subject of data breaches and their consequences to the U.K. headlines.¹ Subsequently, financial services firms, retail organisations, or local councils suffering a breach chose to proactively publicise such incidents in order to better control the ensuing fall-out. Attention surrounding data breaches accelerated at the end of the year following the continued loss of large amounts of personal and private information by both private industry and the government.

2007 Annual Study: U.K. Cost of a Data Breach

This 2007 Ponemon Institute benchmark study, sponsored by PGP Corporation and Symantec Corporation, examines the costs incurred by 21 U.K. businesses after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is first study in the U.K. based on a proven methodology used for the last 3 years to produce a similar study in the United States.

Breaches included in the survey ranged from less than 2,500 records to more than 125,000 records from eight different industry sectors.

Among the study's key findings:

- **Total costs:** The total averages costs of a data breach reached £47 per record compromised. The average total cost per reporting company was more than £1.4 million per breach and ranged from £84,000 to almost £3.8 million.
- **Cost of lost business:** The cost of lost business was the most significant component of data breach costs, averaging more than £496,000 or £17 per record compromised. Lost business accounts for 36 percent of costs in the study.
- **Other data breach costs vary; notification costs least significant:** Costs associated with a data breach other than lost business accounted for the majority of breach costs (64 percent). Given the lack of legally mandated notification of impacted individuals, notification costs averaged only £1 per record. Detection and other activities initiated following a breach both averaged £15 per record.
- **Lost or stolen laptops and mobile devices is the most frequent cause of a data breach:** 36 percent data breaches in the sample were due to lost or stolen laptops or other devices such as USB flash drives.
- **Encryption and data loss prevention use increase following a breach:** Encryption and data loss prevention (DLP) solutions were the top two technology responses following a data breach. This finding indicates that organisations increasingly understand the benefits of enterprise data protection (EDP) in securing data wherever it is stored or used.

¹ "FSA fines Nationwide £980,000 for information security lapses," 14 February 2007: <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>

Additional study findings:

- **Increased customer churn significant following a breach:** The resulting abnormal customer churn rate for the period following a data breach averaged 2.5 percent. Abnormal churn rates ranged from negligible to almost 7 percent. Greater customer turnover leads to lower revenues and a higher cost of new customer acquisition resulting from increased marketing to recover lost customer business.
- **Financial services firms impacted most:** The cost of a data breach for financial services organisations was £55 per compromised record, or more than 17 percent higher than the average, demonstrating that organisations with high expectations of trust and privacy have more to lose from a data breach.
- **Third-party data breaches cost more:** Breaches by third-party organisations such as outsourcers, contractors, consultants, and business partners were reported by 38 percent of respondents. Breaches by third parties were also more expensive than breaches by the enterprise itself, averaging £59 per record compared to £42 per record.
- **Incident response roles and responsibilities:** The group most frequently involved in the response to a data breach was the IT security department (62 percent of organisations), with compliance and business units sharing responsibility 55 percent and 43 percent of the time, respectively.

Conclusions

This study establishes a benchmark for U.K. organisations to evaluate the risk and impact of a data breach. Although notification of impacted individuals is not a legal requirement in the U.K., recent developments in London and Brussels indicate that this situation could change. The House of Lords' August 2007 *Personal Internet Security Report*² calls for the government to take action ahead of the European Union and introduce breach notification requirements similar to those in more than 35 U.S.³ states. At the same time, the E.U. is considering updates to the ePrivacy Directive that includes breach notification for the Telecoms sector.⁴

Even with all the time, effort, and money invested by organisations in data privacy and compliance initiatives of various shapes and sizes, data breaches continue to occur. Leading enterprise IT managers and industry analysts recognize that organisations must focus on proactively protecting their data instead of relying exclusively on written policies, procedures, and training.

The survey reveals:

- Trust may be intangible and hard to quantify, but the result of breaking that trust is clear: 36 percent of breach costs are due to lost business.

² "Personal Internet Security," House of Lords, Science and Technology Committee, August 2007: http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm

³ More information on U.S. state laws is available from the National Conference of State Legislatures: <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>

⁴ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, November 2007
http://ec.europa.eu/information_society/policy/ecom/doc/library/proposals/698/com_2007_0698_en.pdf

- In this first annual survey, breaches where a third-party organisation was entrusted with protecting data incurred higher costs than those that occurred when enterprise itself was responsible. Given the cost disparity between in-house and third-party breaches, organisations should closely evaluate the enterprise data protection policies and systems used with and by third-party outsourcers or consultants.
- Organisations that have built their brand on trust have more to lose from a data breach, demonstrated by the 17 percent higher costs of a data breach for financial services providers compared to an average breach.
- Encryption and data loss prevention solutions top the list of most frequently named post-breach technology measures deployed to help avert a future data breach.

As information risk management becomes important across the enterprise, the investment required to prevent a data breach appears to be dwarfed by the resulting costs of a breach. With average breach costs totaling £1.4 million and the source of many breaches (such as laptops and USB flash drives) critical to productivity, the return on investment (ROI) and justification for preventative measures is clear.

Preventative Solutions

Automated, cost-effective enterprise data protection solutions are now available to secure data wherever it is stored or used, both within an organisation and among business partners. Centralised deployment of data loss prevention and encryption solutions allows information protection to be aligned with corporate security policies and regulatory or business-partner mandates. Centralised management allows security best practices to be automatically enforced throughout the enterprise.

