2009 Annual Study: Global Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventive Solutions

Executive Summary:

This 2009 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the comparative cost incurred by organizations in five countries 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 first annual survey of this issue.

Breaches included in the survey ranged from approximately 2,500 to approximately 101,000 lost or stolen records from 18 different industry sectors.

Benchmark research conducted by

Ponemon Institute, LLC

April 2010

Table of Contents

Executive Summary

PGP Corporation and the Ponemon Institute are pleased to report the results of our first annual study concerning the cost of data breach incidents for global companies. Ponemon Institute research indicates that data breaches continue to have serious financial consequences on organisations. This year's report, entitled *2009 Global Cost of a Data Breach Study*, found that data breach costs in countries with national data breach notification laws were significantly higher than in countries without such legislation.

Ponemon Institute first conducted its Cost of a Data Breach study in the United States more than five years ago. Since then, we have expanded the study to include the United Kingdom, Germany, Australia and France. This initial study established objective methods for quantifying specific activities that result in direct, indirect and opportunity 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.

The 2009 results of this research represent the consolidated analysis of five national cost of data breach studies: United States, United Kingdom, Germany, France and Australia (all converted into US dollars). Our current analysis of the actual data breach experiences of more than 130 organizations from 18 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.

Some of the top findings from the 2009 Global study include:

- **Organisations in all five countries experience very costly data breaches.** The average organisational cost of a data breach was $3.4 million and the average cost per compromised record was $142. The most expensive data breach event included in this year's study cost one organisation more than $31 million to resolve.

- **Data breach costs in countries with national data breach notification laws were significantly higher than in countries without such legislation.** For example, in the United States, where 46 states have now introduced laws forcing organisations to publicly disclose the details of breach incidents, the cost per lost record was 43 percent higher than the global average. In Germany, where equivalent laws were passed part way through last year (in July 2009), costs were second highest, 25 percent above the worldwide average. In Australia, France and the United Kingdom, where these types of law have not yet been introduced, costs were all below the average. When breach notification laws are introduced across the rest of the world, other countries will follow the same pattern and costs will rise.

- **Data breaches diminish customer confidence and trust, and lead to abnormally high customer turnover (churn) and lost business that directly drive data breach costs.** In this year's study, the average abnormal churn rate across all 133 incidents was 4 percent, which we measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). Almost half (44 percent) of the incurred data loss expenses related to the cost of lost business, reflecting the added expense of consumer churn and the increased difficulty of attracting new customers in the wake of negative publicity. Again, costs varied dramatically between countries and were highest in the United States, where the cost of lost business was, on average, equivalent to 66 percent of overall expenses. As

more countries add data breach notification laws, their ability to keep breaches secret will diminish and their costs associated with churn and attracting new business will continue to grow.

- **For better or worse, data breaches are becoming more common.** Fifty percent of all cases in this year's study involved organisations that had their first breach. All countries reported an average of 16 percent higher costs for organisations that had their first breach. France had the highest increase, 33 percent, while Germany and Australia tied for the lowest at 11 percent. One possible reason is that these organisations do not have experience in responding to data breaches and may not be as knowledgeable and efficient. This finding also suggests companies that experience data breaches become more efficient at managing costs over time.

- **Third-party flubs and malicious attacks are the most common and expensive breach types.** Thirty-five percent of all cases in this year's study involved data breaches concerning outsourced data to third parties and 36 percent involved a malicious or criminal attack that resulted in the loss or theft of personal information. All countries reported strong to tremendous increases in costs from these causes, with an average per-record increase of 49 percent from third-party incidents and 47 percent from malicious attacks. The United States had the lowest increase from third-party mistakes, 12 percent, while France by far had the highest – 116 percent. The higher costs could be due to additional forensics investigation and consulting fees. Malicious or criminal attacks cost much more in countries without data breach notification laws. Malicious attacks increased the cost per compromised record the most in France (121 percent more) and Australia (61 percent more). By contrast, hostile attacks increased per-record costs only by 25 percent in the United Kingdom, 23 percent in Germany and a mere 7 percent in the United States. These findings suggest that organizations must start protecting themselves more proactively from increasingly aggressive malicious outsiders. Another explanation is that training and awareness programs are having a positive effect on insider threats to sensitive data.

- **Forty-three percent of participating companies engaged an outside consultant to assist them over the course of the data breach incident.** Because so many organisations reported that this was their first breach, almost half engaged consultants to help them respond. Our findings suggest that engaging a consultant or other third-party expert to assist in the data breach incident can raise the average cost per compromised record by an average of 41 percent. Specifically, US and UK respondents that engaged a consultant experienced, on average, a per record data breach cost that was 25 percent and 9 percent lower, respectively, than companies that decided to go it alone. On the other hand, German and Australian respondents that brought in help saw their costs increase by 24 and 25 percent, respectively. French respondents saw their costs skyrocket by 191 percent, the largest single increase we saw in this study. These figures are more likely an indication of certain organisations deciding to devote more resources and responsiveness to data breach issues in general than a statement on the quality of consulting work itself. The large number of first-time breach victims could have affected this statistic as well, as companies look for help dealing with new threats.

- **Strong CISO leadership helps keep costs down.** In 40 percent of participating companies, the CISO (or equivalently titled security executive) was in charge of managing the data breach incident. While other functional areas are typically involved in crisis management activities surrounding the data breach, our results suggest CISO leadership decreases the overall cost per compromised record by an average of 21 percent compared to companies without such leadership. Benefits varied widely; Australian companies saw only a 3-percent decrease, while German companies saw their costs plummet 45 percent.

2009 Annual Global Study: Cost of a Data Breach

This 2009 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the costs incurred by 133 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 first annual survey of this issue.

Breaches included in the survey ranged from roughly 2,500 to approximately 101,000 records from 18 different industry sectors.

What we learned from the 2009 results:

The total cost of a data breach was $142 per compromised record. According to participants, data breaches cost their companies an average of $142 per compromised record – of which $63 pertained to indirect costs including lost business due to abnormal turnover (churn) of existing and future customers.[1] Direct costs – which include detection, escalation, notification and ex-post response – were $79. Actual costs varied widely by country. The United States had the highest cost per compromised record, $204, followed by Germany at $177. The other countries had substantially lower costs – France at $119, Australia at $114 and the United Kingdom with the lowest at $98 per compromised record.

Data breaches are costly events for organisations. The average organisational cost of a data breach was $3.4 million. The United States had the most expensive average data breach cost of $6.75 million. Germany came in second with almost less than half that total at $3.44 million. The United Kingdom and France had nearly identical average costs at $2.57 million and $2.53 million, respectively. Australia had the cheapest average cost of $1.83 million.

The most expensive data breach event included in this year's study cost a company more than $31 million to resolve. The least expensive total cost of data breach for a company included in our study was approximately $341,736. The magnitude of the breach event ranged from approximately 2,500 to approximately 101,000 lost or stolen records. Data breach costs appear to be linearly related to the size or magnitude of the breach event.

Data breaches diminish customer confidence and trust, leading to abnormally high customer turnover (churn) that directly drives data breach costs. In this year's study, the average abnormal churn rate across all 133 incidents was 4 percent, which we measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). All five countries' rates hovered within a percent of each other, with Australia and the United States having the lowest rates, France and Germany the highest, and the United Kingdom almost squarely on the average.

For all countries, lost business was the largest component of total cost per record – 44 percent on average and ranging from 30 percent in France to 66 percent in the United States. The US average cost per compromised record of lost business was $135, while the German average cost was $61 and the UK average cost was $45, respectively. The Australian average cost per record was $38 and the lowest average per-record cost of all was for France, $36. The cost of lost business means consumers are concerned about how well organizations safeguard personal data. These decisions to take their business elsewhere reflect increased awareness of what's happening in other countries and greater focus on cybersecurity issues in general and appreciation for the need for data protection in particular.

The direct cost countries spent most on was ex-post response. On average, the five countries surveyed spent more than a quarter (27 percent) on ex-post response. Germany paid the most in average ex-post response costs per compromised record, $54, because Germans see data protection as a mark of an organization's trustworthiness and thus expect it to help them after a breach. The United States came in second at $46. France paid $41 per record, Australia $33 per record and the United Kingdom $25 per record.

[1] For purposes of comparability across different breach incidents, we measure data breach cost on a per compromised record basis.

