2010 Annual Study:
U.S. Cost of a Data Breach

Compliance pressures, cyber attacks targeting sensitive data drive leading IT organizations to respond quickly and pay more

A benchmark study of 51 U.S. companies about the financial impact, customer turnover and preventive solutions related to breaches of sensitive information

March 2011

Research conducted by
Ponemon Institute, LLC

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

Table of Contents

Executive Summary

The Ponemon Institute proudly presents the *2010 U.S. Cost of a Data Breach*, the sixth annual study concerning the cost of data breach incidents for U.S.-based companies, sponsored by Symantec. Ponemon Institute research indicates that data breaches continue to have serious financial consequences on organizations. This year's report found that for the second year in a row, escalating data security threats and compliance pressures to combat them are driving more organizations to respond so rapidly to data breaches that they pay significantly higher costs.

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

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

The findings of this benchmark study pertain to the actual data breach experiences of 51 U.S. companies from 15 different industry sectors, all of which participated in the 2010 study. We believe the findings of this study are important because they can be generally applied to U.S. organizations that experience large data breaches (between 1,000 and 100,000 compromised records).

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

The report 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 analyze the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates.

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

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

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

We base our conclusion -- that anxieties about regulatory compliance and data breaches from cyber attacks may be driving many organizations to rush breach response and pay much more for it -- on key findings, including:

- For the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least common one
- Organizations are more proactively protecting themselves from malicious attacks
- Companies' investments in finding and remediating data breaches may be paying off
- For the third straight year, direct costs accounted for a larger proportion of overall data breach costs

2010 Annual Study: Cost of a Data Breach

This 2010 Ponemon Institute benchmark study, sponsored by Symantec Corporation, examines the costs incurred by 51 organizations 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 sixth annual study of this issue.

Breaches in the study ranged from nearly 4,200 records to 105,000 records from 15 different industry sectors.

What we learned from the 2010 results:

Top Findings

More organizations favor rapid response to data breaches, and that is significantly costing them: Forty-three percent of companies notified victims within one month of discovering the data breach, up 7 points from 36 percent last year. That growth marks the largest percent increase among data breach response attributes. For the second year in a row, these "quick responders" paid significantly more per record than companies that moved more slowly. In 2010, quick responders had a per-record cost of $268, up $49 (22 percent) from $219 the year before. Companies that took longer paid $174 per record, down $22 (11 percent) from 2009.

Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for the organization, especially during the detection, escalation and notification phases. The notable increase in companies responding quickly to breaches, despite the additional cost, may reflect pressure companies feel to comply with commercial regulations and state and federal data protection laws. We will closely watch this issue in future reports.

For the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least common one: Nearly a third (31 percent) of all cases in this year's study involved a malicious or criminal attack. That figure is up 7 points from 2009 after having doubled the year before and marks the first time malicious attacks were not the least common cause for breaches. Breach costs for malicious attacks skyrocketed: The 2010 cost per compromised record of a data breach involving a malicious or criminal act averaged $318, up $103 (48 percent) from 2009 and the highest of any data breach cause this year. The huge increases reinforce the extreme danger hostile breaches pose.

Organizations are more proactively protecting themselves from malicious attacks: Of the various causes of data breaches, malicious or criminal attacks increased the most in 2010. For the first time, malicious or criminal attacks are no longer the least common breach cause.

At the same time, three response characteristics increased in frequency: the number of organizations responding quickly (within 30 days), those putting CISOs in charge of data breach response, and those with an above-average IT security posture. Taken together, these figures may indicate more organizations are taking more active steps to thwart hostile attacks. Moreover, breaches due to systems failures, lost or stolen devices and third-party mistakes all fell. All these point to companies becoming more conscientious about preventing data breaches in the worsening threat environment.

These figures correspond with findings from the *2010 Annual Study: U.S. Enterprise Encryption Trends* report, also conducted by the Ponemon Institute and sponsored by Symantec.[1] Namely, the report found that protecting against viruses, malware, and spyware infection has become organizations' No. 1 data protection priority. Nearly all respondents (97 percent) considered cyber attacks as the most severe threat to their ability to carry out their missions. Moreover, the report also found that 88 percent of organizations surveyed had at least one data breach, up slightly from 2009.

[1] *2010 Annual Study: U.S. Enterprise Encryption Trends*, The Ponemon Institute, November 2010

Companies’ investments in finding and remediating data breaches may be paying off: Both detection and escalation and ex-post response have posted significant double-digit cost increases for the past five years. In particular, increases in legal defense costs remain a main reason for increased spending in ex-post response, as companies fear successful class action lawsuits by breach victims.

Companies may be doing the right things to allay that fear. The cost of lost business stayed relatively stable at around $4.5 million for the third straight year. In that time, lost business has decreased proportionally to overall data breach costs; in 2010, it accounted for 63 percent of the total cost, down 3 percent from 2009 and 6 percent from 2008. The decrease in spending on lost business closely matches the amount spent on detection and escalation and ex-post response.

This data appears to support the major finding from the *2010 Enterprise Encryption Trends* study: 2010 marked the first time that regulatory compliance surpassed data breach mitigation as the main driver behind the implementation of encryption technologies (and, by extension, other data protection technologies). Compliance with data protection regulations requires organizations to do more to find, disclose and fix breach-related problems. These tasks correspond with the detection and escalation, notification and ex-post response cost activities, respectively. Strong growth in both detection and escalation and in ex-post response could reflect increased compliance activities, as those two stages often require more investment than the notification process.

For the third straight year, direct costs accounted for more of overall data breach costs: Direct costs rose 5 points to 34 percent this year, while indirect costs dropped the same amount to 66 points. While indirect costs still outweigh direct costs by nearly two to one, this study data reinforces the trend started in 2008 of direct costs comprising a larger fraction of overall spending. In 2010, direct costs accounted on average for $73 (34 percent) of the total average cost, up $13 (22 percent) from 2009. Increased legal defense costs remained the primary driver for the increases. At the same time, indirect costs continued their slow decline; this year’s average of $141 was down $3 (2 percent) from 2009.

The sharp growth in direct costs and slight but persistent decrease in indirect costs over the past three years may indicate that companies are taking their response to data breaches more seriously than ever. Organizations’ efforts to repair the damage breaches cause may be slowly building customer and partner confidence, lowering the number of present and potential customers who take their business elsewhere after a breach. These results may also bolster the argument that organizations are focusing more on regulatory compliance, as direct costs correspond to the cost activities covered by data protection regulations (detection and escalation, notification and ex-post response).

Overall Trends

Breach costs directly reflect IT security best practices and threat trends: One of the most consistently striking trends in the U.S. study year after year is that data breach costs more or less correlate directly with the presence or absence of major data breach causes (malicious attacks, for example) or data protection best practices (such as CISO leadership). Specifically, 2010 costs for breaches involving all major causes (malicious or criminal attacks, negligence and systems failures, as well as first timers, lost or stolen devices and third-party mistakes) grew between 15 and 48 percent from 2009. Conversely, breaches that lacked those factors or illustrated best practices dropped even more precipitously to take the bottom rankings. These breach types saw their costs drop between 1 percent and 27 percent. These figures may indicate that organizations’ data breach costs stayed relatively stable or only increased a small amount in most cases. The exception was the top six breach causes and especially the top three, which saw by far the greatest rises.

For the fifth year in a row, data breach costs have continued to rise: Data breaches continue to cost organizations more every year. The average organizational cost of a data breach this year increased to $7.2 million, up 7 percent from $6.8 million in 2009. Total breach costs have grown every year since 2006. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year.

Data breaches are costing more at both ends of the scale, but particularly the top. The most expensive data breach included in this year’s study cost a company $35.3 million to resolve, up $4.8 million (15 percent) from last year. The least expensive data breach was $780,000, up $30,000 (4 percent) from 2009. As in prior years, data breach cost appears to be directly proportional to the number of records compromised. Therefore, larger breaches continue to be a more serious cause for concern than smaller breaches.

Customer turnover in direct response to breaches remains the main driver of data breach costs: For the second straight year, abnormal churn or turnover of customers after data breaches appears to be the dominant factor in data breach cost. Regulatory compliance contributes to lower churn rates by boosting customer confidence in organizations' IT security practices. Average abnormal churn rates across all 51 incidents stayed level at 4 percent. The industries with the highest 2010 churn rate remained pharmaceuticals and healthcare (both up a point to 7 percent). The industries with the lowest abnormal churn rates were public sector (less than 1 percent) and retail (1 percent). Sectors with the highest 2010 average per-record costs were communications ($380), financial ($353) and pharmaceutical ($345). Those with the lowest costs were media ($131), education ($112), and public sector ($81).

Training and awareness programs remain the most popular post-breach remedies, but encryption and other technologies are gaining fast: Training and awareness programs barely stayed in first place with nearly two-thirds (63 percent, down 4 points) of respondents using them. Expanded use of encryption stayed the most popular technology solution and, with 61 percent (up 3 points), took sole possession of second place this year. Interestingly, since 2008, technological solutions have seen the strongest growth while personnel and policy solutions have grown more slowly. Taken together, these figures may indicate that companies continue to rely upon educating their workforce and enabling it to personally help stop future data breaches. At the same time, though, companies are increasingly aware of, and willing to implement, technological solutions to help prevent and mitigate breaches.

Data Breach Types – Cause[2]

Breaches by third-party outsourcers are becoming slightly less common but much more expensive: Third-party mistakes continued their slight decline in 2010 to 39 percent. The cost of such breaches rose significantly, however, up $85 (39 percent) to $302 per record. These figures may indicate that compliance with government and commercial regulations for data protection are dramatically raising breach costs involving outsourced data.

Breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat: The prevalence of breaches concerning mobile devices holding sensitive data stayed roughly the same at 35 percent this year, down a point. Per-record costs rose $33 (15 percent) to $258 per record. Our research suggests that device-oriented breaches have consistently cost more than many other breach types. This may be because investigations and forensics into lost or stolen devices are more difficult and costly.

Companies are more vigilant about preventing systems failures: The number of breaches caused by systems failures dropped 9 points in 2010 to 27 percent. Breaches from systems failures averaged $210, up $44 (27 percent). The noticeable drop in breaches from systems failures may point to organizations becoming more conscientious in ensuring their systems can help prevent and mitigate breaches (through new security technologies and/or compliance with security policies and regulations).

Negligence remains the most common threat, and an increasingly expensive one: The number of breaches attributed to negligence edged up a point to 41 percent. Breaches from negligence in 2010 averaged $196 per record, up $42 (27 percent) from 2009. The relatively stable incidence of negligence may indicate that ensuring employee and partner compliance remains an ongoing challenge. These figures may reflect the growing prevalence and cost of malicious breaches, as well as organizations' growing competency in handling breaches from systems failures and negligence.

Data Breach Types – Response[3]

"First timers" pay the highest breach costs: One in five (20 percent) of respondents in 2010 faced their first data breaches involving the loss or theft of more than 1,000 records containing personal information. That figure stayed

[2] Causes also include malicious or criminal attacks discussed in the Top Findings.
[3] Response also includes quick responders discussed in the Top Findings.

relatively level. Although rare, these “first timers” paid the highest average costs of anyone in the 2010 study. This year, the cost per compromised record of an organization’s first data breach averaged $326 (up $98 or 43 percent). These findings may indicate that attacks are becoming more insidious and damaging, which would require greater resources to combat. First timers often lack breach response experience that can help lower costs.

To better manage data breaches and reduce breach costs, more companies are trusting their CISOs: Forty-five percent of respondents had a CISO (or equivalent title) manage data breaches, up 5 points from 2009. Breach response costs involving CISO leadership rose $36 (23 percent) to $193 per record. This year’s results may indicate that more companies see CISO leadership as an essential part of their data breach prevention and mitigation efforts.

Fewer organizations are using external consulting support, even though such support lowers data breach costs: The proportion of respondents that engaged outside consultants fell 7 points this year to 37 percent. Breaches with external consulting support rose $21 (12 percent) to $191. The noticeable drop in the use of external consulting support may be tied to the finding above that more organizations are responding quickly to breaches. Organizations in a rush to respond may not believe they have the time to bring in outside help to meet compliance requirements. This in turn could help explain the increase in popularity of relying on CISOs, as organizations can quickly leverage these internal resources and see similar cost benefits.

More companies had better-than-average security postures, and those organizations enjoyed much lower data breach costs: Forty-five percent of respondents had a Security Effectiveness Score (SES) above the median value determined from benchmark results.[4] That figure is up 3 points from 2009. As expected, organizations with a more favorable security posture (SES above the median) experienced a lower average cost per record than those with an SES below the median. Accordingly, organizations above the median had an average cost per compromised record of $147, $55 (27 percent) less than last year. More companies may be exceeding the SES median because they are strengthening their IT security posture as part of their efforts to meet regulatory compliance requirements.

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

Suggested Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organizations 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 organization 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

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

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

Next Steps

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

- Take as slow and thoughtful an approach to data breach response as possible, given federal and state legal requirements applicable to location, industry and circumstances of the breach. Prepare in advance as much as possible to enable quick and cost-effective response.

- Ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for extensive business travelers. Also, consider implementing inventory control, anti-theft devices and data loss prevention (DLP) policies, practices and technologies.

- Vet and evaluate the security posture of third parties before sharing confidential or sensitive information. Pick responsible vendors that can guarantee data protection through encryption and appropriate procedures and controls. Also, ensure that third parties protect data on their employees' mobile devices.

Introduction

Government, industry and the American public in 2010 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. One series of breaches, however, made global headlines and made data security a front-burner issue: WikiLeaks.

WikiLeaks, an international nonprofit organization specializing in publishing anonymously submitted material, between April and December 2010 released hundreds of thousands of sensitive and classified U.S. military, diplomatic and government documents. The Pentagon declared that 400,000 documents pertaining to U.S. military involvement in Afghanistan, the Iraq War Logs, were the largest leak of classified documents in U.S. military history.[5] Even as the organization drew praise for increasing the transparency and accountability of the U.S. and other governments, it also received harsh condemnation for putting classified information, national security and international diplomacy at risk.