Next Steps

This report enables organisations to forecast in detail the specific actions and costs required to recover from a data security breach. The report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology cost of preventing data breaches.

Introduction

Stolen laptops, compromised databases, lost backup tapes, or mismanaged email—all can result in the loss of valuable customer information. Organisations that experience a data breach can suffer the loss of existing customer confidence, damage to their brand, and loss of future revenue from new customers that take their business elsewhere. Equally damaging are the actual costs associated with legal requirements to notify customers that their private, sensitive, and confidential information has been mishandled.

In 2007, the U.K. saw the rise of widely publicised data breaches. Growing media attention, dissatisfaction of consumers, and action by regulatory authorities to enforce penalties under existing law, created a de facto requirement for informing the public of a data breach.

The fine of almost £1 million imposed by the Financial Services Agency (FSA) for the loss of a laptop in early 2007 first brought the subject of data breaches and their consequences to the U.K. headlines.⁵ Subsequently, financial services firms, retail organisations, or local councils suffering a breach chose to proactively publicise such incidents. Attention surrounding data breaches accelerated at the end of the year following the continued loss of large amounts of personal and private information by both private industry and the government.

When a breach occurs, an organisation investigates, customers and media learn of the event, and in the end some customers curtail or discontinue their business - what is the corporate cost to recover? The Ponemon Institute, Symantec, and PGP Corporation are pleased to offer the third annual survey that quantifies the actual costs incurred by 21 organisations compelled to notify individuals of data privacy breaches. Summarized in this document, the study provides detailed information from responses to questions companies face when responding to a data breach:

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

⁵ “FSA fines Nationwide £980,000 for information security lapses,” 14 February 2007: <http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>

Study Overview & Methodology

The Ponemon Institute's annual benchmark study, begun in 2005 in the United States, examines the costs organisations incur when responding to data breach incidents in the United Kingdom resulting in the loss or theft of protected personal information.

- To complete the study, benchmark surveys were sent to companies known to have experienced a breach involving the loss or theft of consumer data during the year.
- Of that group, 21 companies agreed to participate by completing the survey. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from an actual data loss incident.
- The reported number of individual records breached ranged from less than 2,500 records to 105,000 records from companies in 8 different industry sectors.
- The 2007 survey shows that 38 percent of breaches occurred when data was held by third parties. A third-party breach is defined as a case where a third party (such as professional services, outsourcers, vendors, business partners) was in the possession of the data and responsible for its protection. In comparison, an in-house breach is defined as a case where the protection of data was the responsibility of the organisation itself (by an employee or for data on the corporate network, for example).

Table 1 summarizes the 21 study participants by industry and source of data breach:

Industry	# Organisations	# In-House Breaches	# Third-Party Breaches
Finance services	11	7	4
Retail	4	3	1
Professional services	1	0	1
Technology	1	1	0
Telecom	1	0	1
Transportation	1	1	0
Media	1	1	0
Hospitality	1	0	1
Total	21	13	8
	100%	62%	38%

Table 1: Study participants and data breach source

Study Methodology

The study looked at core process-related activities associated with a company's detection of and response to a data breach, identifying four "cost centers":

- **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, email, 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 to minimize potential harm. Redress activities also include ex-post responses such as credit report monitoring or the reissuing of a new account or credit card.

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

To extrapolate these opportunity costs, the study uses a shadow costing method that relies on the “lifetime value” of an average customer as defined for each participating organisation. These costs are dependent on two significant components:

- **Turnover or “churn” of existing customers:** The estimated number of customers that 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 that will not have a relationship with the organisation as a consequence of the breach. This number is provided as an annual percentage.

Key Report Findings

The Ponemon Institute's annual benchmark study examines the costs organisations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

Data breach costs, lost business most significant component: For 2007, the per-record compromised costs of a data breach for the sample is £47. Lost business costs are the most significant component of a data breach, accounting for 46% of total breach costs.

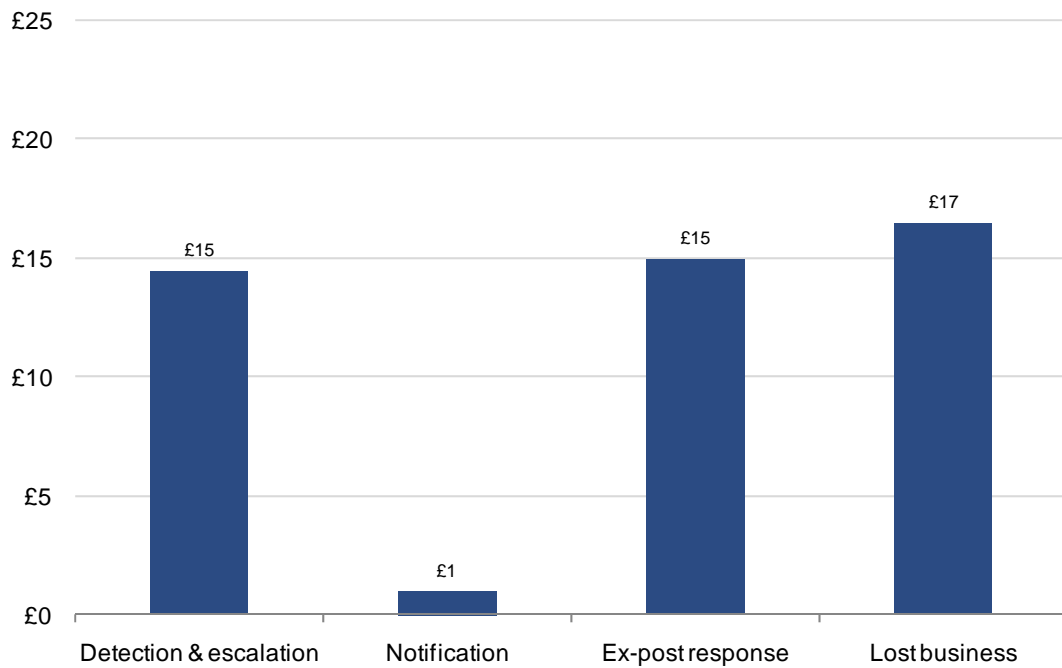


Figure 1: Data breach costs by centre per record compromised

Note: The cost of lost business includes both lost business due to churn and increased customer acquisition costs.