Respondents devoted an average of 18 percent of total cost per record to detection and escalation. German respondents spent the most on detection and escalation, $52 per compromised record. German detection and escalation costs are much higher than in other countries because German organizations are much more focused on attacks to data and systems and thus have more security in place to mitigate risk. The high cost also reflects the investment required in new technologies and processes in order to comply with the country's recent notification legislation. Australia, France and the United Kingdom spent $38 per record, $36 per record and $18 per record, respectively. In the United States, where laws were first enforced in 2005, these costs were small by comparison ($8) and have decreased over recent years, suggesting that American organisations have developed more efficient detection and escalation processes over time. French, Australian and UK firms should expect their costs to follow the same trend: initially rising in order to ensure compliance with emerging regulations and then declining once processes become more refined.

All countries surveyed spent the least on notification, spending on average only 7 percent of their total costs on it. US respondents had the highest notification cost, $15 per compromised record. The other four countries spent considerably less per record -- $10 in the United Kingdom, $9 in Germany, $6 in France and only $4 in Australia.

Five industries spanned all five country reports: financial, communications, technology, consumer and retail. Financial breaches had the highest average cost per compromised record ($188), followed by communications ($165), technology ($130), consumer ($123) and retail ($94). Countries with data breach laws had much higher costs – on average, US costs were 36 percent and German costs were 32 percent higher than the average. The other countries had substantially lower average costs – Australian costs were 16 percent lower, French costs were 20 percent lower and UK costs were 32 percent lower than the average.

Fifty percent of all cases in this year's study involved organisations that had their first breach. All countries reported higher costs for organisations that had their first breach, with an average of 16 percent. France had the highest increase, 33 percent, while Germany and Australia tied for the lowest at 11 percent. One possible reason is that the organisation does not have experience in responding to a data breach and may not be as knowledgeable and efficient. This finding suggests companies that experience data breaches become more efficient at managing costs over time.

Thirty-five percent of all cases in this year's study involved third-party mistakes or flubs. Data breaches involving outsourced data to third parties, especially when the third party is offshore, are quite costly. This could be due to additional forensics investigation and consulting fees. All countries reported strong to tremendous increases in costs from third-party incidents, with an average increase of 49 percent. The United States had the lowest increase, 12 percent, while France by far had the highest – 116 percent.

Thirty-six percent of all cases in this year's study involved a malicious or criminal attack that resulted in the loss or theft of personal information. Our research shows data breaches involving malicious or criminal acts were much more expensive than incidents resulting from every other factor except third-party flubs, which it almost matched. All countries reported strong to tremendous increases in costs from third-party incidents, with an average increase of 47 percent. Malicious or criminal attacks cost much more in countries without data breach notification laws. Malicious attacks increased the cost per compromised record the most in France (121 percent more) and Australia (61 percent more). By contrast, hostile attacks increased per-record costs only by 25 percent in the United Kingdom, 23 percent in Germany and a mere 7 percent in the United States. These findings suggest that organizations must start protecting themselves more proactively from increasingly aggressive malicious outsiders. Another explanation is that training and awareness programs are having a positive effect on insider threats to sensitive data.

Forty-three percent of participating companies engaged an outside consultant to assist them over the course of the data breach incident. Because so many organisations reported that this was their first breach, almost half engaged consultants to help them respond. Our findings suggest that engaging a consultant or other third-party experts to assist in the data breach incident can raise the average cost per compromised record by an average of 41 percent. Specifically, US and UK respondents that engaged a consultant experienced, on average, a per record data

breach cost that was 25 percent and 9 percent lower, respectively, than companies that decided to go it alone. On the other hand, German and Australian respondents that brought in help saw their costs increase by 24 and 25 percent, respectively. French respondents saw their costs skyrocket by 191 percent, the largest single increase we saw in this study. These figures are more likely an indication of certain organisations deciding to devote more resources and responsiveness to data breach issues in general than a statement on the quality of consulting work itself. The large number of first-time breach victims could have affected this statistic as well, as companies look for help dealing with new threats.

Thirty-five percent of all cases in this year's study involved employee negligence. Negligence-related breaches were the least costly breach type in our study, averaging 25 percent less than other incidents. All countries studied saw much lower costs related to negligence, ranging from 19 percent in France to 35 percent in the United States.

Thirty-two percent of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. All countries experienced noticeably higher data breach costs associated with these items, with an average of 22 percent and France seeing a 72-percent increase. The only exception was Germany, which saw its related costs drop by 10 percent.

In 40 percent of participating companies, the CISO (or equivalently titled security executive) was in charge of managing the data breach incident. While other functional areas are typically involved in crisis management activities surrounding the data breach, our results suggest CISO leadership decreases the overall cost of data breaches. Across all five country studies, companies with a CISO (or equivalent title) who managed the data breach incident experienced an average cost per compromised record that was 21 percent lower compared to companies without such leadership. Benefits varied widely; Australian companies saw only a 3-percent decrease, while German companies saw their costs plummet 45 percent.

Twenty-eight percent of all cases in this year's study involved a systems glitch. Systems glitch-related breaches were among the least costly of all breach types, with costs 15 percent lower on average than other types. The United Kingdom reported a marginal 1-percent increase due to glitches, while Germany, Australia and the United States saw costs 17 percent, 26 percent and 27 percent lower, respectively.

Thirty-seven percent of participating companies notified appropriate parties within one month of discovering the data breach (a.k.a. quick responders). Our findings suggest that companies that execute notification quickly can experience a much higher average cost per compromised record of data breach than companies that move more slowly. Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for organisations – especially during the detection, escalation and notification phases – which raised total costs by an average of 13 percent among respondents. Quick response ratcheted up data breach costs in the United States by 12 percent and in France by a whopping 112 percent. Conversely, it lowered costs in Australia by 16 percent, the UK by 18 percent and Germany by 23 percent.

Organisations with a better security posture had lower data breach costs than their less-prepared peers. Forty-seven percent of participating companies achieved a security effectiveness score (SES) that was above the median value determined from benchmark results.[2] Those organisations with a more favorable security posture (SES above the median) experienced a slightly lower average cost per compromised record of data breach than organisations with an SES below the median. The beneficial effect varied by country but averaged 10 percent; the United States, Australia and France all saw decreases of 7 percent or less, while Germany had an 11-percent drop and the United Kingdom had a remarkable 29-percent decrease in costs.

[2]The SES is a methodology developed by Ponemon Institute and PGP Corporation in 2005 for its annual encryption trends study. The SES measures the effectiveness of an organisation's security posture. Since its inception five years ago, this proprietary security scoring method has been used in more than 80 studies involving information security practitioners in organisations throughout the world.

Expanded use of encryption is the most popular preventive measure taken after data breaches. On average, 47 percent of respondents indicated they used encryption to protect their data after a breach. Other popular preventive measures taken after data breaches were additional manual procedures and controls (46 percent) and training and awareness programs (44 percent). Other remediation procedures following the breach incident included: strengthening of perimeter controls (33 percent), data loss prevention (DLP) solutions (31 percent), endpoint security solutions (28 percent), identity and access management solutions (27 percent), and security certification or audit (25 percent). The least popular solutions were security intelligence and event management (SIEM) systems (24 percent) and other system control practices (16 percent).

To prevent future breaches, most UK, Australian and French companies prefer manual- and policy-based approaches over technological solutions. Although most US companies still prefer manual and policy solutions as post-breach remediation measures, many companies use enabling prevention and remediation technologies often and effectively. Most German organizations prefer technological solutions, especially encryption, as post-breach remediation measures. The new data breach notification legislation helped drive German organizations to embrace their faith in technology in general, but especially to known and trusted solutions.

Because this is a benchmark study of more than 130 companies in five countries, we cannot generalise about the practices of all companies. However, a possible reason for the popularity of manual and policy-based solutions is that they may be faster to implement and are less expensive than technology solutions.

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 manual and policy approaches may come first to mind for many companies, those approaches by themselves are not as effective as a multi-pronged approach that includes 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 of these technologies currently available 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 first annual report enables organisations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This 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 and other costs of preventing data breaches.

Companies should also consider following industry best practices, including:

- Companies should vet and evaluate the security posture of third parties before sharing confidential or sensitive information.

- To minimize customer churn (turnover), companies should draft communications that clearly define the issue and root cause of the breach incident. Whenever feasible, the company should take steps that minimize

potential harm to data breach victims – for instance, the company may consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.

- When in doubt about requirements, companies should seek the counsel of consultants and legal experts to ensure the notification process complies with the plethora of national and European data breach notification laws.
- Companies should ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for people who travel extensively for business.
- Companies should 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.
- Companies should discover ways to embrace technological solutions as well as manual and policy solutions.