WikiLeaks' numerous announcements over the year hammered home the dangers all organizations – public and private, U.S. and international – face from unauthorized access and dissemination of sensitive data. The leaks also underscored how the same data protection principles apply to government and private sector alike. The scale of the problem is gargantuan: In the United States alone, more than 2,300 breaches have put more than 512 million records at potential risk between 2005 and 2011.[6] In 2010, nearly 600 breaches put more than 12 million records in jeopardy.

The twin onslaughts of data breaches and cyber attacks have caused regulators to crack down on organizations to ensure they implement required data security controls or face harsher penalties. A common realization is growing across all industry sectors that the only way to effectively counter these threats is a holistic risk management approach to IT security.

In addition to these threats, the Great Recession of 2008 has forced many U.S. companies to reduce costs and improve efficiencies, leading to increased use of outsourcers, mobile technologies and application delivery models such as cloud computing. A major side effect of moving so much data off in-house IT networks is that organizations must take more responsibility for protecting their data wherever it is – especially when that data is in third-party hands.

The WikiLeaks breaches augmented public and government attention to cybersecurity, which drove Congress to make further progress on a national data breach notification law that would standardize data breach protections nationwide. Discussions continued on three bills introduced in 2009: The Data Accountability and Trust Act (DATA) (HR 2221), the first data breach notification bill passed by the U.S. House of Representatives; the Personal Data Privacy and Security Act (S. 1490); and the Data Breach Notification Act (S. 139).

This year saw additional and potentially more sweeping bills put on the table. Senators introduced the Data Security Act of 2010 (S. 3579) and the Data Security and Breach Notification Act of 2010 (S. 3742), a companion bill to HR 2221. In the House, the Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act (HR 5777) offered stronger restrictions concerning the release of personal information to third parties, as well as providing other protections.

Republican victories in the 2010 elections returned the House of Representatives to GOP control. Some industry experts said that competing interests in a divided Congress could hinder the passage of comprehensive cybersecurity legislation, including data breach notification. A specific and scaled-down data breach notification bill, however, might yet see approval in 2011.[7]

[5] "U.S. says it did not under-report Iraq civilian deaths," Phil Stewart and Andrea Shalal-Esa, Reuters, Oct 25, 2010 http://www.reuters.com/article/2010/10/25/us-wikileaks-iraq-idUSTRE69L54J20101025

[6] *Chronology of Data Breaches*, Privacy Rights Clearinghouse, Jan 2011 www.privacyrights.org/data-breach

[7] "Congress May Be Able to Tackle Tech Issues in 2011," Grant Gross, IDG News, Jan 11, 2011 http://www.pcworld.com/businesscenter/article/216444/congress_may_be_able_to_tackle_tech_issues_in_2011.html

Lawmakers in at least 18 states introduced security breach legislation in 2010[8]. Since 2004, 46 states[9] 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 human error, technology problems, or malicious acts.

Although the specific conditions for notification vary by state, organizations may not be required to notify individuals 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 organization’s reputation. But when organizations experience data breaches and must notify customers or clients, what costs do they encounter as they attempt to recover?

The Ponemon Institute and Symantec Corporation are pleased to offer the sixth annual study that quantifies the actual costs incurred by 51 organizations compelled to notify individuals of data privacy breaches. Summarized in this document, the study provides detailed information from responses to questions organizations face when responding to data breaches:

- 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?

This report reveals how much companies pay for each kind of data breach studied. We track how much organizations can save if they follow best practices and avoid major causes of breaches. We look into how much those savings have changed from earlier studies. Finally, we discuss what caused the changes and what those causes mean to organizations in an evolving data protection environment.

[8] National Conference of State Legislatures, Security Breach Legislation 2010: http://www.ncsl.org/default.aspx?tabid=20100

[9] National Conference of State Legislatures, State Security Breach Notification Laws as of October 12, 2010: http://www.ncsl.org/default.aspx?tabid=13489

Study Overview & Methodology

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

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

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

The findings of this benchmark study pertain to the actual data breach experiences of 51 U.S. companies from 15 different industry sectors, all of which participated in the 2010 study. We believe the findings of this study are important because they can be generally applied to U.S. organizations that experience large data breaches (between 1,000 and 100,000 compromised records).

- Fieldwork for this research commenced in March 2010 and continued until the end of December 2010.
- The Ponemon Institute invited more than 400 organizations to participate; all invited organizations were known to have experienced a breach sometime in 2010. The breaches involved the loss or theft of personal customer, consumer or student data and required notification according to U.S. state laws.
- Of that group, 51 companies agreed to participate by completing the study. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from actual incidents.
- All organizations voluntarily agreed to participate with the promise of complete confidentiality and anonymity.
- The reported number of individual records breached ranged from nearly 4,200 to 105,000 records from companies in 15 different industry sectors.
- The 2010 study shows that 39 percent of breaches occurred due to external causes, down 3 points from 2009 and 5 points from 2008. A third-party breach is defined as a case where a third party (such as professional services, outsourcers, vendors, business partners) possessed and was responsible for protecting the data. In comparison, an in-house breach is defined as a case where the organization itself was responsible for protecting the data.

Study Methodology

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

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

- Ex-post response: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harm. Redress activities also include ex-post response such as credit report monitoring or the reissuing of a new account or credit card.

In addition to the above process-related activities, most companies experience opportunity costs associated with a breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our research shows that the negative publicity associated with a data breach incident can often damage companies' reputations and may lead to abnormal turnover, or churn, rates and a diminished rate for new customer acquisitions.

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

- 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 organization 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 organization's churn or turnover rates directly.

Key Report Findings

For the fifth year in a row, data breach costs have continued to rise: Data breaches continue to cost organizations more every year. The average organizational cost of a data breach this year increased to $7.2 million, up 7 percent from $6.8 million in 2009 and 9 percent from $6.7 million in our 2008 study. Data breaches in 2010 cost their companies an average of $214 per compromised record, up $10 (5 percent) from last year and $12 (6 percent) from 2008.

Total breach costs have grown every year since 2006. Data breaches are costing more at both ends of the scale, but particularly the top. The most expensive data breach included in this year's study cost a company $35.3 million to resolve, up $4.8 million (15 percent) from last year. The least expensive data breach was $780,000, up $30,000 (4 percent) from 2009.

Breach size this year ranged from nearly 4,200 to 105,000 lost or stolen records. As in prior years, data breach cost appears to be directly proportional to the number of records compromised. Therefore, larger breaches continue to be a more serious cause for concern than smaller breaches.

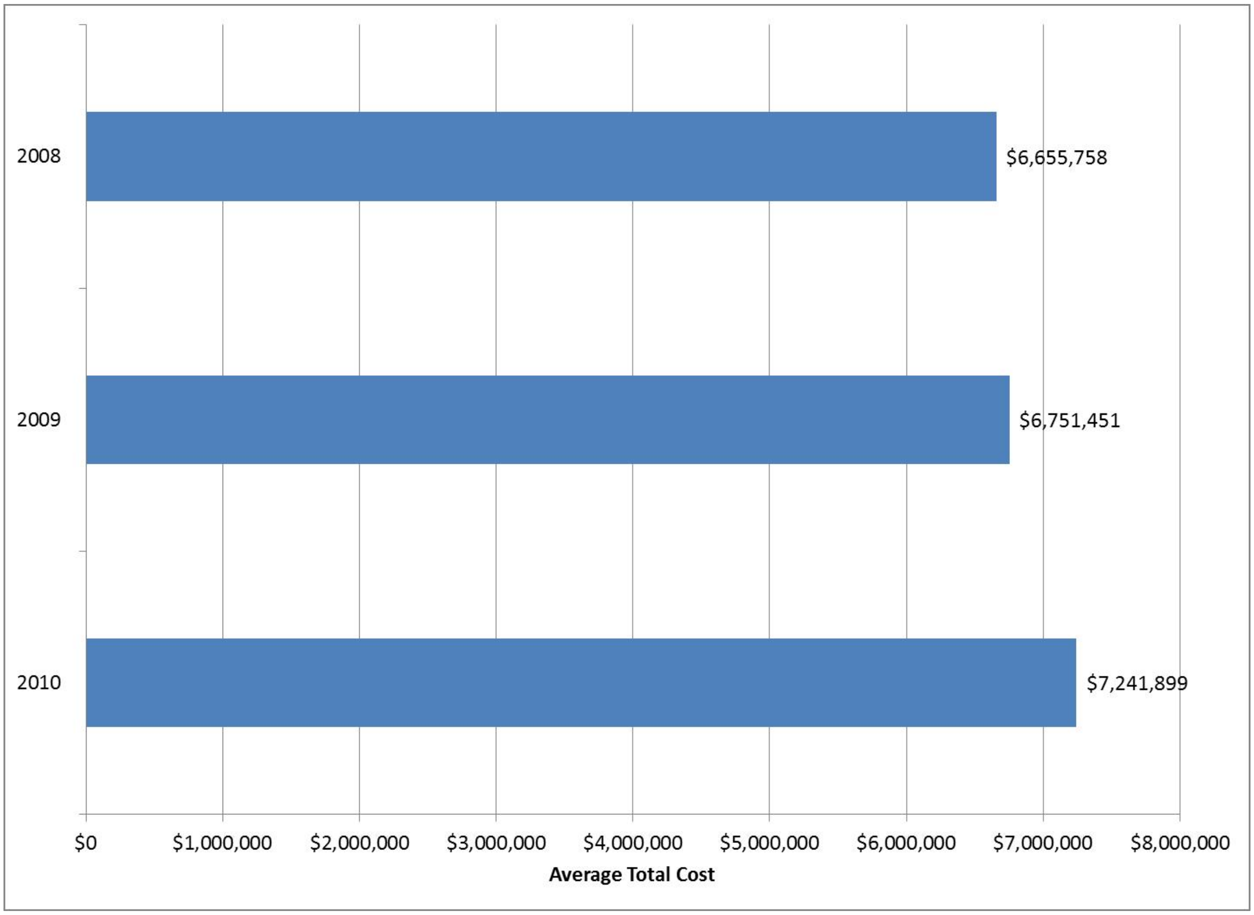


Figure 1: Average organizational cost of a data breach, 2008-10

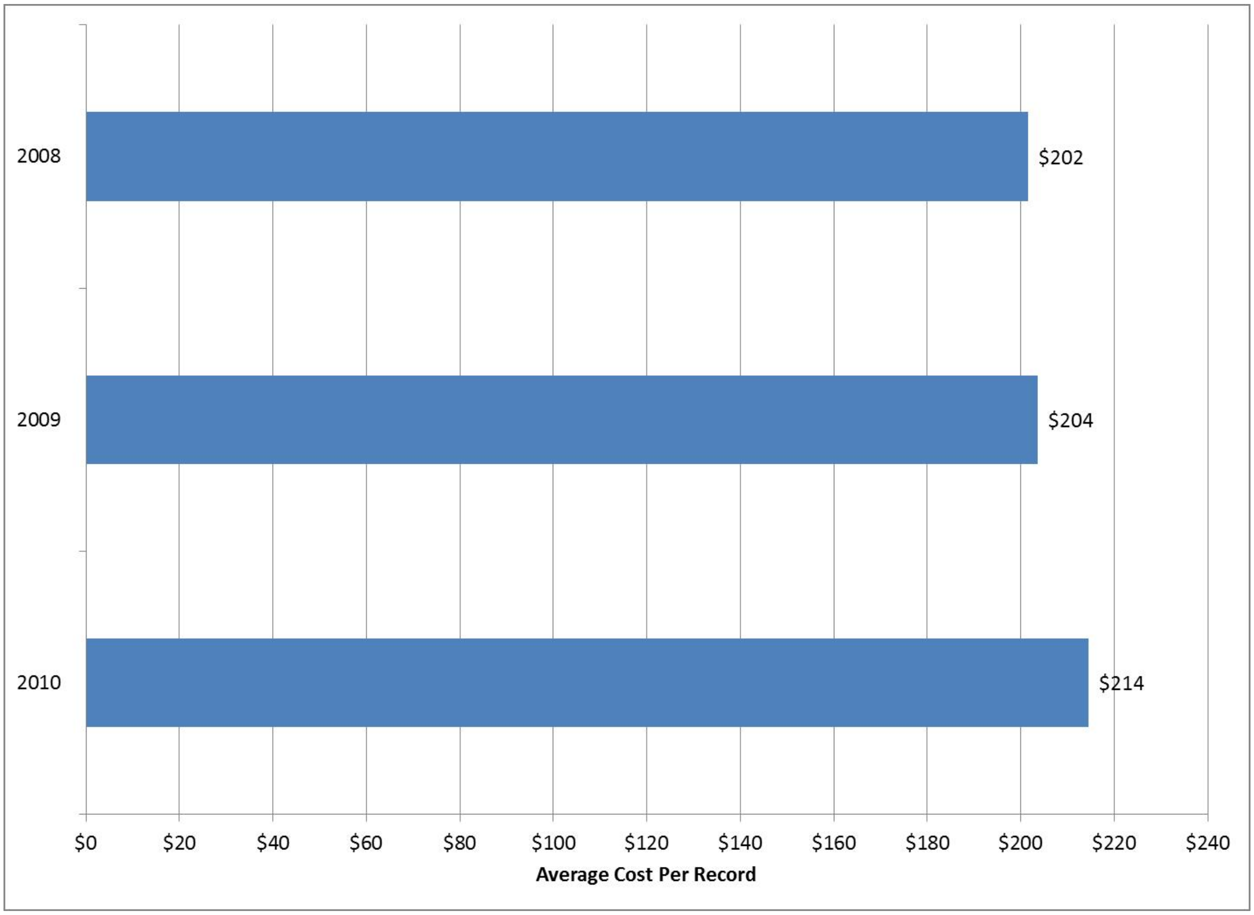
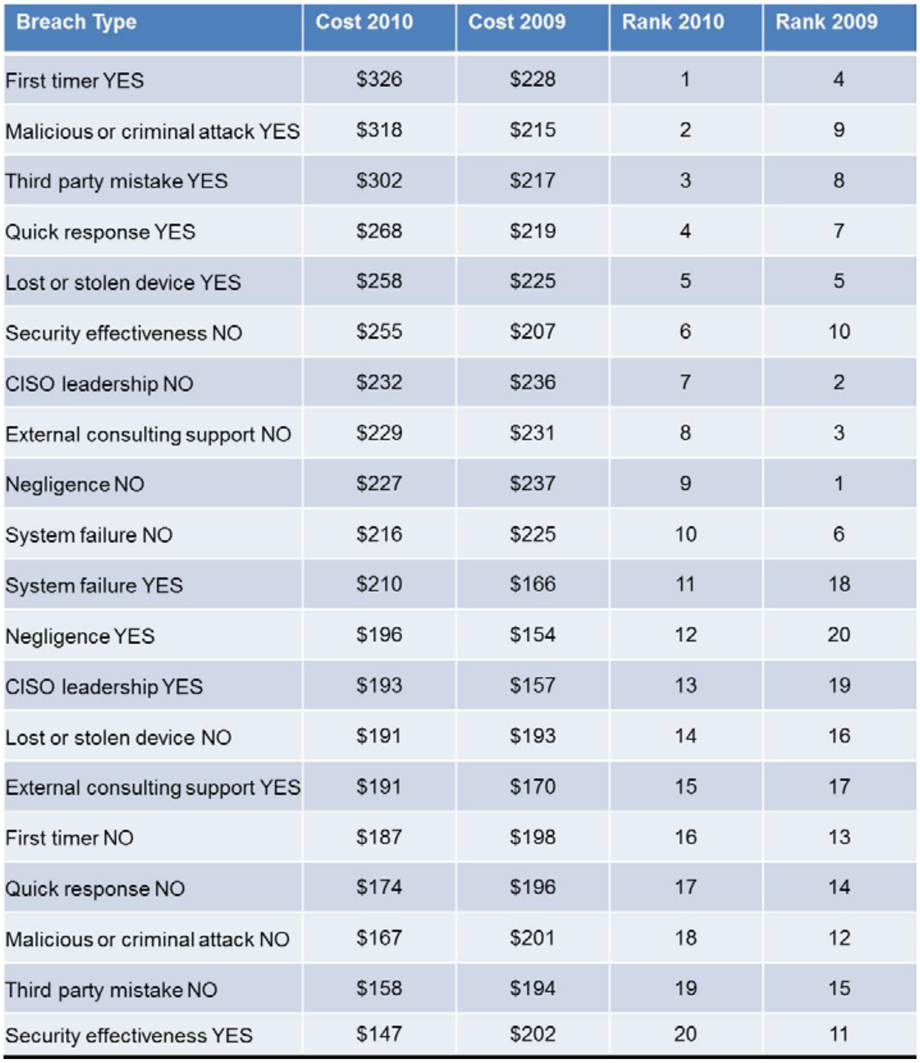