Cause of a data breach: Lost or stolen laptops and other devices such as USB flash drives were the most significant source of a data breach, accounting for over a third of data breach incidents (36 percent). The breach of data paper records was the second most significant source of a breach. In total, 12 percent of incidents were due to some type of malicious intent by an insider, hacker, or code (for example, malware or spyware).

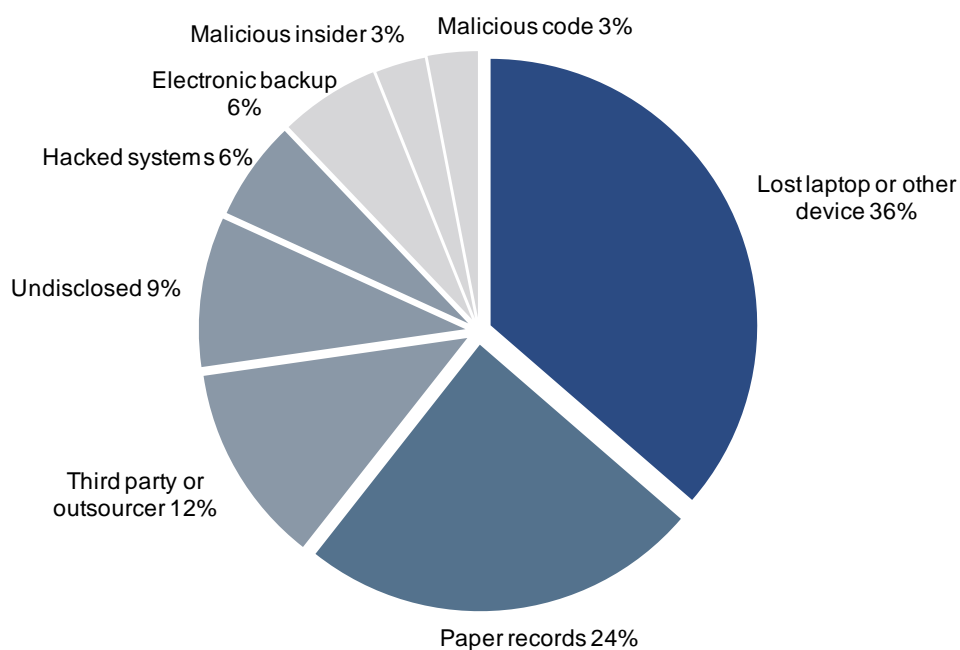


Figure 2: Primary cause of a data breach

Note: Respondents specified the primary cause of a data breach incident. Because some incidents may have occurred when a third party was responsible for data protection but the cause of the data breach was most closely represented by a different type, respondents may not have selected “Third party or outsourcer.” See the following finding for more information on the source of a data breach.

Third parties responsible for more than a third of breach, internal breaches more costly: Third-party organisations such as business process outsourcers or consultants were responsible for 38% of the data breaches reported. Third-party outsourcers or consultants often analyze or process large volumes of customer-related information. Likewise, third-party breaches were significantly more expensive, costing £59 per record compromised compared to £42 for internal breaches.