Introduction

Throughout 2009 and heading into 2010, the government, industry and public in the countries we studied understood more than ever the damage that data breaches can do. High-profile data breaches continued to occur in both the public and private sectors. In addition to this, the rising media coverage and public awareness of data breach issues have prompted an examination of the need for data breach notification laws.

A string of high-profile cases involving the loss, theft and misuse of data by government agencies and businesses in the United States, Britain and Germany[3] has driven those Governments to make improving cybersecurity – and particularly protection of personal information and national cyber infrastructure and sensitive data – a national priority. Data protection was a key issue in the September 2009 German federal elections and the new coalition government promised to pass legislation improving data protection for German employees.[4] In February 2009, the Obama Administration ordered a 60-day federal cybersecurity review,[5] which recommended urgent action and suggested that "increased liability for the consequences of poor security" might improve the situation – a recommendation that resonates with the findings in this report and the actions of the countries we studied.

In December 2009, the Transportation Security Administration, part of the U.S. Department of Homeland Security, accidentally published its passenger screening criteria online, embarrassing an already hard-hit agency and industry.[6] The British Rural Payments Agency (RPA) announced in October 2009 that it lost two back-up tapes of confidential data on more than 100,000 farmers in May 2009.[7] Heartland Payment Systems, which processes 100 million transactions per month for more than 250,000 businesses, announced in January 2009 that malicious hackers may have compromised 130 million of its transactions, causing the potentially biggest data breach ever.[8]

In Australia, preserving the confidentiality of patient records in the national Medicare database continues to spark debate, as the Australian Privacy Commissioner has indicated that 400 cases of unauthorised access of personal medical records have occurred in the past four years.[9] This issue is gaining prominence as the Council of Australian Governments discusses the creation of a national electronic health plan. Recent statistics from France indicate that 67 percent of French organisations have been hit by at least one data breach incident within the last year and 92 percent of those breaches were never disclosed, as France lacks any legal or regulatory requirement to do so.[10]

Additionally, broader economic and technological trends are making data protection – and its absence during a breach – even more relevant. The struggling global economy has forced organisations to cut staff and IT budgets, increasing the risk of both former insiders and hostile outsiders seeking unauthorized access to sensitive data. At the same time, cloud computing and Software as a Service (SaaS) continue to rise in popularity while posing serious IT management and security challenges. Surveys show that the costs associated with data breaches continue to rise, to an average cost per record of £64 in the United Kingdom and US$204 in the United States, respectively.[11]

---

[3] *Privacy and Data Protection Law: European Developments,* Ernst & Young, July 2009.
[4] "Germany Strengthens Data Protection Act, Introduces Data Breach Notification Requirements," Jones Day, 26 Oct 2009 http://www.jonesday.com/germany-strengthens-data-protection-act-introduces-data-breach-notification-requirement-10-26-2009/
[5] "Obama hints at cybersecurity shakeup with review," CNET, http://news.cnet.com/8301-13578_3-10159975-38.html
[6] "TSA passenger screening manual leaked online," Washington Post, Dec 9, 2009. http://articles.sfgate.com/2009-12-09/news/17182687_1_tsa-officials-passenger-screening-homeland-security
[7] "Backup Tapes Go Missing From Government Agency," eWeek Europe, Nov 5, 2009. http://www.eweekeurope.co.uk/news/news-security/backup-tapes-go-missing-from-government-agency-2354
[8] "Heartland Payment Systems Hit By Data Security Breach," InformationWeek, Jan 20, 2009. http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212901505
[9] "Medicare staff using medical records to spy", ABC News, http://www.abc.net.au/pm/content/2010/s2834531.htm
[10] The Ponemon Institute, "2009 Annual Study: France Enterprise Encryption Trends Study," Sep 2009
[11] The Ponemon Institute, "2009 Annual Study: U.K. Cost of a Data Breach", Feb 2010 and "2009 Annual Study: U.S. Cost of a Data Breach", Jan 2010

As a result of these pressures, and responding to public demand, all five countries surveyed in this study took major steps to augment their data protection legislation in 2009. The three countries that already have data breach notification laws in place – Germany, the United Kingdom[12] and the United States – passed new laws to improve data protection. In February 2009, the US Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act, which included the US' first federally mandated data breach notification requirements.[13]

Germany has a strong tradition of data protection legislation and has been at the forefront of EU discussions on the need to safeguard customer and employee information. The German Government in July 2009 approved numerous amendments to the Federal Data Protection Act, the Bundesdatenschutzgesetz (BDSG), including its first-ever requirement to notify victims and publicly announce data breaches.[14]

The similarities between the latest BDSG amendments and U.S. state data breach notification laws – which have contributed to U.S. data breach costs averaging 87 percent higher than in Germany[15] – may indicate that German companies could soon see their own data breach costs rise.[16] Additionally, Germany may cause a domino effect among other European Union Member States, similar to how California's enactment of the first state data breach notification law in 2003 has since led to 46 U.S. states passing their own laws[17] and for growing support in the U.S. Congress for a national law.

Starting in June 2009, all UK Government departments had to show compliance with a new Information Assurance Standard, IAS6.[18] Designed to decrease the number of data breaches, the Standard also applies to any service provider holding personal data on behalf of the Government, including outsourcing firms and hosting providers.

Australia and France, which currently lack any data breach notification laws, announced national initiatives to provide them. The Australian Government in October 2009 announced it would enact the most sweeping privacy law reforms – which would eventually include mandatory data breach notification – since enacting the Commonwealth Privacy Act more than 20 years ago.[19]

The French Senate in March 2010 passed bill n°93 (2009-2010),[20] which would impose a broad security obligation on data controllers to inform the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertes or CNIL) of any data breaches. It would double the maximum fine CNIL can impose, from $300,000 to $600,000, putting CNIL's punitive powers on par with data protection offices in the United Kingdom and Spain. The National Assembly will now consider the bill.[21]

---

[12] UK data breach notification requirements exist for finance and public sector organisations only.
[13] "Healthcare Organizations Pressed By HITECH, HIPAA Security Measures," Network Computing, Feb 17, 2010. http://www.networkcomputing.com/data-protection/healthcare-organizations-pressed-by-hitech-hipaa-security-pressures.php
[14] BDSG § 42a.
[15] The Ponemon Institute, "2008 Annual Study: German Cost of a Data Breach" and "2008 Annual Study: U.S. Cost of a Data Breach"
[16] Jones Day
[17] National Conference of State Legislatures, State Security Breach Notification Laws as of December 9, 2009: http://www.ncsl.org/Default.aspx?TabId=13489
[18] "Government suppliers given IAS6 warning," CRN UK, http://www.channelweb.co.uk/crn/news/2242115/government-suppliers-given-ias6
[19] The Australian, "Government to re-write Privacy Act", October 14, 2009 http://www.theaustralian.com.au/news/government-to-re-write-privacy-act/story-e6frgal6-1225786600364
[20] http://www.senat.fr/leg/ppl09-331.html
[21] Stephane Bellec, "Le Senat adopte la notification obligatoire des failles de securite en enterprise," http://pro.01net.com/editorial/514406/le-senat-adopte-la-notification-obligatoire-des-failles-de-securite-en-entreprise/

Finally, the European Parliament and Council of Telecoms Ministers approved the EU Telecoms Reform Package in November 2009.[22] The package included a data breach notification law requiring European communication providers, including ISPs, to notify consumers when they lose sensitive customer data. This new law influenced data breach notification legislation in France, Germany and the United Kingdom.

Three countries added or expanded the powers of high-level government positions for cybersecurity. The Obama Administration filled the long-vacant position of White House Cybersecurity Coordinator and created the first-ever federal CIO and CTO positions.[23] The British Ministry of Justice (MOJ) provided its privacy watchdog, the Information Commissioner's Office (ICO), the power to fine organisations that lose personal data up to £500,000.[24] The Australian Department of Defence opened its new Cyber Security Operations Centre in Canberra and sought to fill many senior IT security staff positions at its Australian Defence Force Computer Security Incident Response Team (CSIRT).[25]

Currently, Germany, the United Kingdom and the United States have passed laws requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to negligence (insider threats), human error, technology problems, or malicious acts. France and Australia do not currently require data breach notification, although the Australian Office of the Privacy Commissioner, the office responsible for best practice in handling personal identifiable information (PII), has published a voluntary guide to managing data breach incidents. The office recommends the adoption of encryption solutions to protect data 'at rest', 'in use' and 'in transit' to mitigate the risk of future breaches.[26]

Although the specific conditions for notification vary by industry, organisations may not be required to notify individuals of data breaches 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

Responding to a data breach incident includes activities intended to prevent losing customers or consumer trust and help preserve an organisation's reputation. But when organisations experience data breaches and must notify customers or clients, what costs do they encounter as they attempt to recover?