Figure 2: Average cost per record of a data breach, 2008-10

Breach costs directly reflect IT security best practices and threat trends: This year's list of most expensive data breach types reads like a rogues' gallery of major data protection threats appearing daily in news headlines. One of the most striking trends in the U.S. study year after year is that data breach costs more or less correlate directly with the presence or absence of major data breach causes (malicious attacks, for example) or data protection best practices (such as CISO leadership). Specifically, breaches including the presence of major causes and absence of best practices rose significantly in 2010 to dominate the top rankings. The opposite was also true: organizations that avoided problems and ensured they had the right support inside and out fared much better.

These figures may indicate that organizations that follow data protection best practices can greatly decrease their potential data breach costs. Another possible conclusion is that lack of experience and/or thoughtful response to breaches can also significantly increase response costs.

What's more, costs for breaches involving all major causes (malicious or criminal attacks, negligence and systems failures, as well as first timers, lost or stolen devices and third-party mistakes) grew between 15 and 48 percent from 2009. Conversely, breaches that lacked those factors or illustrated best practices dropped even more precipitously to take the bottom rankings. These breach types saw their costs drop between 1 percent and 27 percent.



Breach Type	Cost 2010	Cost 2009	Rank 2010	Rank 2009
First timer YES	$326	$228	1	4
Malicious or criminal attack YES	$318	$215	2	9
Third party mistake YES	$302	$217	3	8
Quick response YES	$268	$219	4	7
Lost or stolen device YES	$258	$225	5	5
Security effectiveness NO	$255	$207	6	10
CISO leadership NO	$232	$236	7	2
External consulting support NO	$229	$231	8	3
Negligence NO	$227	$237	9	1
System failure NO	$216	$225	10	6
System failure YES	$210	$166	11	18
Negligence YES	$196	$154	12	20
CISO leadership YES	$193	$157	13	19
Lost or stolen device NO	$191	$193	14	16
External consulting support YES	$191	$170	15	17
First timer NO	$187	$198	16	13
Quick response NO	$174	$196	17	14
Malicious or criminal attack NO	$167	$201	18	12
Third party mistake NO	$158	$194	19	15
Security effectiveness YES	$147	$202	20	11

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

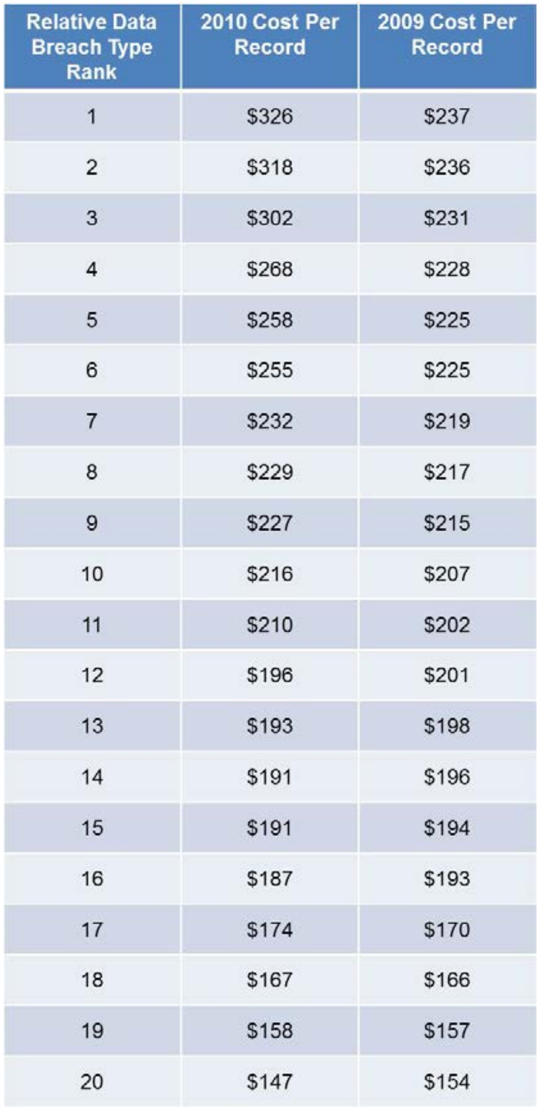
Note: Data breach types are categorized by whether the breach involved a specific attribute (e.g. First timer YES) or all other breach types not involving that attribute (e.g. First timer NO).

In this year's rankings, 10 breach types rose in the rankings, nine fell and one (experiencing the loss or theft of a device bearing sensitive data) stayed the same. Of the 20 ranks, 14 had higher costs per record in 2010 than in 2009 and six had lower costs. First timers rose three spots to first place, malicious or criminal attacks leaped seven spots to second place, third-party mistakes jumped five spots to third place and quick response rose three spots to fourth.

Interestingly, breaches involving negligence and systems failures rose the most in 2010 – up eight slots and seven slots, respectively. These impressive leaps moved these breach types from the bottom rankings to the middle of the pack. These figures may indicate that companies are taking both breach types more seriously but recognize that other factors – especially malicious or criminal attacks and third-party mistakes – warrant much more concern.

From 2009 to 2010, the highest average per record costs companies experienced increased by $89 (37 percent), from $237 to $326. The three most costly breach types in 2010 were each more than 30 percent higher than in 2009. These three represented three of the most pressing concerns companies face regarding data breaches: being a first-time breach victim, protecting against malicious and criminal attacks and preventing third-party mistakes.

By contrast, the least expensive breach in 2010 was only $7 (5 percent) cheaper than in 2009, from $154 to $147. These figures may indicate that organizations' data breach costs stayed relatively stable or only increased a small amount in most cases. The exception was the top six breach causes and especially the top three, which saw by far the greatest increases.



Relative Data Breach Type Rank	2010 Cost Per Record	2009 Cost Per Record
1	$326	$237
2	$318	$236
3	$302	$231
4	$268	$228
5	$258	$225
6	$255	$225
7	$232	$219
8	$229	$217
9	$227	$215
10	$216	$207
11	$210	$202
12	$196	$201
13	$193	$198
14	$191	$196
15	$191	$194
16	$187	$193
17	$174	$170
18	$167	$166
19	$158	$157
20	$147	$154

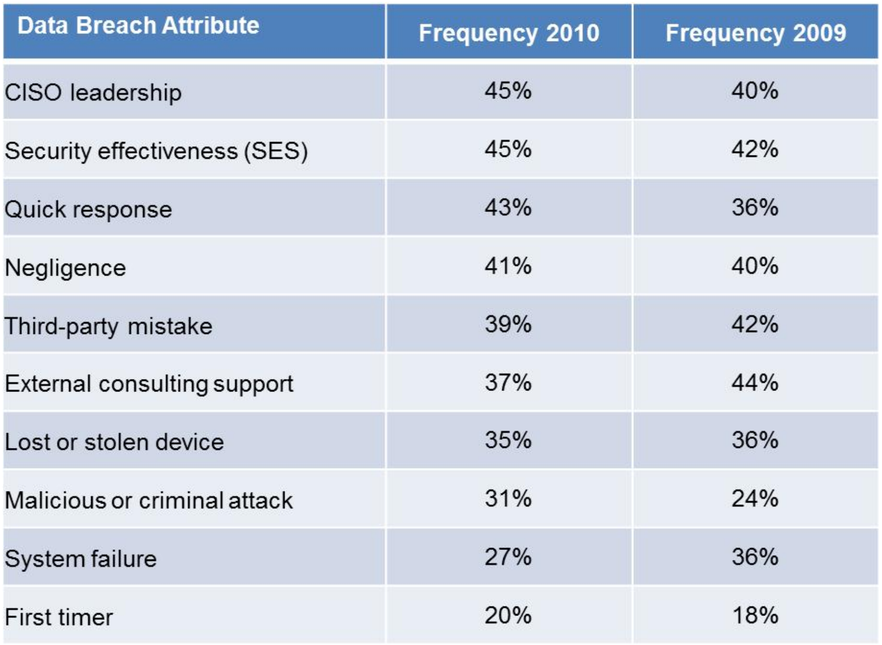
Table 2: Breach cost comparison by relative ranking, 2009-10

Organizations are more proactively protecting themselves from malicious attacks: Of the various causes of data breaches, malicious or criminal attacks increased the most in 2010. For the first time, malicious or criminal attacks were no longer the least common breach cause.

The frequency of different data breach types may underscore the growing threat of malicious and criminal attacks. Of the various data breach causes, malicious or criminal attacks increased the most in 2010 (up 7 points) and, for the first time, were no longer the least common reason. Meanwhile, companies with an above-average IT security posture increased by 3 points.

At the same time, three response characteristics increased in frequency: the number of organizations responding quickly (within 30 days), those putting CISOs in charge of data breach response, and those with an above-average IT security posture. Taken together, these figures may indicate more organizations are taking more active steps to thwart hostile attacks. Moreover, breaches due to systems failures, lost or stolen devices and third-party mistakes all fell. These two factors may point to companies becoming more conscientious about preventing data breaches.

While preventing malicious breaches is a top priority, only one cause of data breaches – negligence – was present in more than 40 percent of studied cases. The two most expensive breach types overall – those happening to first-time victims and those caused by malicious or criminal attacks – occurred less than one-third of the time. These figures may indicate that only a minority of data breaches attract the majority of media and industry attention.



Data Breach Attribute	Frequency 2010	Frequency 2009
CISO leadership	45%	40%
Security effectiveness (SES)	45%	42%
Quick response	43%	36%
Negligence	41%	40%
Third-party mistake	39%	42%
External consulting support	37%	44%
Lost or stolen device	35%	36%
Malicious or criminal attack	31%	24%
System failure	27%	36%
First timer	20%	18%

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

These figures correspond with findings from the *2010 Annual Study: U.S. Enterprise Encryption Trends* report, also conducted by the Ponemon Institute and sponsored by Symantec.[10] Namely, the report found that in 2010, protecting against viruses, malware, and spyware infection became organizations' No. 1 data protection priority. Nearly all respondents (97 percent) considered cyber attacks as the most severe threat to their ability to carry out their missions.

Moreover, the *U.S. Enterprise Encryption Trends* report also found that 88 percent of organizations surveyed had had at least one data breach, up slightly from 2009. A worrying trend, however, was that respondents having more than five data breaches a year are the only group that is growing, and growing fast. These figures reinforce the rising recognition that malicious attackers can get at critical data, particularly unprotected data. That fear made other data protection issues lower priorities.

[10] *2010 Annual Study: U.S. Enterprise Encryption Trends*, The Ponemon Institute, November 2010

Companies' investments in finding and remediating data breaches may be paying off: Organizations became much more proactive in finding and starting their response to data breaches in 2010. On average, detection and escalation cost $455,000, up 72 percent from $264,000 in 2009 and 68 percent from $271,000 in 2008.

Companies also devoted noticeably more resources to contacting and helping data breach victims. Ex-post response saw strong gains, up 15 percent from $1.5 million last year to $1.7 million this year. The 2010 figure marks a 34-percent increase from $1.3 million in 2008 as well.