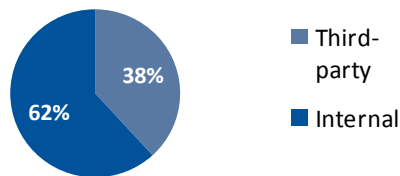


Figure 3: Share of data breaches by responsible party

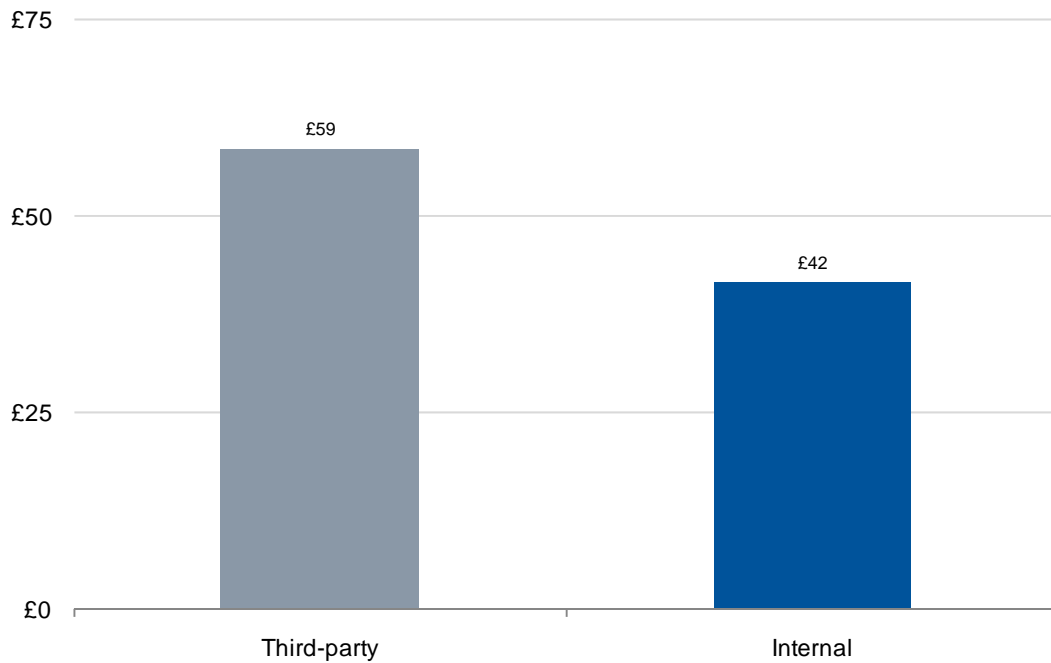


Figure 4: Comparing data breach costs by responsible party

Increased churn rates following a breach: Following a data breach, organisations suffered an average increased customer churn rate of 2.50 percent. Four out of the 21 organisations suffered abnormal churn rates of more than 4 percent. Greater customer turnover leads to lower revenues and a higher cost of new customer acquisition resulting from increased marketing to recover lost customer business. These churn rates demonstrate that customers are concerned about the impact of a data breach – concerned enough to discontinue their business relationship.

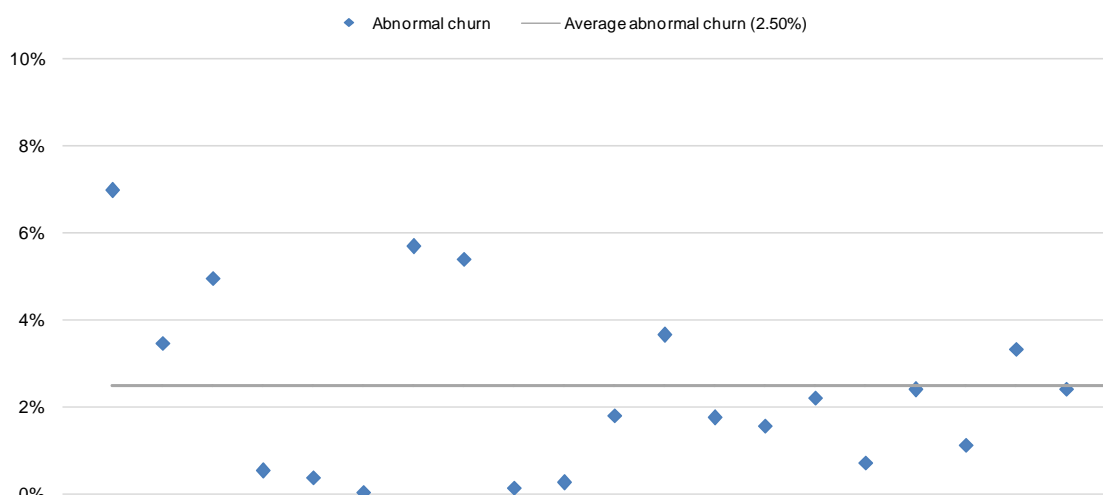


Figure 5: Abnormal churn rates following a data breach incident

Technology measures implemented following a breach: As the result of a data breach, organisations frequently implemented technology solutions to protect and detect confidential data as part of an enterprise data protection strategy. Organisations ranked encryption and data loss prevention solutions as the technologies most often implemented or expanded in use after an incident.

Top technology measures implemented (in rank order)
Encryption
Data loss prevention
Identity and access management
Endpoint security controls
Security event management
Perimeter controls

Table 2: Technology measures implemented as a result of a data breach

Expectations of trust and privacy drive data breach costs higher: The expectation customers have for financial services firms to treat their confidential data with greater care is illustrated by a 17 percent higher cost of a data breach compared to the survey average.