The Ponemon Institute and PGP Corporation are pleased to offer the first annual survey that quantifies the actual costs incurred by organisations compelled to notify individuals of data privacy breaches. Summarised in this document, the study provides detailed information from responses to questions organisations face when responding to a data breach:

- What are the potential legal costs?
- What are industry-average costs resulting from a breach, including the detection, investigation, notification, and possible services offered to affected individuals?
- 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 it?

[22] "European 'internet freedom' law agreed, ZDNet UK, Nov 5, 2009. http://www.zdnet.co.uk/news/networking/2009/11/05/european-internet-freedom-law-agreed-39860587/
[23] "Federal CTO Chopra Completes Obama's Tech Triad," InformationWeek, April 20, 2009. http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=216900246
[24] "MoJ gives green light to £500k data-breach fines," ZDNet UK, Jan 13, 2010. http://www.zdnet.co.uk/news/regulation/2010/01/13/moj-gives-green-light-to-500k-data-breach-fines-39985171/
[25] "Defence's cyber-security splurge just beginning," ZDNet Australia, http://www.zdnet.com.au/defence-s-cyber-security-splurge-just-beginning-339301576.htm
[26] Office of the Privacy Commissioner, "Guide to handling personal information breaches", August 2008

Study Overview & Methodology

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

- To complete the study, benchmark surveys were sent to more than 600 organisations that were known to the researcher and believed to a data breach involving the loss or theft of personal customer, consumer or student data during the past year.
- Of that group, more than 130 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 approximately 2,500 to approximately 101,000 records from companies in 18 industry sectors.
- The 2009 survey shows that 41 percent of breaches occurred due to external causes. 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 Aggregate statistics
Converted into $US dollars:

Countries	Average churn	Minimum total cost (US$)	Maximum total cost (US$)	Minimum breach size	Maximum breach size
US	3.60%	749,654	30,851,628	5,010	101,000
UK	3.90%	556,933	5,982,083	5,210	60,000
FR	4.50%	341,736	8,564,933	2,520	57,700
DE	4.20%	542,093	8,476,477	3,300	63,100
AU	3.40%	380,296	3,755,417	3,368	65,00

Table 1: Aggregate statistics by country
Converted into $US dollars

Study Methodology

Our study addresses core process-related activities that drive a range of expenditures associated with a company's data breach detection and response. The four cost centres are:

- Detection or discovery: Activities that enable a company to reasonably detect the breach of personal data either at risk in storage or in motion.
- Escalation: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- Notification: Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.
- Ex-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 Institute's 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 rates directly.

Key Report Findings

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

Data breaches are costly events for organisations. The average organisational cost of a data breach was $3.4 million. The United States had the most expensive average data breach cost of $6.75 million. Germany came in second with almost less than half that total at $3.44 million. The United Kingdom and France had nearly identical average costs at $2.57 million and $2.53 million, respectively. Australia had the cheapest average cost of $1.83 million.

The most expensive data breach event included in this year's study cost a company more than $31 million to resolve. The least expensive total cost of data breach for a company included in our study was approximately $341,736. The magnitude of the breach event ranged from approximately 2,500 to approximately 101,000 lost or stolen records. Data breach costs appear to be linearly related to the size or magnitude of the breach event.

Country	Av. Cost per record (USD)	Av. Total cost of a breach (USD)
Australia	114	1.83 million
France	119	2.53 million
Germany	177	3.44 million
UK	98	2.57 million
U.S.	204	6.75 million
Average	**142**	**3.43 million**

Table 2: Average total cost of a data breach by country, 2009

Average cost of data breach by country, 2009
$1,000,000 omitted

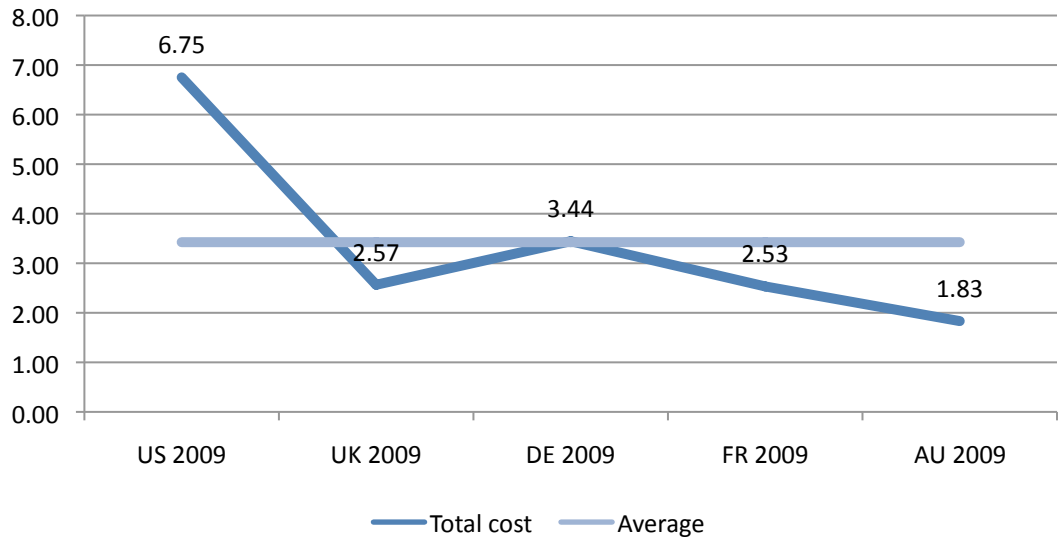

Figure 1: Average total cost of a data breach by country, 2009

The total average cost of a data breach was $142 per compromised record. According to participants, data breaches cost their companies an average of $142 per compromised record – of which $63 pertained to indirect costs including lost business due to abnormal turnover (churn) of existing and future customers.[27] Direct costs – which include detection, escalation, notification and ex-post response – were $79. Actual costs varied widely by country. The United States had the highest cost per compromised record, $204, followed by Germany at $177. The other countries had substantially lower costs – France at $119, Australia at $114 and the United Kingdom with the lowest at $98 per compromised record.

Data breach costs in countries with national data breach notification laws were significantly higher than in countries without such legislation. For example, in the United States, where 45 states have now introduced laws forcing organisations to publicly disclose the details of breach incidents, the cost per lost record was 43 percent higher than the global average. In Germany, where equivalent laws were passed part way through last year (in July 2009), costs were second highest, 25 percent above the worldwide average. In Australia, France and the United Kingdom, where these types of law have not yet been introduced, costs were all below the average. When breach notification laws are introduced across the rest of the world, other countries will follow the same pattern and costs will rise.

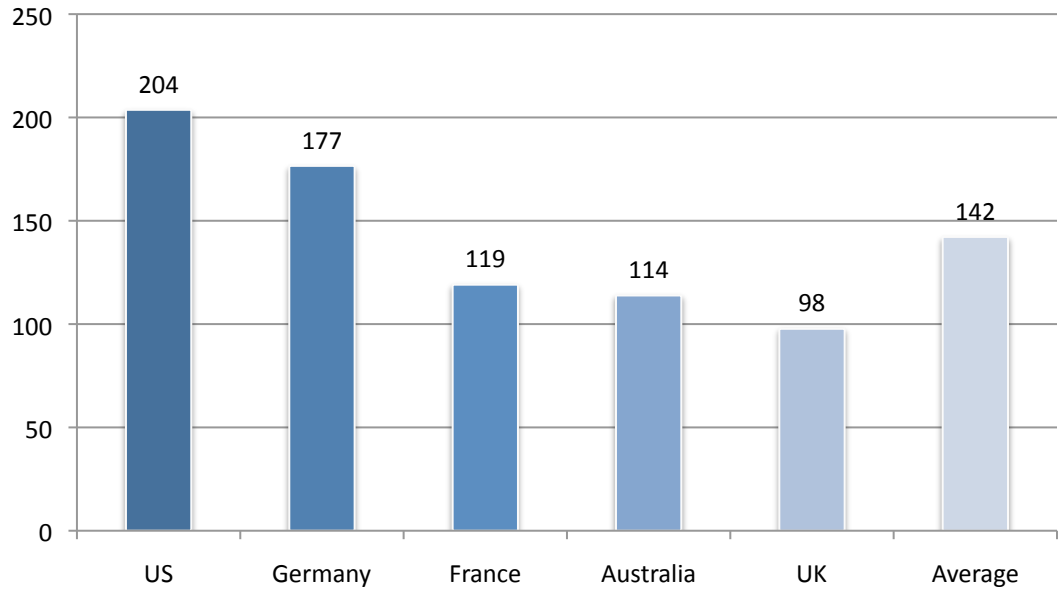

Figure 2: Average cost per record by country, 2009

[27] For purposes of comparability across different breach incidents, we measure data breach cost on a per compromised record basis.