The changes are evident in the per-record costs as well. Detection and escalation accounted for $13 of the total 2010 per-record cost, up $5 (6 percent) from both 2009 and 2008. Ex-post response was $51 of the total 2010 per record cost, up $6 (13 percent) from 2009 and $12 (31 percent) from 2008.

Both detection and escalation and ex-post response have posted significant double-digit cost increases for the past five years. In particular, increases in legal defense costs remain a main reason for increased spending in ex-post response, as companies fear successful class action lawsuits by breach victims.

Companies may be doing the right things to allay that fear. The cost of lost business stayed relatively stable at around $4.5 million for the third straight year. In that time, lost business has decreased proportionally to overall data breach costs; in 2010, it accounted for 63 percent of the total cost, down 3 percent from 2009 and 6 percent from 2008. Spending on lost business closely matches spending on detection and escalation and ex-post response.

Finally, notification costs rose slightly to $511,000 overall and $15 per record. Their proportion of total per record cost has stayed almost the same for the fourth straight year, at roughly 7 percent. These figures may indicate that companies are familiar with notification mechanisms and their experience has helped stabilize costs.

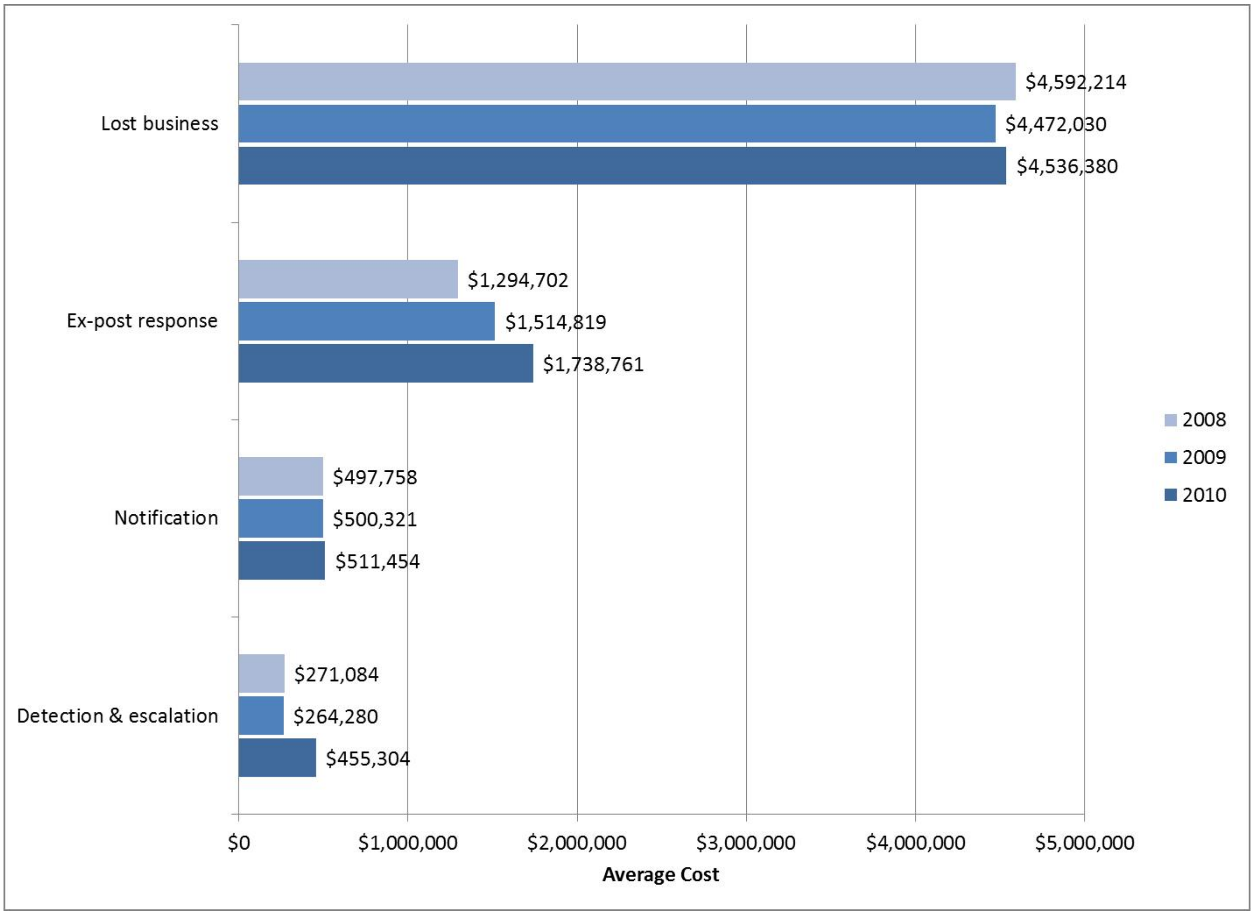


Figure 3: Average data breach cost by cost activity, 2008-10

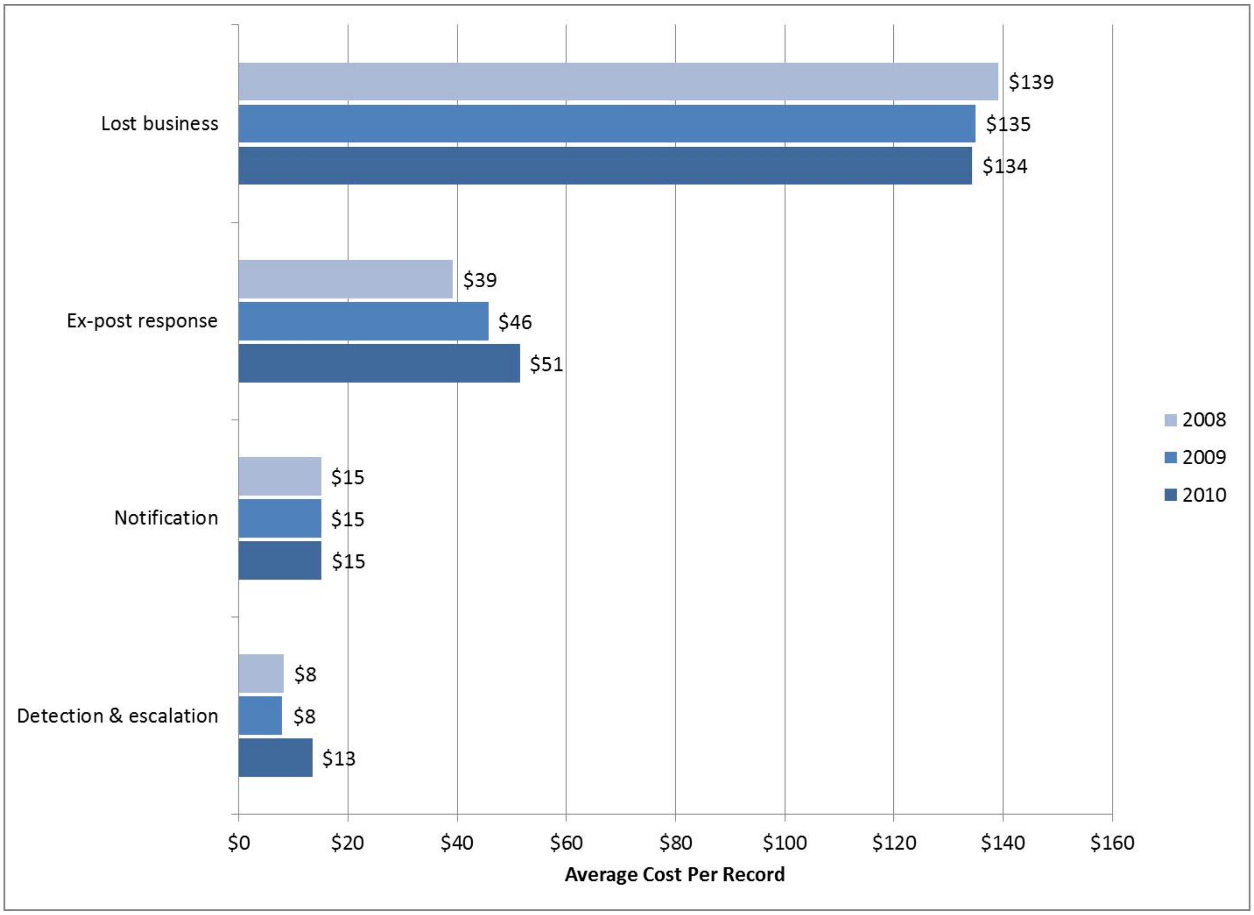


Figure 4: Average cost per record by cost activity, 2008-10

This data appears to support the major finding from the *2010 Enterprise Encryption Trends* study: 2010 marked the first time that regulatory compliance surpassed data breach mitigation as the main driver behind the implementation of encryption technologies (and, by extension, other data protection technologies).

In that study, more than two-thirds (69 percent) of respondents stated regulatory compliance was their main reason, up 5 points from 2009 and 11 points from 2008. Meanwhile, mitigating data breaches saw its second annual decline to 63 percent, down 4 points from 2009 and 8 points from 2008. These figures illustrate a growing acceptance that regulations are important, while at the same time data breaches are becoming more part of the fabric of IT security.

Key regulations driving encryption use remained the same from 2008 and 2009, including state privacy laws (such as those in California, Massachusetts and others), PCI requirements, and the Health Information Portability & Accountability Act (HIPAA). Interestingly, PCI requirements have seen the greatest increase in influence by far over the past four years, rising 49 points from 15 percent in 2007 to 64 percent this year.

PCI is becoming one of the most important drivers to action because failure to comply means organizations can’t do online credit card transactions, which holds organizations to a much higher level of accountability. At the same time, traditional compliance drivers such as Sarbanes-Oxley and Graham-Leach-Bliley have decreased in prominence over time in terms of driving encryption projects as companies integrate compliance with those regulations into their standard operations.

This year’s *Cost of a Data Breach* cost activity figures may reflect the increased focus on regulatory compliance. Compliance with data protection regulations requires organizations to do more to find, disclose and fix breach-related problems. These tasks correspond with the detection and escalation, notification and ex-post response cost activities, respectively. Strong growth in both detection and escalation and in ex-post response could reflect increased compliance activities, as those two stages often require more investment than the notification process.

For the third straight year, direct costs accounted for a larger proportion of overall data breach costs: Direct costs represent measurable accounting line items organizations have for specific data breach response activities. Indirect costs include lost customer business due to churn, customer acquisition costs and indirect opportunity costs of direct costs. This last figure – which represents the disruption to normal business operations that data breach response causes – is difficult to break down specifically for each direct cost but has a pronounced overall effect on total data breach costs.

Direct costs rose 5 points to 34 percent this year, while indirect costs dropped the same amount to 66 points. While indirect costs still outweigh direct costs by nearly two to one, this study data reinforces the trend started in 2008 of direct costs comprising a larger fraction of overall spending.

In 2010, direct costs accounted on average for $73 (34 percent) of the total average cost, up $13 (22 percent) from 2009 and $23 (46 percent) from 2008. Increased legal defense costs remained the primary driver for the increases. At the same time, indirect costs continued their slow decline; this year’s average of $141 was down $3 (2 percent) from 2009 and $11 (7 percent) from 2008.

The sharp growth in direct costs and slight but persistent decrease in indirect costs over the past three years may indicate that companies are taking their response to data breaches more seriously than ever. Organizations’ efforts to repair the damage breaches cause may be slowly building customer and partner confidence, lowering the number of present and potential customers who take their business elsewhere after a breach. These results may also bolster the argument that organizations are focusing more on regulatory compliance, as direct costs correspond to the cost activities covered by data protection regulations (detection and escalation, notification and ex-post response).