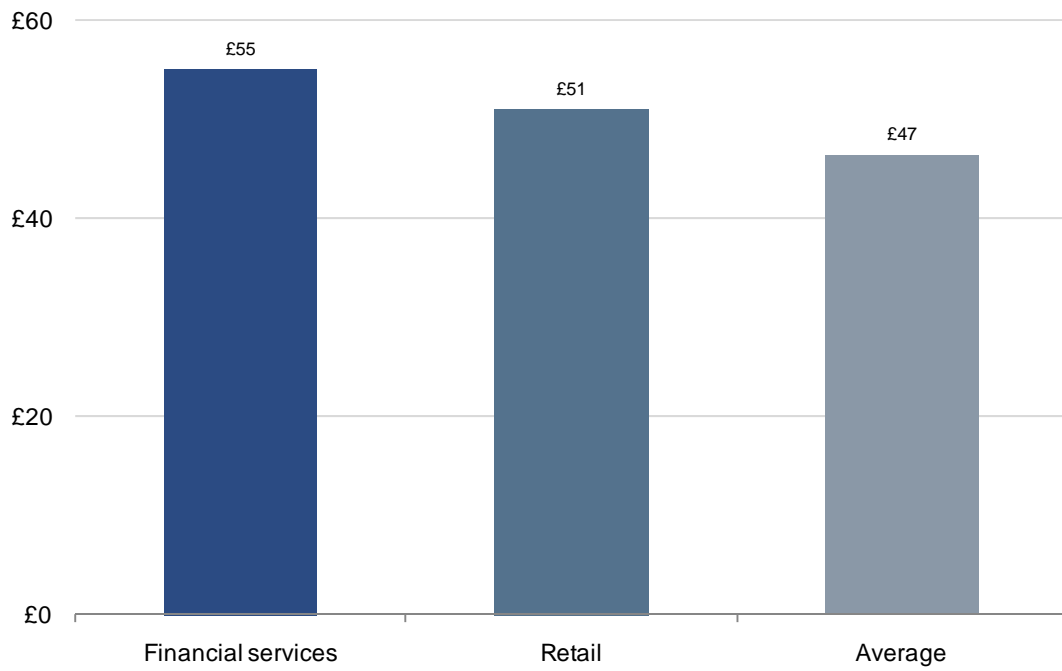


Figure 6: Costs of a breach compared for financial services and retail organisations

Incident response roles and responsibilities: The group most frequently involved in the response to a data breach was the CISO office (62 percent of organisations). The compliance function also frequently shared responsibility 57 percent of the time. IT organisations shared responsibility only 35 percent of the time, indicating that U.K. businesses treat a breach event as a failure of policy and not a technical IT operation. In all but three organisations, the response to a data breach was a shared responsibility among two or more departments.

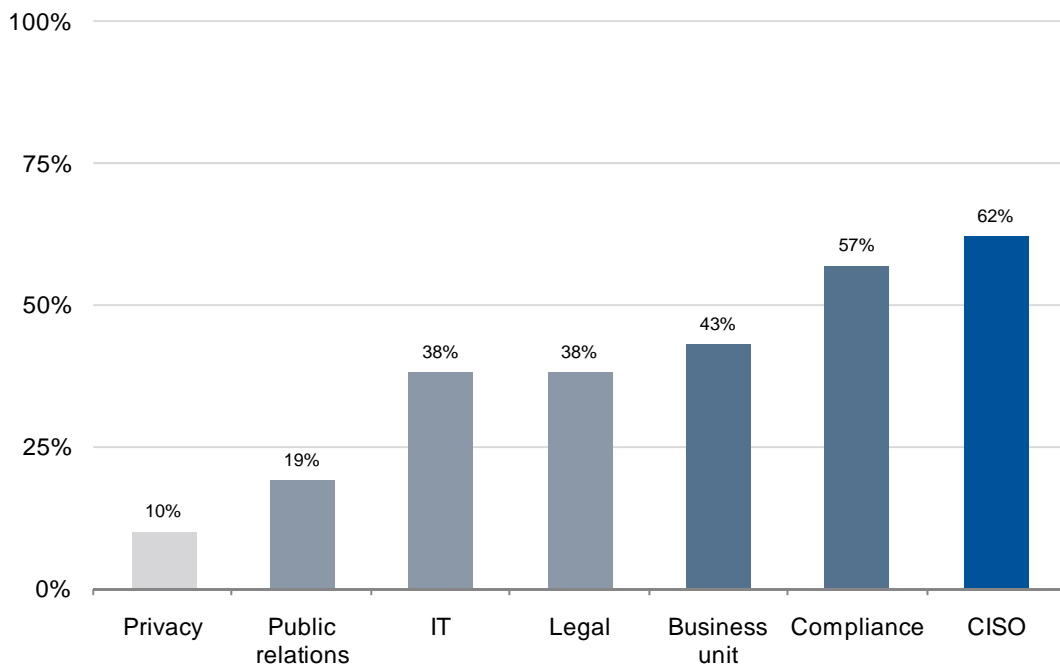


Figure 7: Data breach response shared responsibility

Report Conclusions

This study establishes a benchmark for U.K. organisations to evaluate the risk and impact of a data breach. Although notification of impacted individuals is not a legal requirement in the U.K., recent developments in London and Brussels indicate that this situation could change. The House of Lords' August 2007 *Personal Internet Security Report*⁶ calls for the government to take action ahead of the European Union and introduce breach notification requirements similar to those in more than 35 U.S.⁷ states. At the same time, the E.U. is considering updates to the ePrivacy Directive that includes breach notification for the Telecoms sector.⁸

Even with all the time, effort, and money invested by organisations in data privacy and compliance initiatives of various shapes and sizes, data breaches continue to occur. Leading enterprise IT managers and industry analysts recognize that organisations must focus on proactively protecting their data instead of relying exclusively on written policies, procedures, and training.

The survey reveals:

- Trust may be intangible and hard to quantify, but the result of breaking that trust is clear: 36 percent of breach costs are due to lost business.
- In this first annual survey, breaches where a third-party organisation was entrusted with protecting data incurred higher costs than those that occurred when enterprise itself was responsible. Given the cost disparity between in-house and third-party breaches, organisations should closely evaluate the enterprise data protection policies and systems used with and by third-party outsourcers or consultants.
- Organisations that have built their brand on trust have more to lose from a data breach, demonstrated by the 17 percent higher costs of a data breach for financial services providers compared to an average breach.
- Encryption and data loss prevention solutions top the list of most frequently named post-breach technology measures deployed to help avert a future data breach.

As information risk management becomes important across the enterprise, the investment required to prevent a data breach appears to be dwarfed by the resulting costs of a breach. With average breach costs totaling £1.4 million and the source of many breaches (such as laptops and USB flash drives) critical to productivity, the return on investment (ROI) and justification for preventative measures is clear.