Respondents devoted an average of 18 percent of total cost per record to detection and escalation. German respondents spent the most on detection and escalation, $52 per compromised record. German detection and escalation costs are much higher than in other countries because German organizations are much more focused on attacks to data and systems and thus have more security in place to mitigate risk. The high cost also reflects the investment required in new technologies and processes in order to comply with the country's recent notification legislation. Australia, France and the United Kingdom spent $38 per record, $36 per record and $18 per record, respectively. In the United States, where laws were first enforced in 2005, these costs were small by comparison ($8) and have decreased over recent years, suggesting that American organisations have developed more efficient detection and escalation processes over time. French, Australian and UK firms should expect their costs to follow the same trend: initially rising in order to ensure compliance with emerging regulations and then declining once processes become more refined.

Country	Cost of detection/escalation processes (USD)
Australia	38
France	36
Germany	52
UK	18
U.S.	8
Average	**31**

Table 3: Average per record cost of detection/escalation

Detection & escalation cost:
$1,000,000 omitted

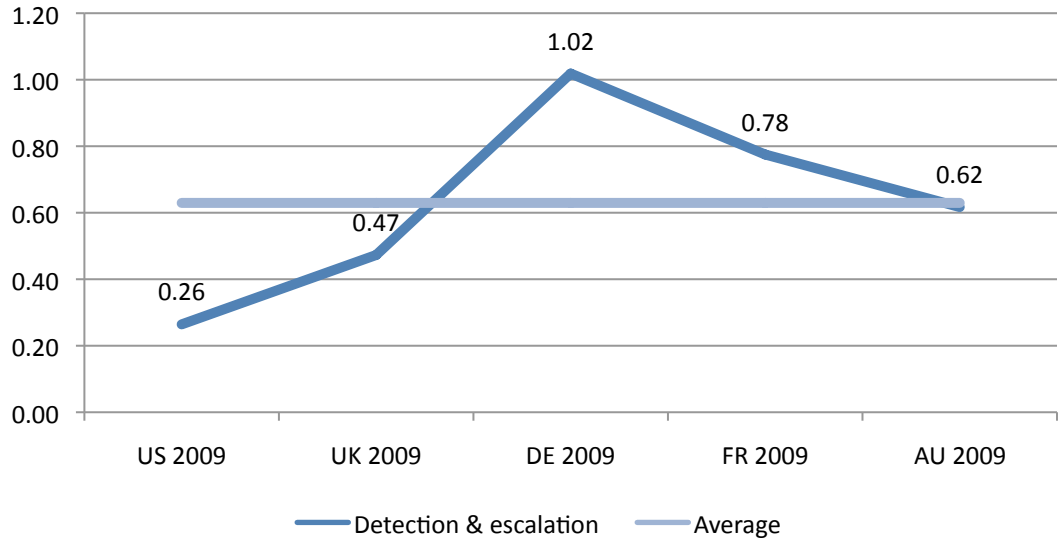

Figure 3: Detection & escalation cost – 2009

All countries surveyed spent the least on notification, spending on average only 7 percent of their total costs on it. US respondents had the highest notification cost, $15 per compromised record. The other four countries spent considerably less per record -- $10 in the United Kingdom, $9 in Germany, $6 in France and only $4 in Australia.

Notification cost:
$1,000,000 omitted

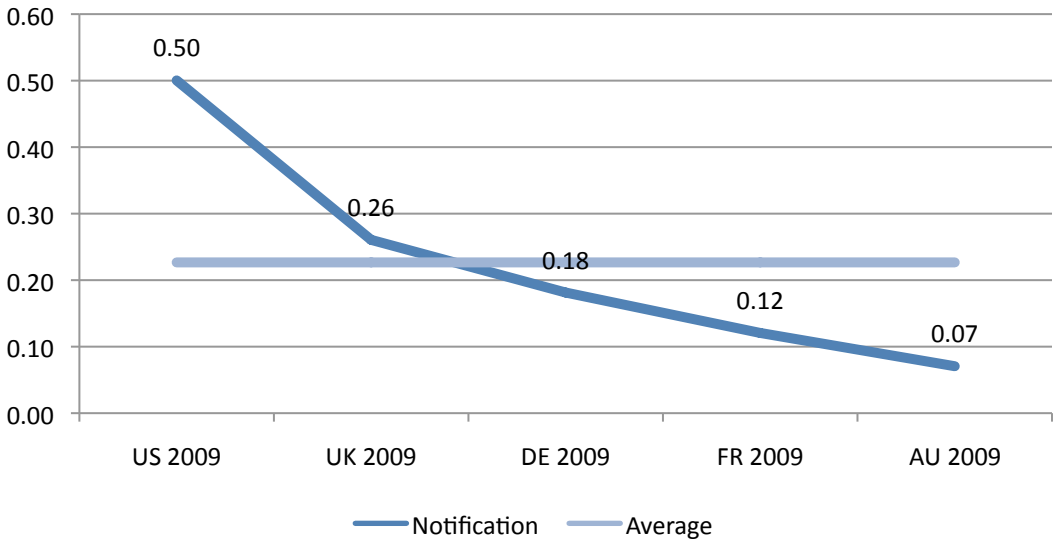

Figure 4: Average notification costs, 2009

The direct cost countries spent most on was ex-post response. On average, the five countries surveyed spent more than a quarter (27 percent) on ex-post response. Germany paid the most in average ex-post response costs per compromised record, $54, because Germans see data protection as a mark of an organization's trustworthiness and thus expect it to help them after a breach. The United States came in second at $46. France paid $41 per record, Australia $33 per record and the United Kingdom $25 per record.

Average ex-post response cost by country, 2009
$1,000,000 omitted

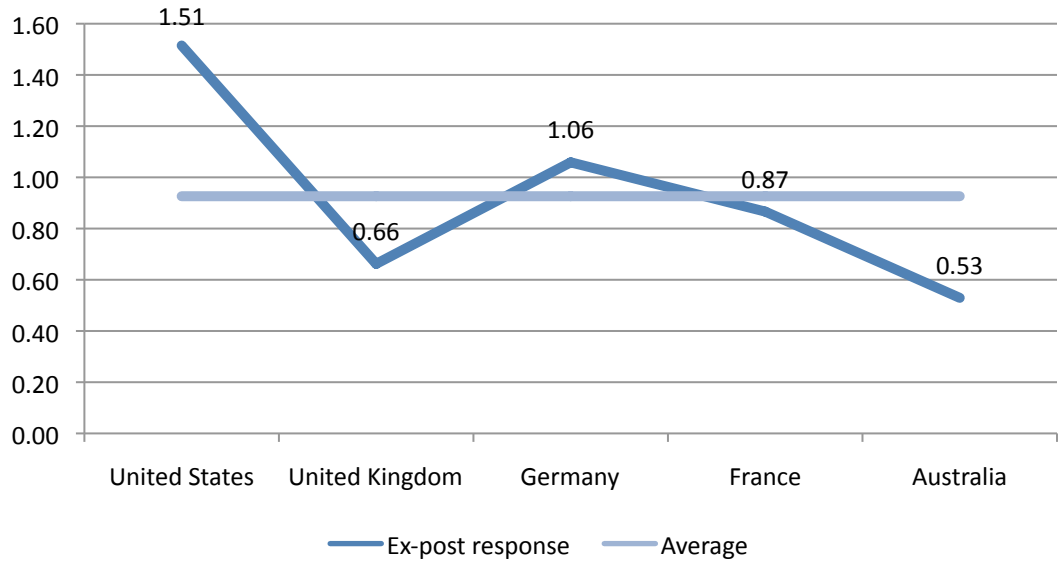

Figure 5: Average ex-post response cost by country, 2009

Data breaches diminish customer confidence and trust, and lead to abnormally high customer turnover (churn) and lost business that directly drive data breach costs. In this year's study, the average abnormal churn rate across all 133 incidents was 4 percent, which we measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). Almost half (44 percent) of the incurred data loss expenses related to the cost of lost business, reflecting the added expense of consumer churn and the increased difficulty of attracting new customers in the wake of negative publicity. Again, costs varied dramatically between countries and were highest in the United States, where the cost of lost business was on average equivalent to 66 percent of overall expenses. As more countries add data breach notification laws, their ability to keep breaches secret will diminish and their costs associated with churn and attracting new business will continue to grow.