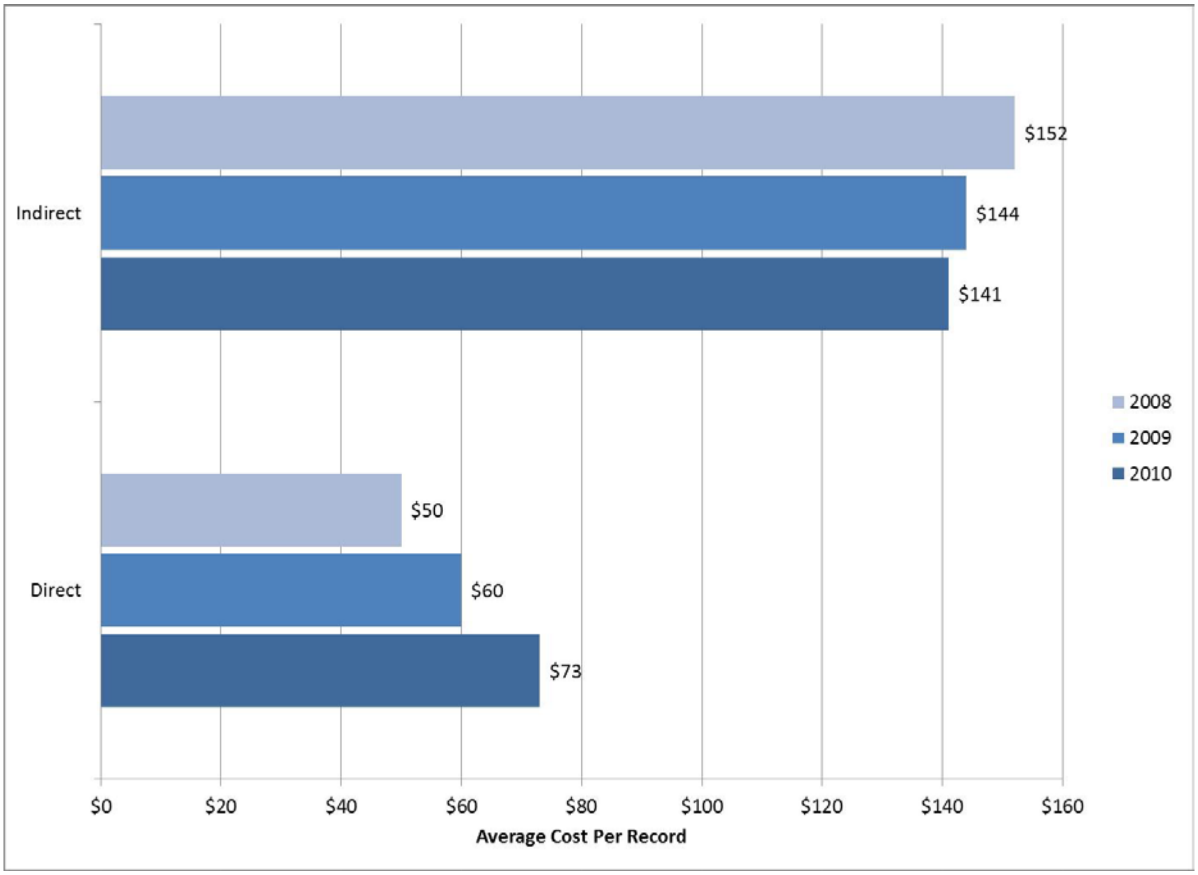
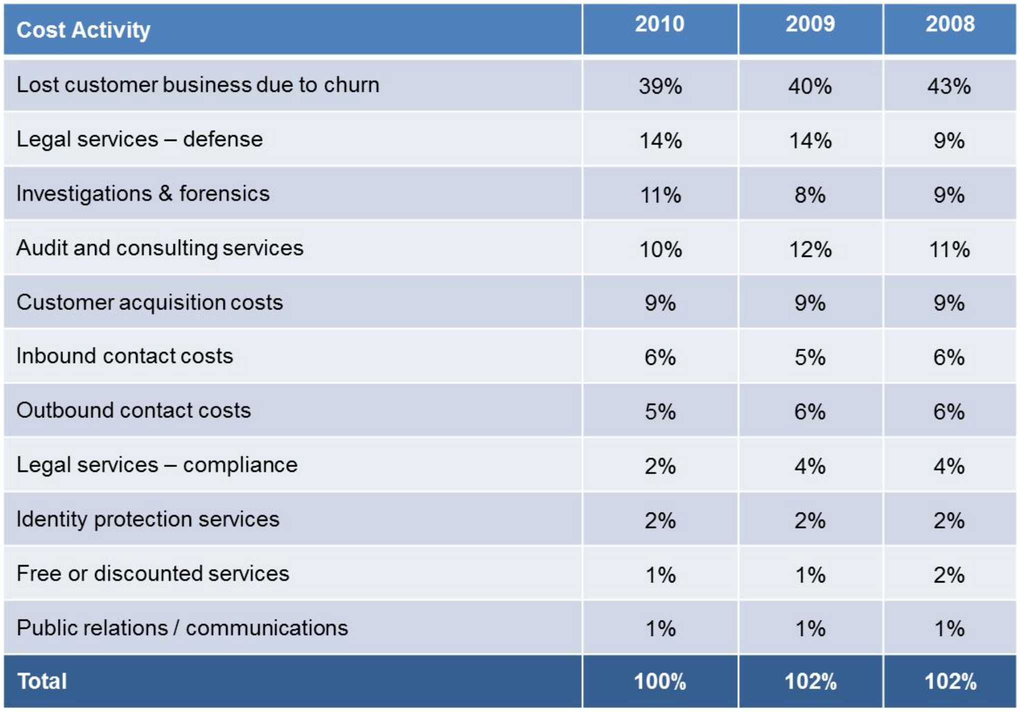


Figure 5: Cost per record of direct and indirect costs, 2008-10

Among specific cost activities, organizations continued to spend the most on lost business due to customer churn, which edged down a point to 39 percent. Legal defense services (14 percent, no change from 2009), investigations and forensics (11 percent, up 3 points) and audit and consulting services (10 percent, down 2 points) were other primary cost centers. Customer acquisition costs have stayed steady at 9 percent of overall spending since 2007.

These figures may indicate that more organizations are taking a proactive role in protecting themselves, both from a legal and IT perspectives. The shift we have seen may also indicate that as companies become more proactive, they need to spend less on lost business, further showing the value of taking the initiative to address data breaches.



Cost Activity	2010	2009	2008
Lost customer business due to churn	39%	40%	43%
Legal services – defense	14%	14%	9%
Investigations & forensics	11%	8%	9%
Audit and consulting services	10%	12%	11%
Customer acquisition costs	9%	9%	9%
Inbound contact costs	6%	5%	6%
Outbound contact costs	5%	6%	6%
Legal services – compliance	2%	4%	4%
Identity protection services	2%	2%	2%
Free or discounted services	1%	1%	2%
Public relations / communications	1%	1%	1%
Total	**100%**	**102%**	**102%**

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

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

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

In this year's study, average abnormal churn rates across all 51 incidents stayed level at 4 percent. We measured that rate by the loss of customers who were directly affected by the data breach (i.e., typically those receiving notification). Nine sectors saw very slight increases, three saw very slight decreases and three did not change.

The industries with the highest 2010 churn rate remained pharmaceuticals and healthcare (each up a point to 8 percent and 7 percent, respectively). Communications dropped a point to 6 percent while financial services and services stayed at 5 percent. Hospitality rose a point to 5 percent as well. The industries with the lowest abnormal churn rates were public sector (less than 1 percent) and retail (1 percent), followed by education, transportation, technology and media (all at 2 percent).

Sectors with the highest 2010 average per-record costs were communications ($380), financial ($353) and pharmaceutical ($345). Those with the lowest costs were media ($131), education ($112), and public sector ($81).

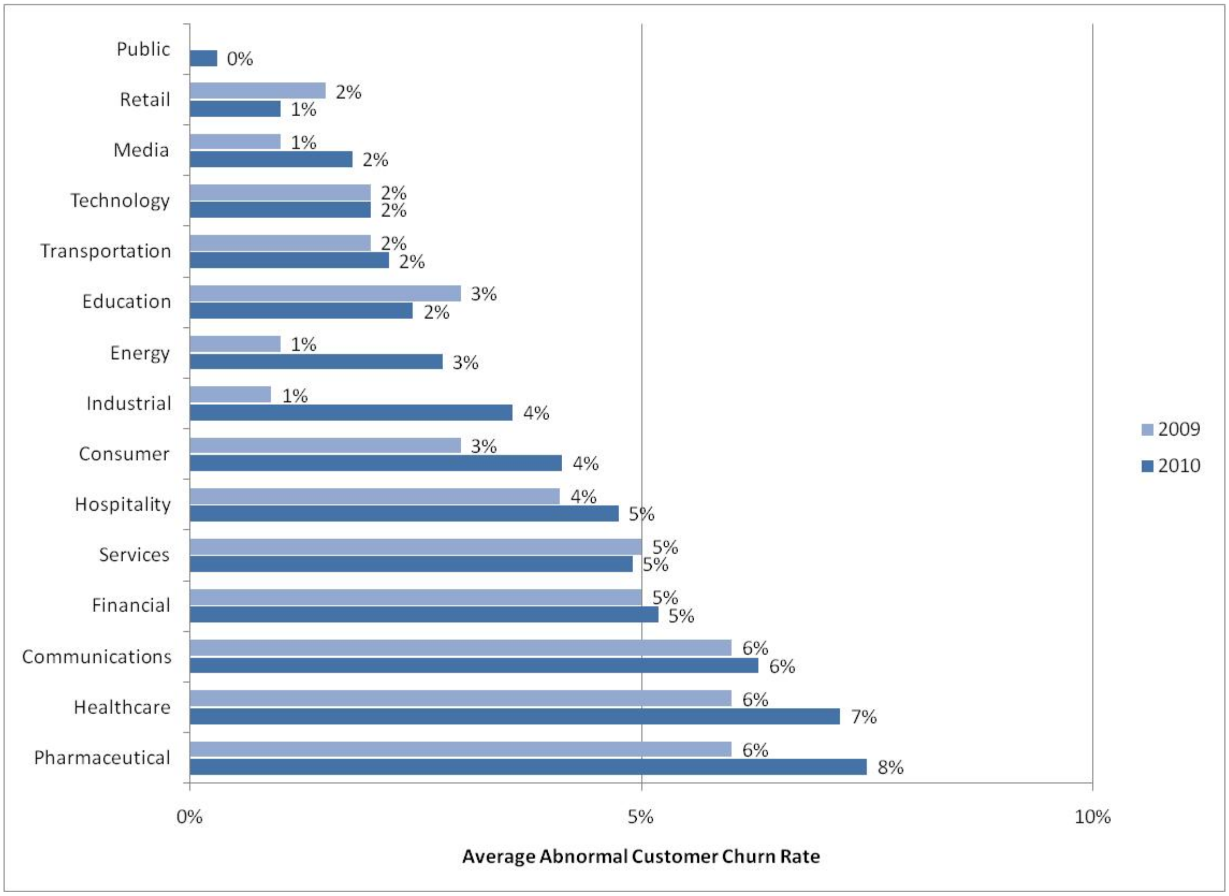


Figure 6: Abnormal churn rates following data breaches by industry classification, 2009-10

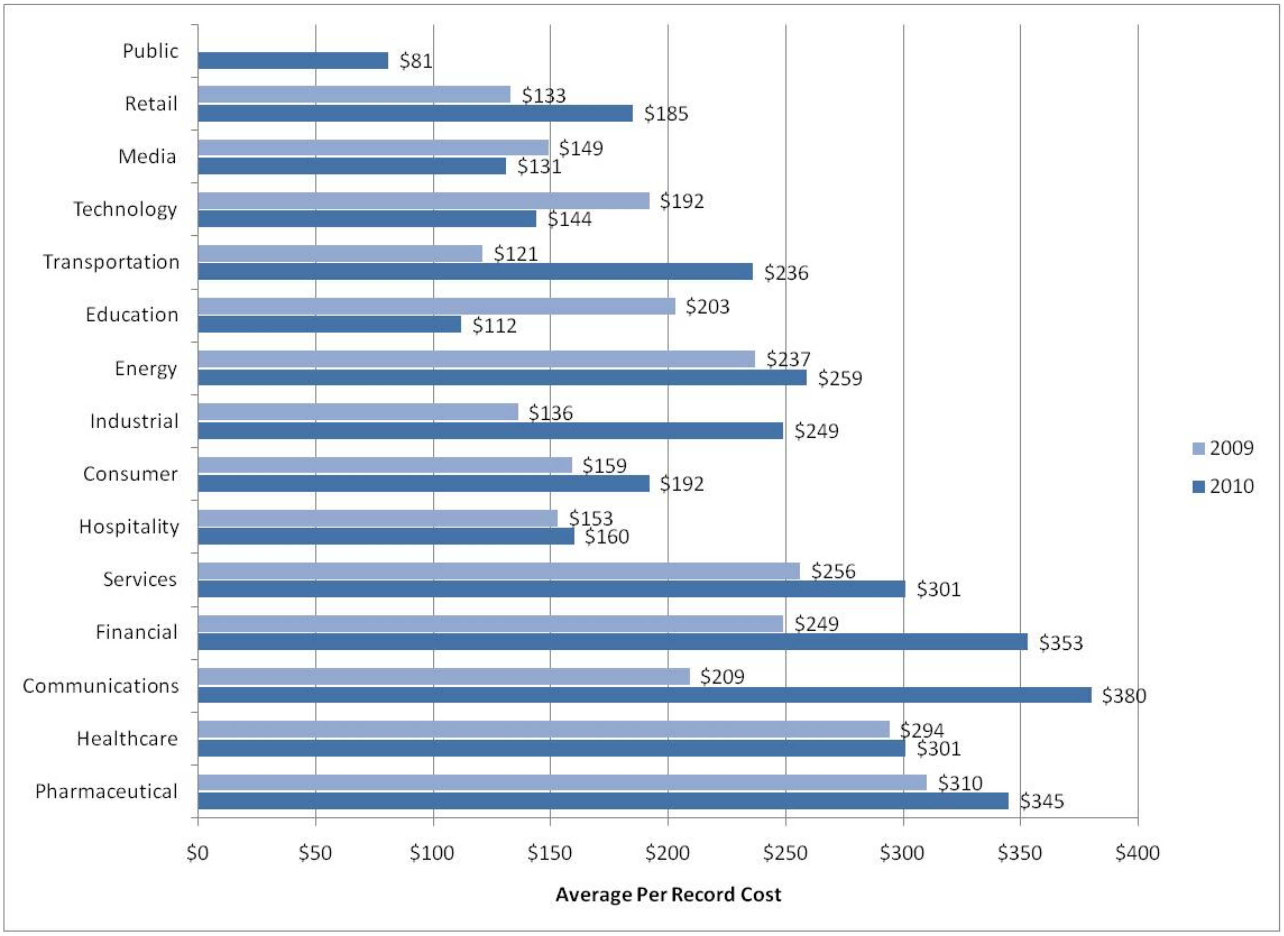


Figure 7: Cost per record of data breaches by industry classification, 2009-10

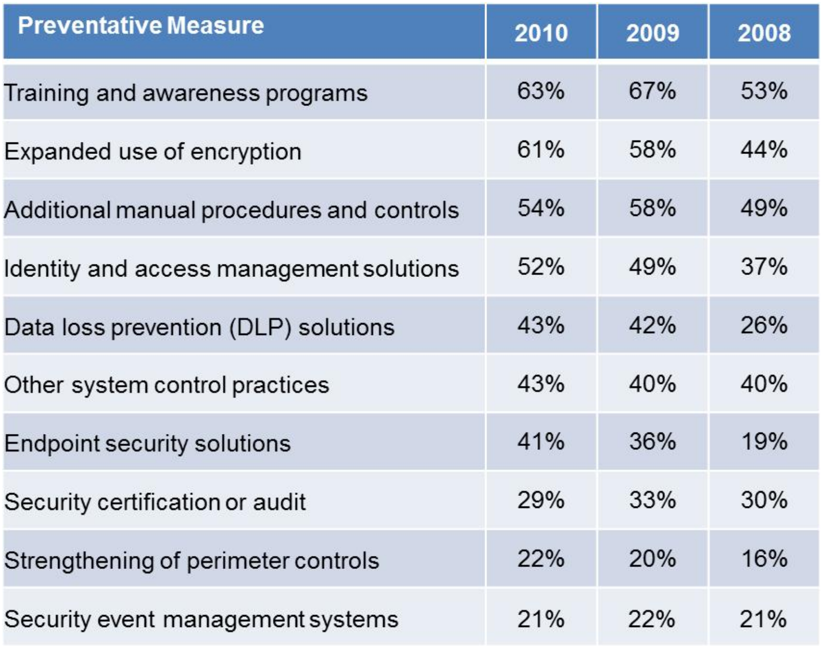
Training and awareness programs remain the most popular post-breach remedies, but encryption and other technologies are gaining fast: After data breaches, organizations often consider a number of possible remedies to protect confidential and sensitive data as part of an enterprise data protection strategy. Training and awareness programs remained the most popular, with nearly two-thirds (63 percent, down 4 points) of respondents using them. Expanded use of encryption stayed the most popular technology solution and, with 61 percent (up 3 points), took sole possession of second place this year.