Preventative Solutions

Automated, cost-effective enterprise data protection solutions are now available to secure data wherever it is stored or used, both within an organisation and among business partners. Centralised deployment of data loss prevention and encryption solutions allows information protection to be aligned

⁶ "Personal Internet Security," House of Lords, Science and Technology Committee, August 2007: http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm

⁷ More information on U.S. state laws is available from the National Conference of State Legislatures: <http://www.ncsl.org/programs/lis/cip/priv/breach.htm>

⁸ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, November 2007
http://ec.europa.eu/information_society/policy/ecom/doc/library/proposals/698/com_2007_0698_en.pdf

with corporate security policies and regulatory or business-partner mandates. Centralised management allows security best practices to be automatically enforced throughout the enterprise.

Next Steps

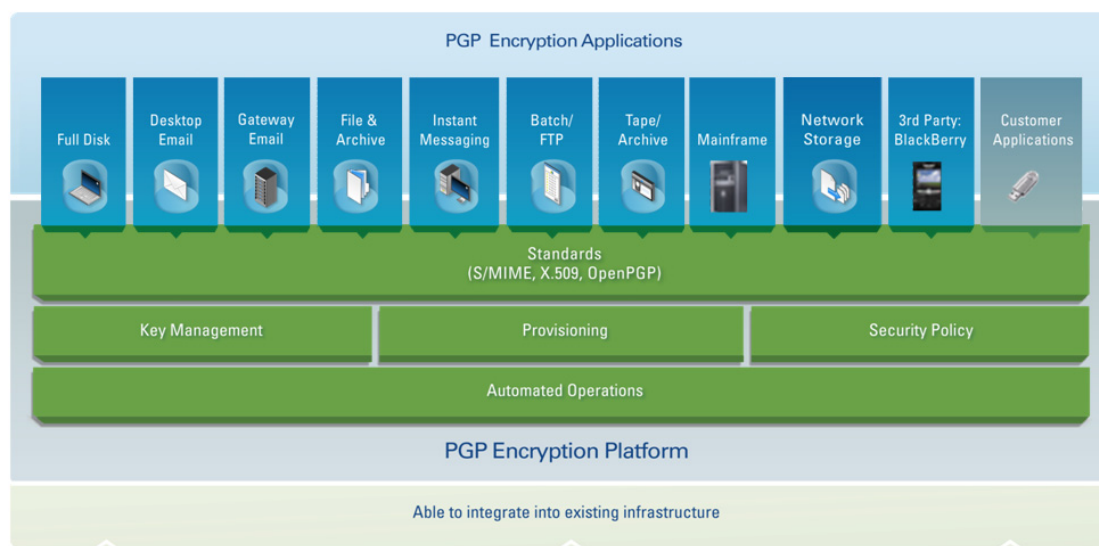
This report enables organisations to forecast in detail the specific actions and costs required to recover from a data security breach. The report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology cost of preventing data breaches.

PGP® Solutions

PGP Corporation has developed the PGP® Encryption Platform to protect confidential information from data breaches, regulatory notification requirements, and resulting remediation costs. As part of an enterprise data protection strategy to defend data wherever it goes, this unified platform allows IT organizations a simple, cost-effective way to provide data security to all internal departments and external partners that handle confidential information.

The PGP Encryption Platform allows for central management with automatic operation, email infrastructure transparency, and removal of laptop/desktop, gateway/server, and mobile/wireless encryption silos. It meets business unit requirements for customer privacy, competitive protection, supply chain integrity, and “brand insurance” against public breaches – without disrupting users.

Once deployed, the PGP Encryption Platform is capable of provisioning encryption applications in a combination of gateway and endpoint locations. This “deploy-once, enable-over-time” approach allows enterprises to address their greatest risks today and grow into a comprehensive security solution over time.



Current PGP encryption applications:

- **PGP® Whole Disk Encryption:** encrypted full disk, files, folders, USB drives, and external backups
- **PGP® NetShare:** encrypted files and folders stored on network file servers

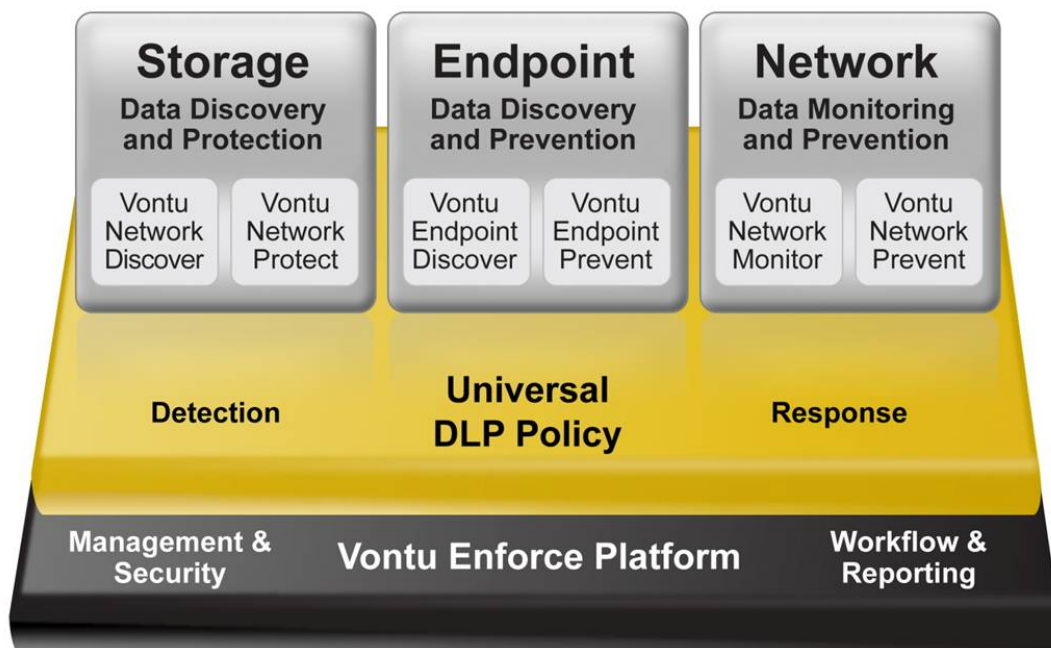
- **PGP Universal™ Gateway Email:** gateway encryption and digital signatures
- **PGP® Desktop Email:** desktop encryption, digital signatures, file shred, and IM encryption
- **PGP® Support Package for BlackBerry®:** PGP encryption on BlackBerry handheld devices
- **PGP® Command Line:** encryption for automated processes and file transfers
- **PGP® Software Development Kit:** encryption for customized, internal applications