Country	% cost caused by lost business
Australia	33%
France	30%
Germany	34%
UK	46%
U.S.	66%
Average	**44%**

Table 4: Percentage cost of lost business by country, 2009

Average lost business by country, 2009
$1,000,000 omitted

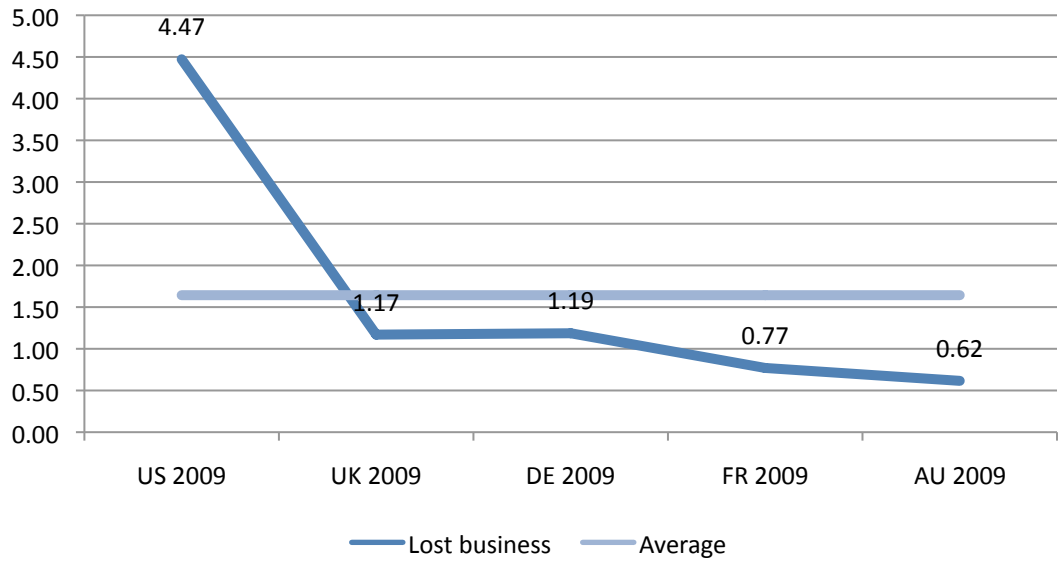

Figure 6: Average lost business by country, 2009

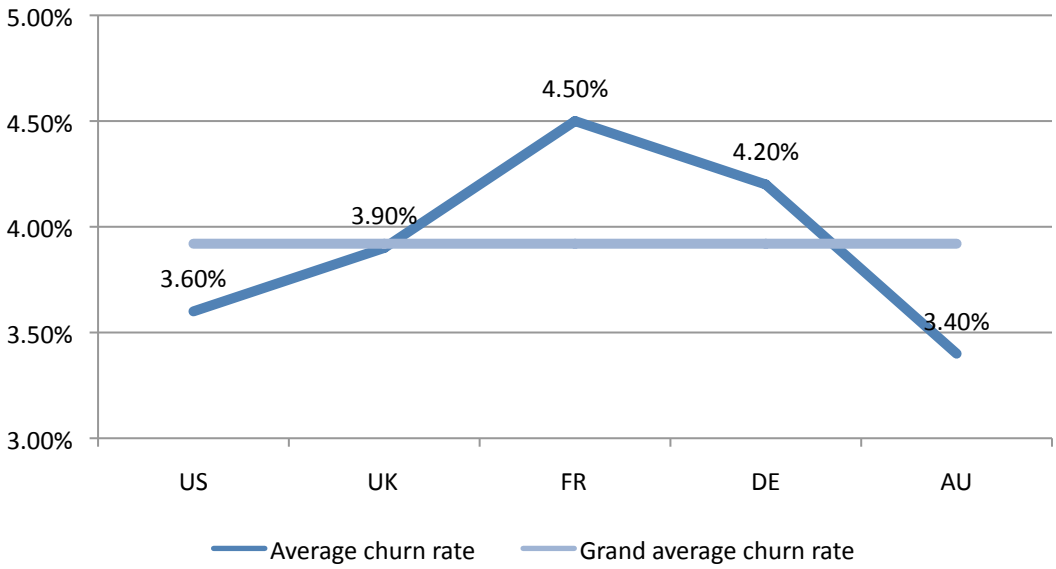

Figure 7: Comparison of average churn rates for five countries, 2009

Summary of per record cost by industry
Converted into $US dollars

Industry Classification	US	UK	FR	DE	AU
Automotive			150	201	
Communications	209	124	95	269	131
Consumer	159	69	98	171	119
Defense			290		
Education	203			204	
Energy	237				
Financial	249	131	187	207	165
Healthcare	294				
Hotel & Leisure	153		134	159	119
Manufacturing	136				
Media	149	83			169
Pharma	310	120	196		
Public sector		90	42	194	99
Research	266			262	
Retail	133	75	63	132	67
Services	256	100	147	141	
Technology	192	79	127	138	112
Transportation	121	140		340	67

Table 5: Summary of per record cost by industry, 2009

Converted into $US dollars

Five industries spanned all five country reports: financial, communications, technology, consumer and retail. Financial breaches had the highest average cost per compromised record ($188), followed by communications ($165), technology ($130), consumer ($123) and retail ($94). Countries with data breach laws had much higher costs – on average, US costs were 36 percent and German costs were 32 percent higher than the average. The other countries had substantially lower average costs – Australian costs were 16 percent lower, French costs were 20 percent lower and UK costs were 32 percent lower than the average.

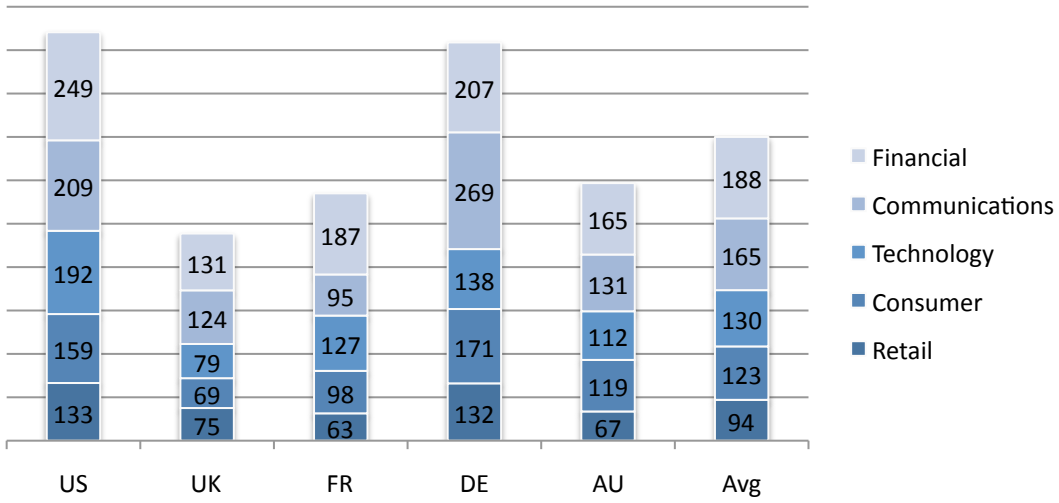

Figure 8: Per record cost for five industries, 2009
Converted into $US dollars

Please note that these five industries are fully represented in all 2009 country studies.

Thirty-six percent of all cases in this year's study involved a malicious or criminal attack that resulted in the loss or theft of personal information. Our research shows data breaches involving malicious or criminal acts were much more expensive than incidents resulting from every other factor except third-party flubs, which it almost matched. All countries reported strong to tremendous increases in costs from third-party incidents, with an average increase of 47 percent. Malicious or criminal attacks cost much more in countries without data breach notification laws. Malicious attacks increased the cost per compromised record the most in France (121 percent more) and Australia (61 percent more). By contrast, hostile attacks increased per-record costs only by 25 percent in the United Kingdom, 23 percent in Germany and a mere 7 percent in the United States. These findings suggest that organizations must start protecting themselves more proactively from increasingly aggressive malicious outsiders. Another explanation is that training and awareness programs are having a positive effect on insider threats to sensitive data.

Third-party flubs and malicious attacks are the most common and expensive breach types. Thirty-five percent of all cases in this year's study involved data breaches concerning outsourced data to third parties and 36 percent involved a malicious or criminal attack that resulted in the loss or theft of personal information. All countries reported strong to tremendous increases in costs from these causes, with an average per-record increase of 49 percent from third-party incidents and 47 percent from malicious attacks. The United States had the lowest increase from third-party mistakes, 12 percent, while France by far had the highest – 116 percent. The higher costs could be due to additional forensics investigation and consulting fees.