Other notable remediation procedures following breach incidents included: additional manual procedures and controls (54 percent, down 4 points), identity and access management solutions (52 percent, up 3 points), data loss prevention solutions (43 percent, up a point), and endpoint security solutions (41 percent, up 5 points).

Interestingly, while all solution categories have seen flat to marked growth since 2008, technological solutions have seen the strongest growth while personnel and policy solutions have grown more slowly. Endpoint security solutions have increased 22 percent, both encryption and data loss prevention solutions have increased 17 percent and identity and access management solutions have risen 15 percent. By comparison, training and awareness programs have increased 10 percent and manual controls only 5 percent.

Taken together, these figures may indicate that companies continue to rely upon educating their workforce and enabling it to personally help stop future data breaches. At the same time, though, companies are increasingly aware of, and willing to implement, technological solutions designed to help prevent and mitigate breaches.

These findings complement similar results from the *2010 Enterprise Encryption Trends* report, which found that the vast majority of organizations continue to adopt encryption. The study revealed that 90 percent of organizations have completed at least one encryption project. Encryption is one of many favored technologies to thwart cyber attacks and protect laptops and other mobile endpoints. As a group, encryption, encryption key management and endpoint security solutions including laptop encryption all had the biggest increases in specific strategic budget allocations – up 10 percent on average since 2008. These figures may indicate that respondents are still deploying older, trusted technologies but are also looking to new technologies to better curtail or prevent data breaches caused by evolving cyber security threats.



Preventative Measure	2010	2009	2008
Training and awareness programs	63%	67%	53%
Expanded use of encryption	61%	58%	44%
Additional manual procedures and controls	54%	58%	49%
Identity and access management solutions	52%	49%	37%
Data loss prevention (DLP) solutions	43%	42%	26%
Other system control practices	43%	40%	40%
Endpoint security solutions	41%	36%	19%
Security certification or audit	29%	33%	30%
Strengthening of perimeter controls	22%	20%	16%
Security event management systems	21%	22%	21%

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

Findings by Breach Type – Cause

For the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least frequent: Of the three overarching breach categories – malicious or criminal attacks, negligence and systems failures[11] -- nearly a third (31 percent) of all cases in this year's study involved a malicious or criminal attack. That figure is up 7 points from 2009, the highest increase in frequency in this year's study. It is also up 19 points from 2008; this second consecutive increase occurred after the incidence of such attacks doubled between 2008 and 2009. This year marks the first time that malicious attacks are not the least frequent cause of data breaches for U.S. companies.

These results may indicate that malicious or criminal attacks are increasingly the main threat to companies' important data. The figures would also appear to support similar findings in the *2010 U.S. Enterprise Encryption Trends* report, which found preventing cyber attacks was respondents' top data protection priority.

Meanwhile, the number of breaches attributed to negligence edged up a point to 41 percent. The number of breaches caused by systems failures dropped 9 points to 27 percent. The noticeable drop in breaches from systems failures may point to organizations becoming more conscientious in ensuring their systems can help prevent and mitigate breaches (through new security technologies and/or compliance with security policies and regulations). The relatively stable figure for negligence, however, may indicate that ensuring employee and partner compliance remains an ongoing challenge.

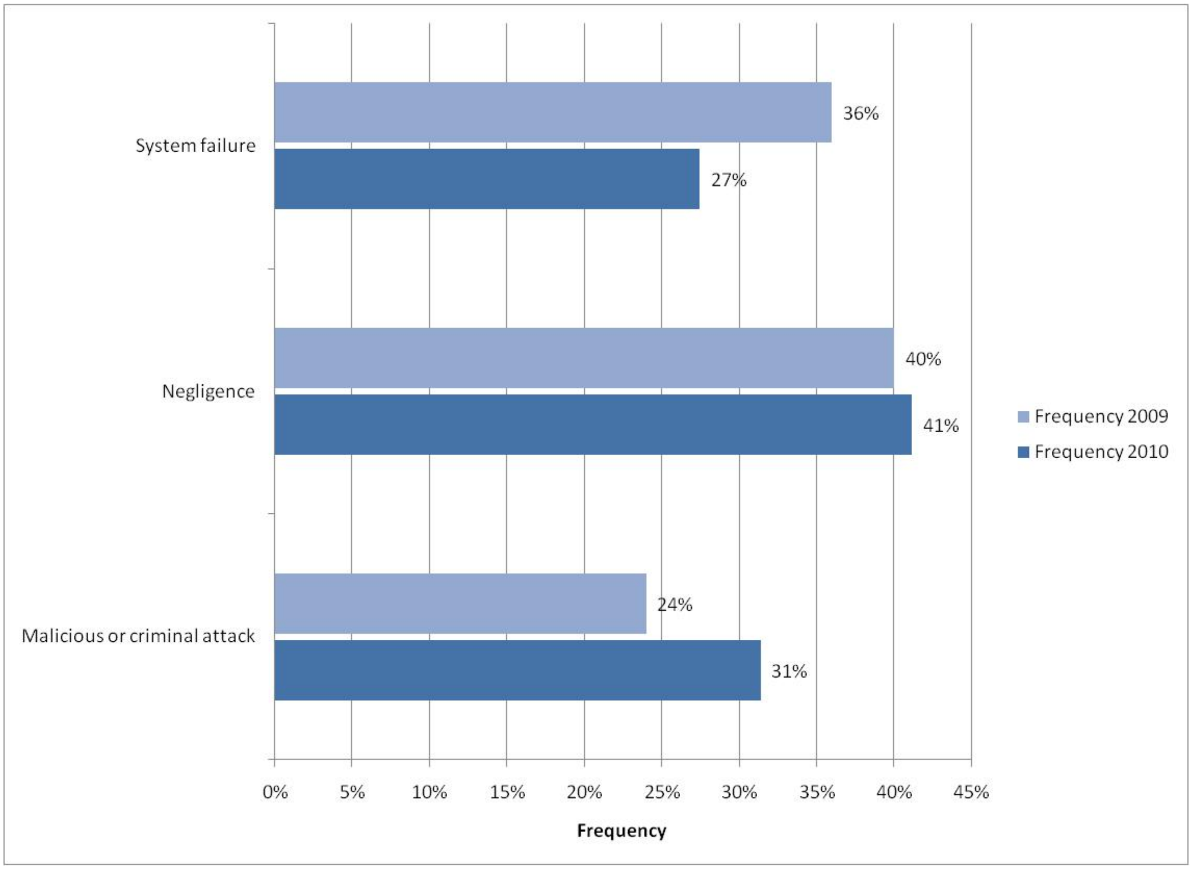


Figure 8: Frequency of primary data breach causes, 2009-10

[11] Third-party mistakes and the loss or theft of data bearing devices are also main causes of data breaches but the reasons they occur fall under these three categories.

Our research shows data breaches involving malicious or criminal acts continued to be much more expensive than incidents resulting from either negligence or systems failures – and that cost is skyrocketing. Accordingly, in 2010 the cost per compromised record of a data breach involving a malicious or criminal act averaged $318 while breaches not involving malicious actors cost $215. Malicious breaches cost $151 (48 percent) more this year than non-malicious breaches, skyrocketing $137 (982 percent) from last year. In 2009, malicious breaches cost only $14 (7 percent) more.

The huge increase reinforces the extreme danger hostile breaches pose. Attacks have become more stealthy and successful, demanding companies spend more resources to deal with them.

At the same time, breach costs for negligence and systems failures rose sharply as well. Breaches from negligence in 2010 averaged $196 per record, up $42 (27 percent) from 2009. Breaches not involving negligence cost $227 per record, down $10 (4 percent). Non-negligent breaches cost $31 (16 percent) more this year than non-negligent breaches, a $52 (62 percent) drop from last year. In 2009, negligent breaches cost $83 (54 percent) more.

Breaches from systems failures averaged $210, up $44 (also 27 percent). Breaches not involving them cost $216, down $9 (4 percent as well). Breaches without systems failures cost only $6 (3 percent) more this year than those with them, a $53 (90 percent) drop from last year. In 2009, failure-related breaches cost $59 (36 percent) more.

The strikingly similar trends for data breaches involving negligence and systems failures may indicate that both companies and their customers take non-malicious breaches seriously and expect companies to spend appropriately to respond to them. Interestingly, for both causes, breaches not involving them still cost more than those that did, but also cost significantly less than last year. These figures may reflect the growing prevalence and cost of malicious breaches, as well as organizations' growing competency in handling breaches from negligence and systems failures.

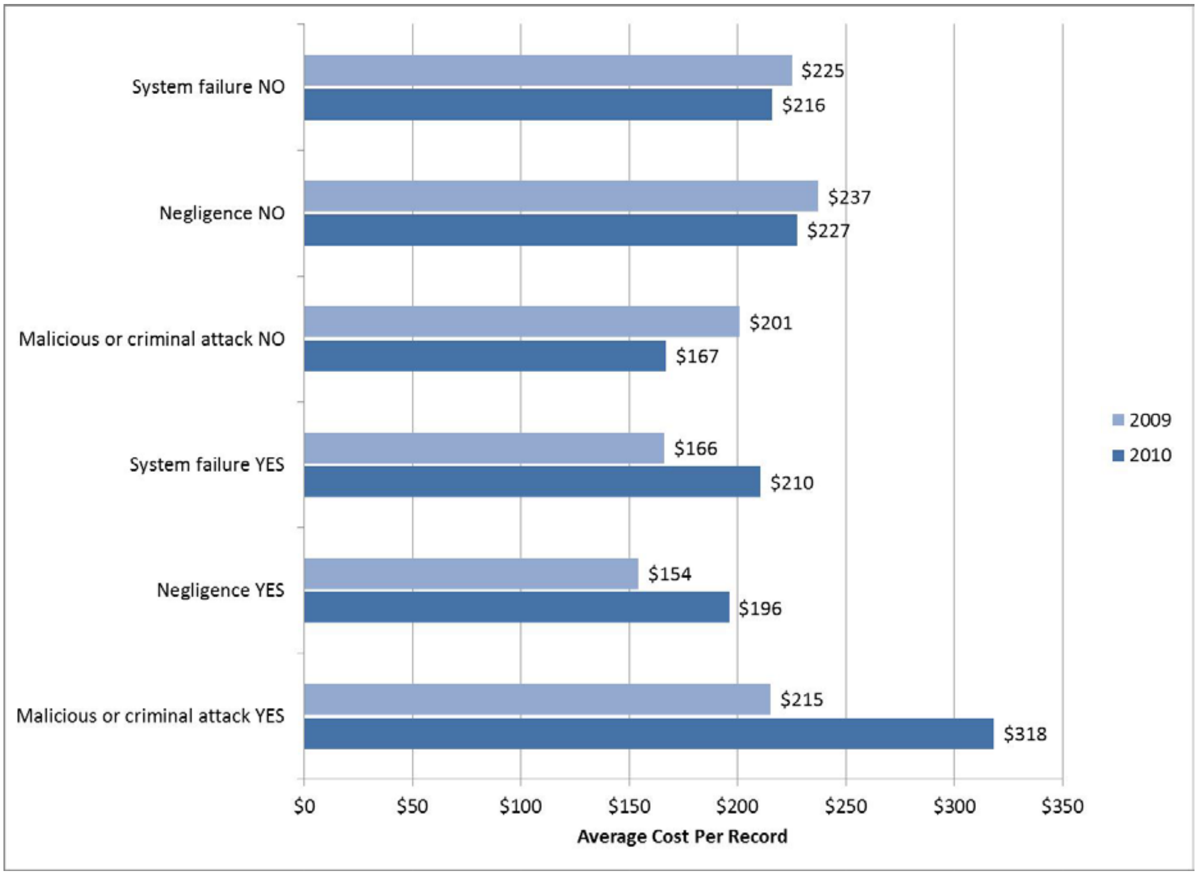


Figure 9: Costs per record of data breaches by primary cause, 2009-10

Breaches involving third-party mistakes by outsourcers are becoming slightly less common but much more expensive: Third-party outsourcers or consultants often analyze or process large volumes of customer-related data. Data breaches can involve outsourced data, especially when the third party is offshore. Third-party mistakes continued their slight decline in 2010 to 39 percent, down 3 points from 2009 and 5 points from 2008.

The cost of such breaches rose significantly, however, up $85 (39 percent) to $302 per record. The cost of breaches not involving third parties dropped but not as sharply, down $36 (18 percent) to $158. Breaches involving third parties cost $144 (48 percent) more this year than internal breaches, a $121 (525 percent) leap from last year. In 2009, third-party breaches cost $23 (11 percent) more.

These figures may indicate that compliance with government and commercial regulations for data protection are dramatically raising breach costs involving outsourced data. These costs could include additional investigation and consulting fees, as well as added costs when companies outsource their data offshore.