The PGP Encryption platform is an automated, server-based architecture that centrally handles all key management, corporate encryption policy, and network infrastructure interaction. It manages both gateway and client encryption applications, providing one uniform encryption policy that is automatically enforced for all users. Automatic encryption and decryption means no user training, minimal IT resource impact, and low operational costs. Its proxy-based design installs without disruption to existing network architectures and easily expands to meet future risks to data security.

PGP Corporation sets the standard for verifying that no backdoors or secret access exists in its product software. The company is the only commercial security vendor to publish source code for peer review. PGP source code has been downloaded more than 100,000 times. The PGP Encryption Platform was one of only 12 innovations identified by a panel of experts to receive The Wall Street Journal 2007 Innovation Award. PGP Whole Disk Encryption and PGP Desktop Email are both *SC Magazine* "Best Buy" products, winning against competing point solutions in hands-on group tests.

Symantec Solutions

Vontu Data Loss Prevention 8 from Symantec is the industry's first integrated solution that combines both endpoint and network-based software to protect confidential data wherever it is stored or used. The layered architecture enables customers to prevent malicious and unintentional data breaches regardless of whether data is stored on the network or on a disconnected endpoint, as well as prevent data from exiting any network gateway or endpoint.



Vontu Data Loss Prevention products include:

- **Network Data Discovery and Protection**
Discover and protect confidential data exposed on file servers, databases, Microsoft SharePoint®, Lotus Notes®, Documentum®, LiveLink®, Microsoft Exchange®, web servers, and other data repositories.
- **Endpoint Data Discovery and Protection**
Discover and inventory confidential data stored on laptops and desktops and prioritize high risk endpoints for additional protection.
- **Endpoint Data Monitoring and Prevention**
Monitor and prevent confidential data from being copied to USB devices, burned to CD/DVDs, downloaded to local drives, sent via webmail, IM, or P2P networks, or hidden using encryption software.
- **Network Data Monitoring and Prevention**
Monitor and prevent data loss with comprehensive coverage including email, IM, Web, Secure Web (HTTPS), FTP, P2P, and generic TCP.
- **Vontu Enforce Platform**
Automatically enforce universal DLP policies with a centralized platform for detection, workflow and automation, reporting, system management and security.

About The Ponemon Institute

The Ponemon Institute© is dedicated to advancing ethical information and privacy management practices in business and government. The Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

Dr. Larry Ponemon is the chairman and founder of the Ponemon Institute. He is also a founding member of the Unisys Security Leadership Institute and an Adjunct Professor of Ethics & Privacy at Carnegie Mellon University's CIO Institute. Dr. Ponemon is a critically acclaimed author, lecturer, spokesman, and pioneer in the development of privacy auditing, privacy risk management, and the ethical information management process.

Previously, Dr. Ponemon was the CEO of the Privacy Council and the Global Managing Partner for Compliance Risk Management at PricewaterhouseCoopers (where he founded the privacy practice). Prior to joining PricewaterhouseCoopers, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG and as the Executive Director of the KPMG Business Ethics Institute. Dr. Ponemon holds a Ph.D. from Union College, attended the Doctoral Program in System Sciences at Carnegie-Mellon University, and has a Masters degree from Harvard University as well as a Bachelors degree from the University of Arizona. Contact The Ponemon Institute at www.ponemon.org or +1 800 887 3118.

About PGP Corporation

PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications allow organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, network storage, file transfers, automated processes, and backups.

PGP® solutions are used by more than 80,000 enterprises, businesses, and governments worldwide, including 95 percent of the Fortune® 100, 75 percent of the Fortune® Global 100, 87 percent of the German DAX index, and 51 percent of the U.K. FTSE 100 Index. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at www.pgp.com or +1 650 319 9000.

About Vontu

Vontu, now part of Symantec, is the leading provider of Data Loss Prevention solutions that combine endpoint and network-based technology to accurately detect and automatically protect confidential data wherever it is stored or used. By reducing the risk of data loss, Vontu solutions from Symantec help organizations ensure public confidence, demonstrate compliance and maintain competitive advantage. Vontu Data Loss Prevention customers include many of the world's largest and most data-driven enterprises and government agencies. Vontu products have received numerous awards, including IDG's InfoWorld 2008 Technology of the Year Award for "Best Data Leak Prevention," as well as SC Magazine's 2006 U.S. Excellence Award for "Best Enterprise Security Solution" and Global Award for "Best New Security Solution." For more information, please visit <http://go.symantec.com/vontu>.