Country	% of breaches caused by criminal attack	% increase in cost
Australia	44	61
France	35	121
Germany	54	23
UK	24	25
U.S.	24	7

Table 6: Percentage of breaches caused by criminal attacks and their increase to overall cost, 2009

Country	% of breaches caused by third party	% increase in cost
Australia	31	39
France	41	116
Germany	27	31
UK	36	31
U.S.	42	12

Table 7: Percentage of breaches caused by third parties and their increase to overall cost, 2009

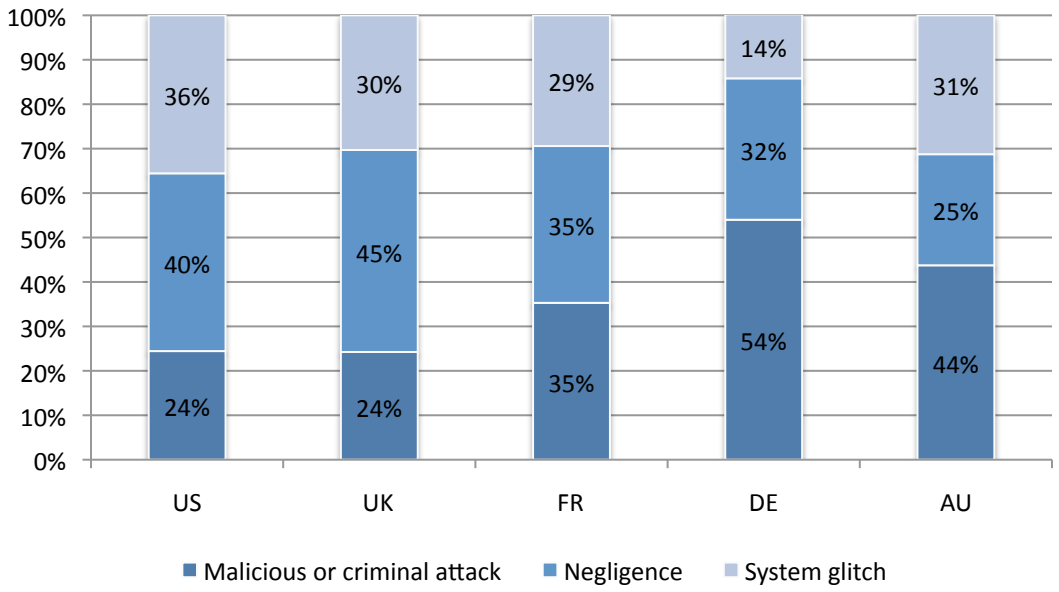

Figure 9: Primary cause of a data breach by country, 2009

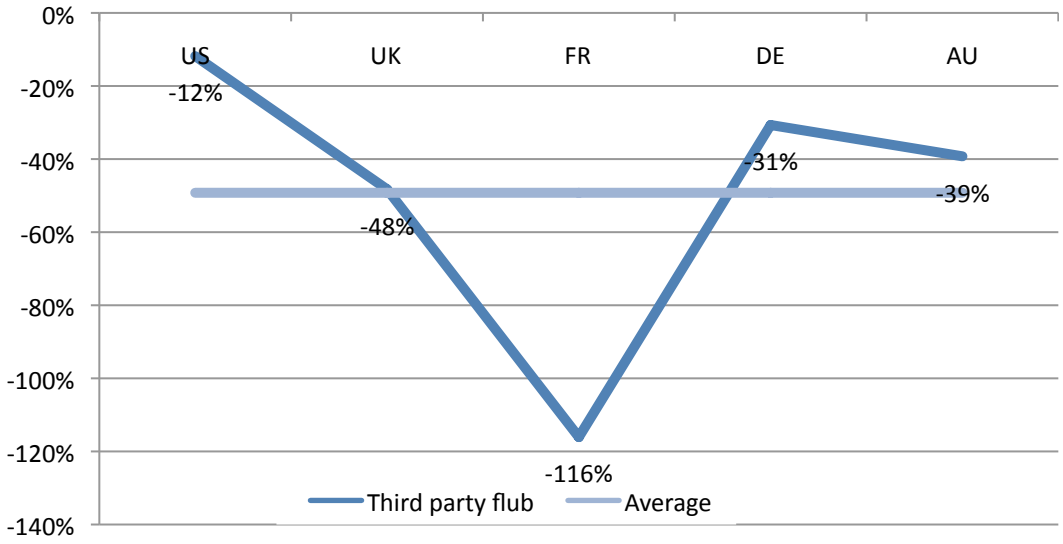

Figure 10: Third party flubs affect per record cost, 2009

A negative percentage indicates that third party mistakes increase the per record cost of data breach.

In 40 percent of participating companies, the CISO (or equivalently titled security executive) was in charge of managing the data breach incident. While other functional areas are typically involved in crisis management activities surrounding the data breach, our results suggest CISO leadership decreases the overall cost of data breaches. Across all five country studies, companies with a CISO (or equivalent title) who managed the data breach incident experienced an average cost per compromised record that was 21 percent lower compared to companies without such leadership. Benefits varied widely; Australian companies saw only a 3-percent decrease, while German companies saw their costs plummet 45 percent.

Country	% of breaches managed by CISO	% reduction in cost
Australia	44	3
France	41	12
Germany	36	45
UK	39	12
U.S.	40	33

Table 8: Percentage of breaches managed by CISO and their effect on cost of overall breach

A positive percentage indicates that CISO leadership decreases the per record cost of data breach

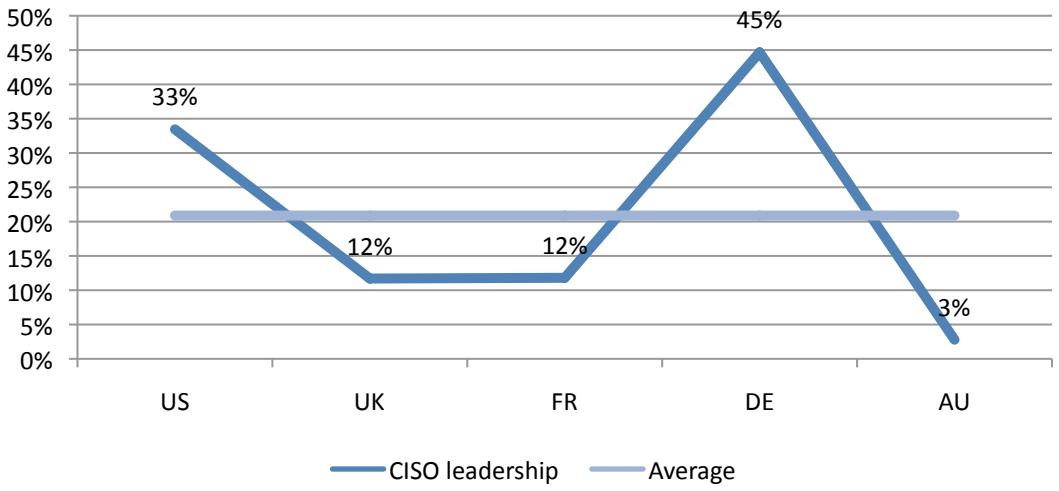

Figure 11: CISO leadership decreases the per record cost of data breach, 2009

Report Conclusions

The findings of this benchmark study suggest that more organisations in the five countries surveyed view data breaches as a fundamental and growing threat. The loss or theft of personal information requiring victim notification leads to significant direct and indirect costs, the biggest of which is abnormal customer turnover driven by diminished customer confidence. The public in these countries expects organisations that request or collect sensitive data to be good stewards of that data. Customers are increasingly willing to end or curtail relationships with organisations that experience breaches, making retaining customer trust a business imperative.

A key finding of this initial report is that data breach costs in countries with national data breach notification laws were significantly higher than in countries without such legislation. For example, in the United States, where 45 states have now introduced laws forcing organisations to publicly disclose the details of breach incidents, the cost per lost record was 43 percent higher than the global average. In Germany, where equivalent laws were passed part way through last year (in July 2009), costs were second highest, 25 percent above the worldwide average. In Australia, France and the United Kingdom, where these types of law have not yet been introduced, costs were all below the average. When breach notification laws are introduced across the rest of the world, other countries will follow the same pattern and costs will rise.

Data breaches are becoming a fact of life. 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 move toward data breach notification legislation that occurred in 2009 will create the desired long-term reductions of the incidence and severity of data breaches for organisations in the countries we studied.