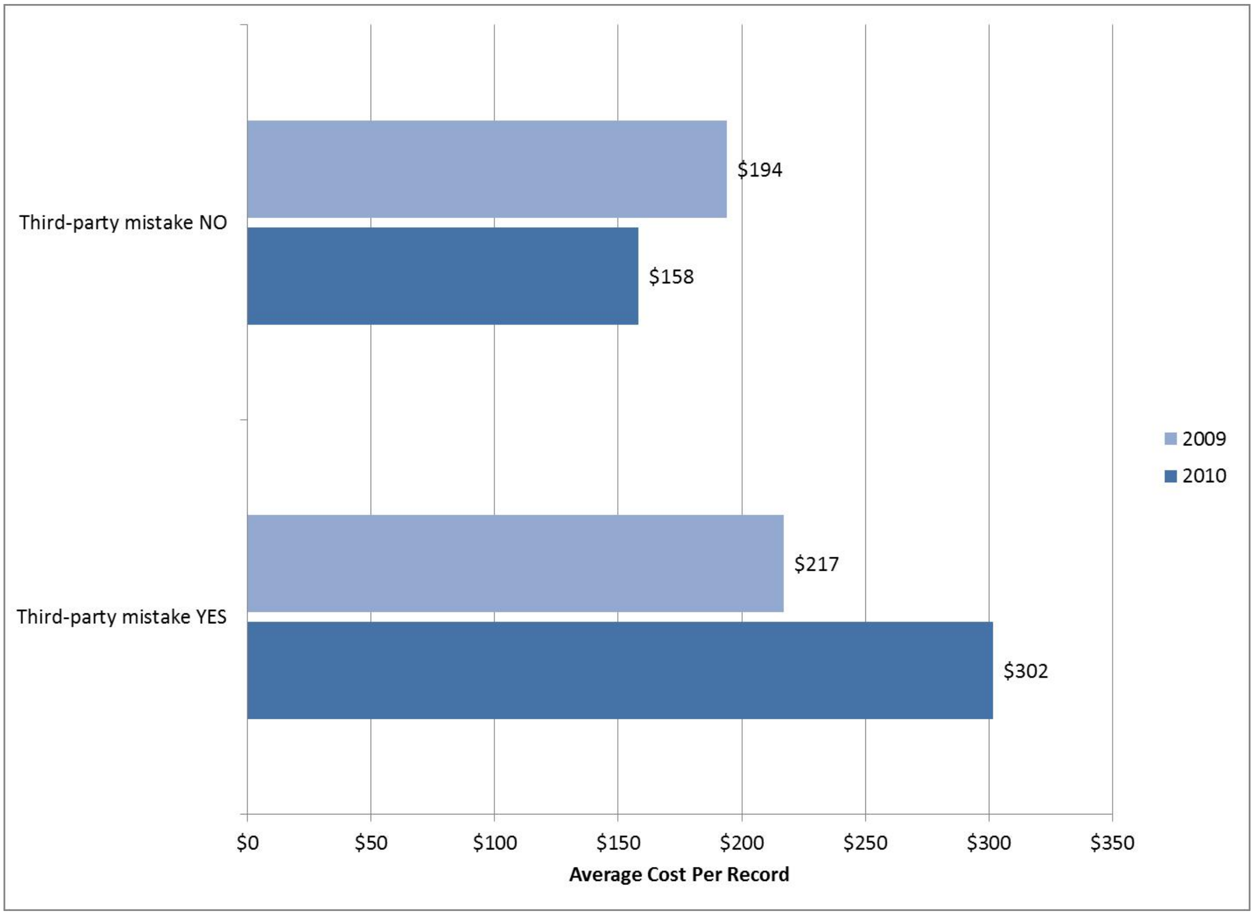


Figure 10: Cost per record of breaches due to third-party mistakes, 2009-10

Breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat: The prevalence of breaches concerning mobile devices holding sensitive data stayed roughly the same at 35 percent this year, down a point. Per-record costs rose $33 (15 percent) to $258 per record for such breaches but stayed virtually flat at $191 for those that did not. Breaches involving lost or stolen devices cost $67 (26 percent) more this year than those that did not, a $35 (109 percent) jump from last year. In 2009, loss- and theft-related breaches cost $32 (14 percent) more.

Our research suggests that device-oriented breaches have consistently cost more than many other breach types. This may be because investigations and forensics into lost or stolen devices are more difficult and costly. Another possible reason is that loss or theft often occurs in public or private spaces not secured as well as facilities where companies keep their non-mobile computing devices (desktops, servers, etc.). Finally, more malicious and criminal attacks are targeting these devices, particularly those used by high-value targets (senior government or company officials while traveling, etc.).

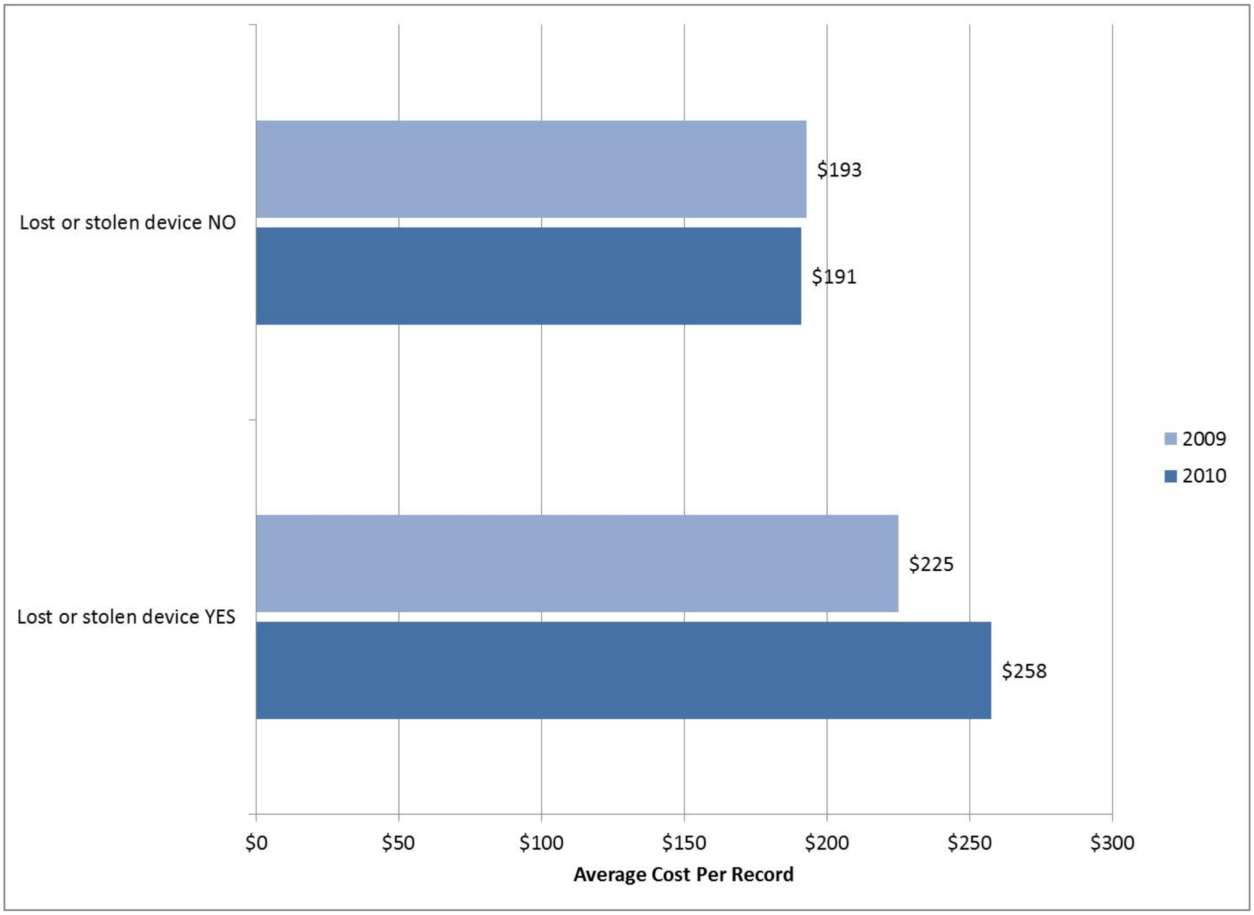


Figure 11: Cost per record of data breaches involving lost or stolen devices, 2009-10

Findings by Breach Type – Response

“First timers” are becoming more common and pay the highest breach costs: One in five (20 percent) of respondents in 2010 faced their first data breaches involving the loss or theft of more than 1,000 records containing personal information. That figure has increased slightly, up 2 points from 2009.

Although rare, these “first timers” paid the highest average costs of anyone in the 2010 report. They consistently pay some of the highest data breach costs of any breach type we study and ranked fourth in last year’s report.

This year, the cost per compromised record of an organization’s first data breach averaged $326 (up $98 or 43 percent) while subsequent breaches averaged $187 (down $11 or 5 percent). First-time breaches cost $139 (48 percent) more this year than subsequent breaches, jumping $109 (362 percent) from last year. In 2009, first-time breaches cost only $30 (13 percent) more.

These findings may indicate that the pool of first timers is growing due to both an increase in IT implementations and the expanding threat of malicious breaches. As stated above, attacks are becoming more insidious and damaging, which requires greater resources to combat. First timers often lack breach response experience that can help lower costs. Fortunately, experience with data breaches may help companies become more efficient at managing costs over time.

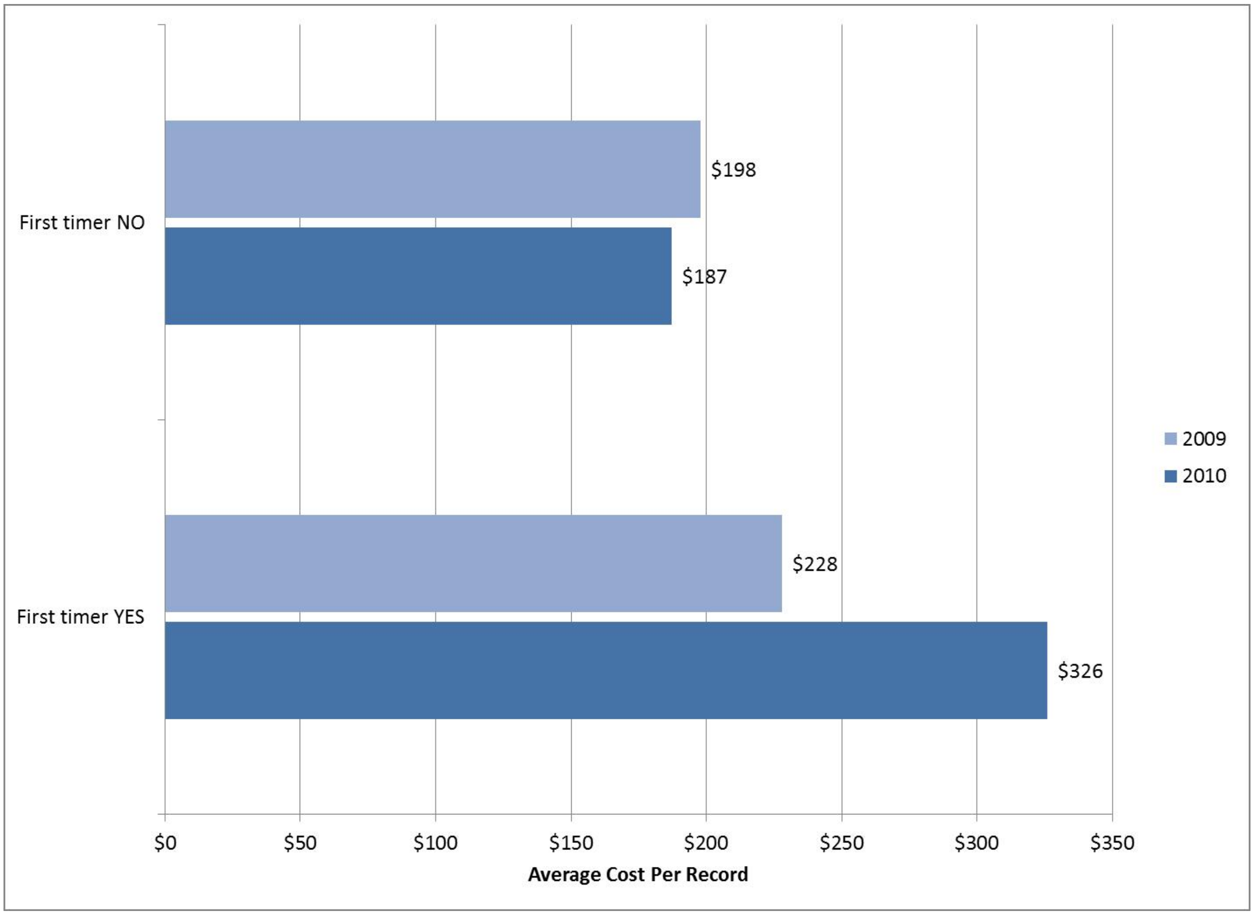


Figure 12: Cost per record of first time and subsequent data breaches, 2009-10

More organizations favor rapid response to data breaches, and that is significantly costing them: Forty-three percent of companies notified victims within one month of discovering the data breach, up 7 points from 36 percent last year. That growth marks the largest percent increase among data breach response attributes.

For the second year in a row, these "quick responders" paid significantly more per record than companies that moved more slowly. In 2010, quick responders had a per-record cost of $268, up $49 (22 percent) from $219 the year before. Companies that took longer paid $174 per record, down $22 (11 percent) from 2009. Breaches for companies that took longer cost $94 (35 percent) less this year than quick-response breaches, a $71 (307 percent) jump from last year. In 2009, organizations that responded more slowly to paid $23 (11 percent) less.

Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for the organization, especially during the detection, escalation and notification phases. The notable increase in companies responding quickly to breaches, despite the additional cost, may reflect pressure companies feel to comply with commercial regulations and state and federal data protection laws. The federal government and attorneys general in some states, such as Massachusetts, can sue companies for negligence if the government officials believe the companies are not responding to a data breach sufficiently fast. We will closely watch this issue in future reports.