Appendix A – Survey Methodology

The Ponemon Institute's study utilizes 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 results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organisations, all U.S.-based entities experiencing a breach involving the loss or theft of customer, consumer, or employee data over the past 12 months. Statistical inferences, margins of error, and confidence intervals cannot be applied to this data, given the nature of the sampling plan.
- **Non-response:** The current findings are based on a representative sample of completed surveys. Twenty one companies completed all parts of the benchmark survey. Non-response bias was not tested, so it is always possible companies that did not participate are substantially different from those that completed the survey in terms of the methods used to manage the data breach process as well as the underlying costs involved.
- **Sampling-frame bias:** Because the 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. The Institute believes 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 survey concise and focused, The Institute decided to omit other important variables such as leading trends and organisational characteristics from its analyses. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- **Estimated cost results.** The quality of survey research is based on the integrity of confidential responses received from companies. Although certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed “shadow costing method,” explained later) rather than actual cost data could create significant bias in presented results.
- **Survey sample.** Out of the 21 surveys completed, financial services and retail organisation made up the largest segments of the sample, account for 71 percent of the survey sample. The following chart and table details the entire sample composition.

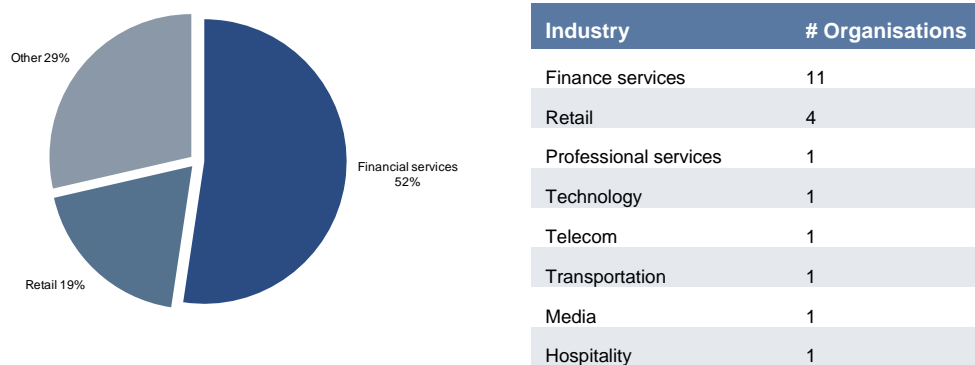


Figure 8 & Table 3: Sample composition by industry vertical

Benchmark Methods

The benchmark survey instrument was designed to collect descriptive information from data protection or information security practitioners about the costs incurred either directly or indirectly concerning the breach event. It also required practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal customer turnover rates that resulted from the breach event.

The survey design relied on a “shadow costing method” used in applied economic research. This method does not 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 survey 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 survey required participants to provide a second estimate for both indirect costs and opportunity costs, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct costs within a given category.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. The Institute believed that a survey focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. It also used a paper instrument, rather than an electronic survey, 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 the public disclosure or notice of the event.

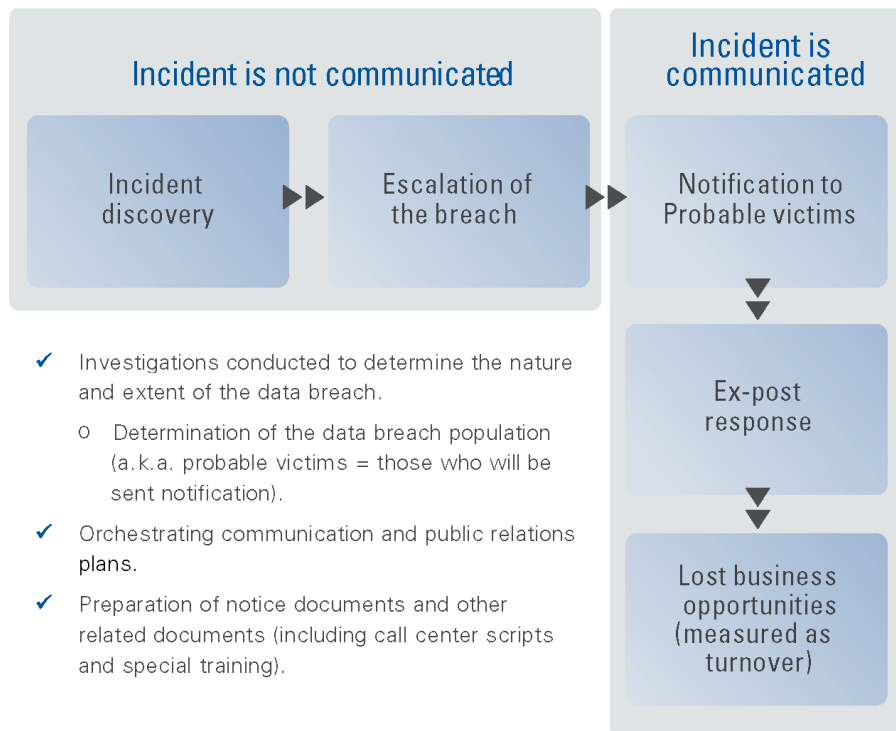


Figure 9: Visual representation of benchmark cost categories