In addition to major findings mentioned above, other key takeaways from the report include:

- **Breaches from employee negligence and systems glitches were common and were among the least costly.** Thirty-five percent of all cases in this year's study involved employee negligence and 28 percent involved a systems glitch. Negligence-related breaches were the least costly breach type in our study, averaging 25 percent less than other incidents. All countries studied saw much lower costs related to negligence, ranging from 19 percent in France to 35 percent in the United States. Systems glitch-related breaches were among the least costly of all breach types, with costs 15 percent lower on average than other types. The United Kingdom reported a marginal 1-percent increase due to glitches, while Germany, Australia and the United States saw costs 17 percent, 26 percent and 27 percent lower, respectively.

- **Data breaches involving lost or stolen laptop computers or other mobile data-bearing devices were a common and expensive form of data breach.** Thirty-two percent of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. All countries experienced noticeably higher data breach costs associated with these items, with an average of 22 percent and France seeing a 72-percent increase. The only exception was Germany, which saw its related costs drop by 10 percent.

- **Quick responders sometimes saved money and sometimes did not.** Thirty-seven percent of participating companies notified appropriate parties within one month of discovering the data breach (a.k.a. quick responders). Our findings suggest that companies that execute notification quickly can experience a much higher average cost per compromised record of data breach than companies that move more slowly. Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for organisations – especially during the detection, escalation and notification phases – which raised total costs by an average of 13 percent among respondents. Quick response ratcheted up data breach costs in the United States by 12 percent and in France by a whopping 112 percent. Conversely, it lowered costs in Australia by 16 percent, the United Kingdom by 18 percent and Germany by 23 percent.

- **Organisations with a better security posture had lower data breach costs than their less-prepared peers.** Forty-seven percent of participating companies achieved a security effectiveness score (SES) that was above the median value determined from benchmark results.[28] Those organisations with a more favorable security posture (SES above the median) experienced a slightly lower average cost per compromised record of data breach than organisations with an SES below the median. The beneficial effect varied by country but averaged 10 percent; the United States, Australia and France all saw decreases of 7 percent or less, while Germany had an 11-percent drop and the United Kingdom had a remarkable 29-percent decrease in costs.

- **Expanded use of encryption is the most popular preventive measure taken after data breaches.** On average, 47 percent of respondents indicated they used encryption to protect their data after a breach. Other popular preventive measures taken after data breaches were additional manual procedures and controls (46 percent) and training and awareness programs (44 percent). Other remediation procedures following the breach incident included: strengthening of perimeter controls (33 percent), data loss prevention (DLP) solutions (31 percent), endpoint security solutions (28 percent), identity and access management solutions (27 percent), and security certification or audit (25 percent). The least popular solutions were and security intelligence and event management (SIEM) systems (24 percent) and other system control practices (16 percent).

  To prevent future breaches, most UK, Australian and French companies prefer manual- and policy-based approaches over technological solutions. Although most US companies still prefer manual and policy solutions as post-breach remediation measures, many companies use enabling prevention and remediation technologies often and effectively. Most German organizations prefer technological solutions, especially encryption, as post-breach remediation measures. The new data breach notification legislation helped drive German organizations to embrace their faith in technology in general, but especially to known and trusted solutions.

  Because this is a benchmark study of 133 companies in five countries, we cannot generalise about the practices of all companies. However, a possible reason for the popularity of manual and policy-based solutions is that they may be faster to implement and are less expensive than technology solutions.

[28] The SES is a methodology developed by Ponemon Institute and PGP Corporation in 2005 for its annual encryption trends study. The SES measures the effectiveness of an organisation's security posture. Since its inception five years ago, this proprietary security scoring method has been used in more than 80 studies involving information security practitioners in organisations throughout the world.

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 manual and policy approaches may come first to mind for many companies, those approaches by themselves are not as effective as a multi-pronged approach that includes 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 of these technologies currently available 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 first annual report enables organisations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This 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 and other costs of preventing data breaches.

Companies should also consider following industry best practices, including:

- Companies should vet and evaluate the security posture of third parties before sharing confidential or sensitive information.

- To minimize customer churn (turnover), companies should draft communications that clearly define the issue and root cause of the breach incident. Whenever feasible, the company should take steps that minimize potential harm to data breach victims – for instance, the company may consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.

- When in doubt about requirements, companies should seek the counsel of consultants and legal experts to ensure the notification process complies with the plethora of national and European data breach notification laws.

- Companies should ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for people who travel extensively for business.

- Companies should 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.

- Companies should have a crisis management plan that clearly defines roles, responsibilities, procedures and timelines.

- Companies should discover ways to embrace technological solutions as well as manual and policy solutions.

- Finally, companies should 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 Ponemon Institute

Ponemon Institute© conducts independent research on consumer trust, privacy, data protection and emerging information security technologies. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of information. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

Our research has been used to set corporate privacy, data protection and security strategies for major organizations around the globe. Ponemon Institute's research services are engaged by organizations in the consumer products, software & technology, financial services, pharmaceutical, telecommunications, services, hospitality and governmental sectors, among others. We work closely with emerging technology firms that specialize in the data management and information security marketplace. Our research projects typically include benchmarking studies, customized research and strategy papers.

For more information, please 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 organisations 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 110,000 enterprises, businesses, and governments worldwide, including 87 percent of the Fortune® 100, 73 percent of the Fortune® Global 100, 80 percent of the German DAX index, and 60 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

Appendix A – Survey Methodology

Our 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 sample: The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of global organisations experiencing a breach involving the loss or theft of customer or consumer data over the past 12 month period.

  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 surveys. An initial invitation was sent to a targeted group of over 200 organisations, all known to have experienced a breach involving the lost or theft of customer or consumer data sometime over the past year. Over 100 organisations globally completed all parts of the benchmark survey. Non-response bias was not tested so it is always possible organisations 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 organisations being studied. It is our belief that the current sampling frame is biased toward organisations with more mature privacy or information security programs.

- Organisation-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, 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 survey research is based on the integrity of confidential responses received from organisations. While reliability checks were incorporated into the benchmark survey 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 survey 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 survey was privacy, data protection or compliance professionals responsible for managing the data breach incident. The survey required these practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a structured survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal churn rates that resulted from the breach event.

The survey 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 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 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 survey items was limited to known cost categories that cut across different industry sectors. We believed that a survey 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 survey, to provide greater assurances of confidentiality.

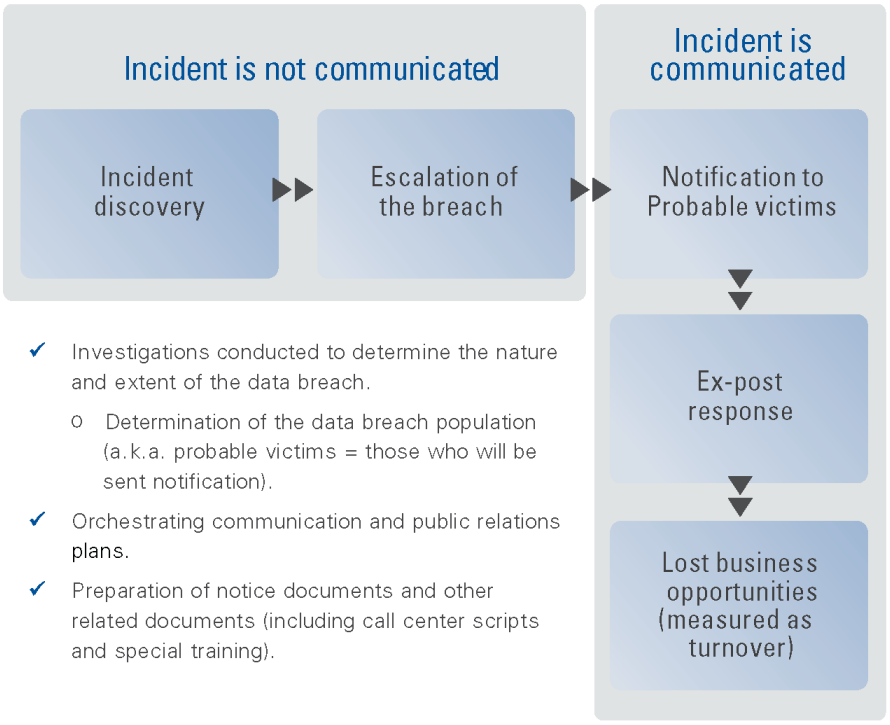

Figure 12: Visual representation of benchmark cost categories