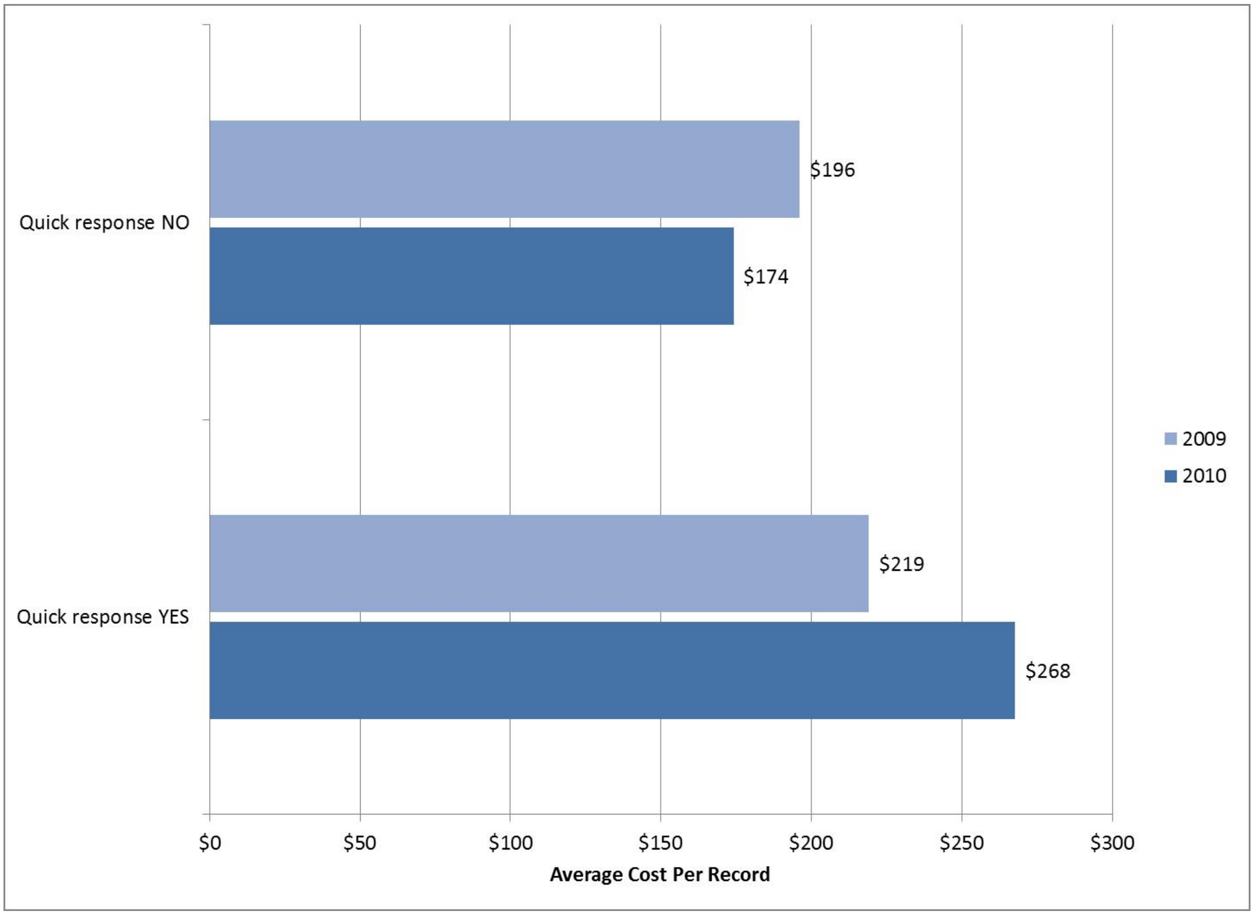


Figure 13: Cost per record of data breaches for quick responders, 2009-10

More companies had better-than-average security postures, and those organizations enjoyed much lower data breach costs: Forty-two percent of respondents had a Security Effectiveness Score (SES) above the median value determined from benchmark results.[12] That figure is up 3 points from last year.

As expected, those organizations with a more favorable security posture (SES above the median) experienced a lower average cost per compromised record than organizations with an SES below the median. Accordingly, organizations with a favorable security posture had an average cost per compromised record of $147, $55 (27 percent) less than last year. Companies below the SES median paid $255, $48 (23 percent) more than in 2009. Breaches involving companies below the SES median cost $108 (74 percent) more this year than those that did not, soaring $103 (2,065 percent) higher than last year. In 2009, companies below the SES median paid only $5 (2 percent) more.

More companies may be exceeding the SES median because they are strengthening their IT security posture as part of their efforts to meet regulatory compliance requirements.

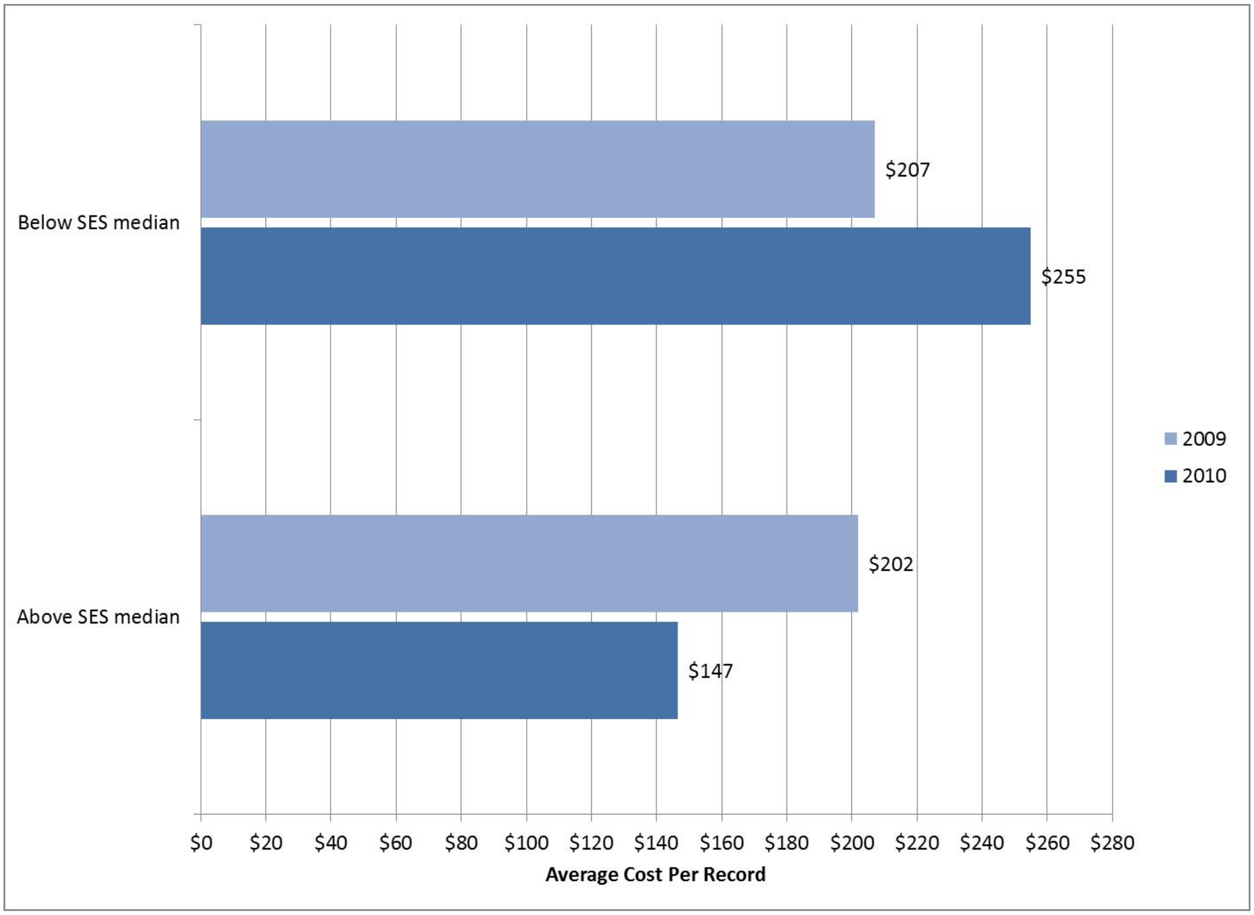


Figure 14: Cost per record of data breaches for companies by SES security posture, 2009-10

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

To better manage data breaches and reduce breach costs, more companies are trusting their CISOs: Forty-five percent of respondents had a CISO (or equivalent title) manage data breaches, up 5 points from 2009.

Breach response costs involving CISO leadership rose $36 (23 percent) to $193 per record. Costs for breach response lacking CISO leadership stayed flat at $232 per record. Breaches involving CISO leadership companies cost $39 (20 percent) less this year than those that did not, a $40 (51 percent) drop from last year. In 2009, companies with CISO leadership paid $79 (50 percent) less.

This year's results may indicate that as data breaches and cyber attacks become more prominent threats, more companies see CISO leadership as an essential part of their data breach prevention and mitigation efforts. More than other senior company IT officials typically involved in crisis management activities surrounding data breach response, CISOs play a strategic role in ensuring security and privacy measures are effectively implemented.

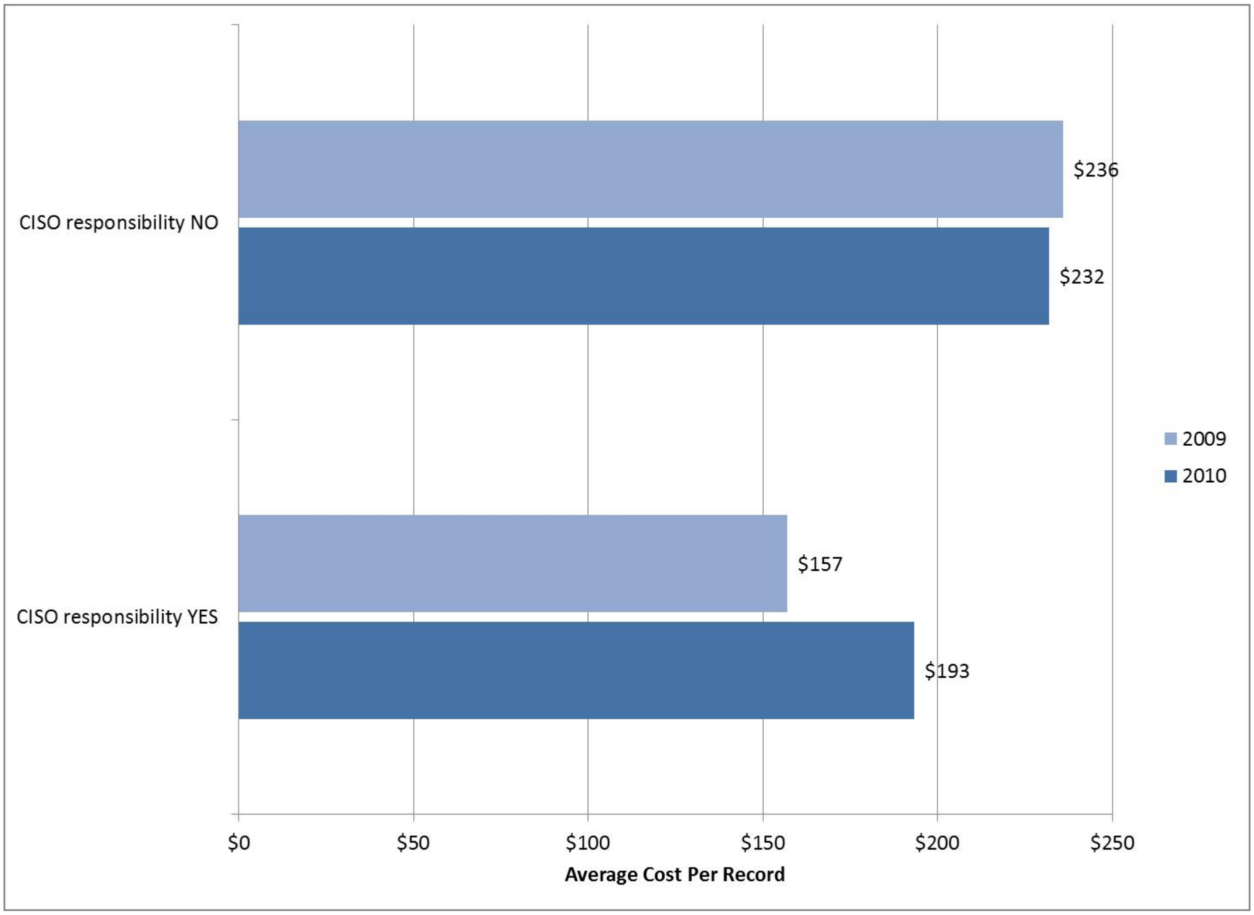


Figure 15: Cost per record of data breaches when CISOs lead breach response, 2009-10

Fewer organizations are using external consulting support, even though such support lowers data breach costs: The proportion of respondents that engaged outside consultants fell 7 points this year to 37 percent. Breaches with external consulting support rose $21 (12 percent) to $191. Costs for breaches lacking it stayed roughly flat at $229 per record.

Breaches involving external consulting support cost $38 (20 percent) less this year than those that did not, a $23 (38 percent) drop from last year. In 2009, companies using consultants paid $61 (36 percent) less.

The noticeable drop in the use of external consulting support may be tied to the finding above that more organizations are responding quickly to breaches. Organizations in a rush to respond may not believe they have the time to bring in outside help to meet compliance requirements. This in turn could help explain the increase in popularity of relying on CISOs, as organizations can quickly leverage these internal resources and see similar cost benefits.

Our results suggest that expert guidance, whether via CISO leadership or external consulting support, substantially reduces overall data breach costs. In each case, companies with such help paid 20 percent less than if they lacked it. Even though those savings are healthy, they are way down from last year. While specialized guidance from without or within still helps keep breach costs down, those investment costs are rising as organizations race to keep pace with escalating data protection threats.

Additionally, organizations that engage outside consultants may have lower average costs because they have more resources and be more responsive overall to IT security issues than those that do not. That in turn may mean they can respond to breaches more cost effectively.

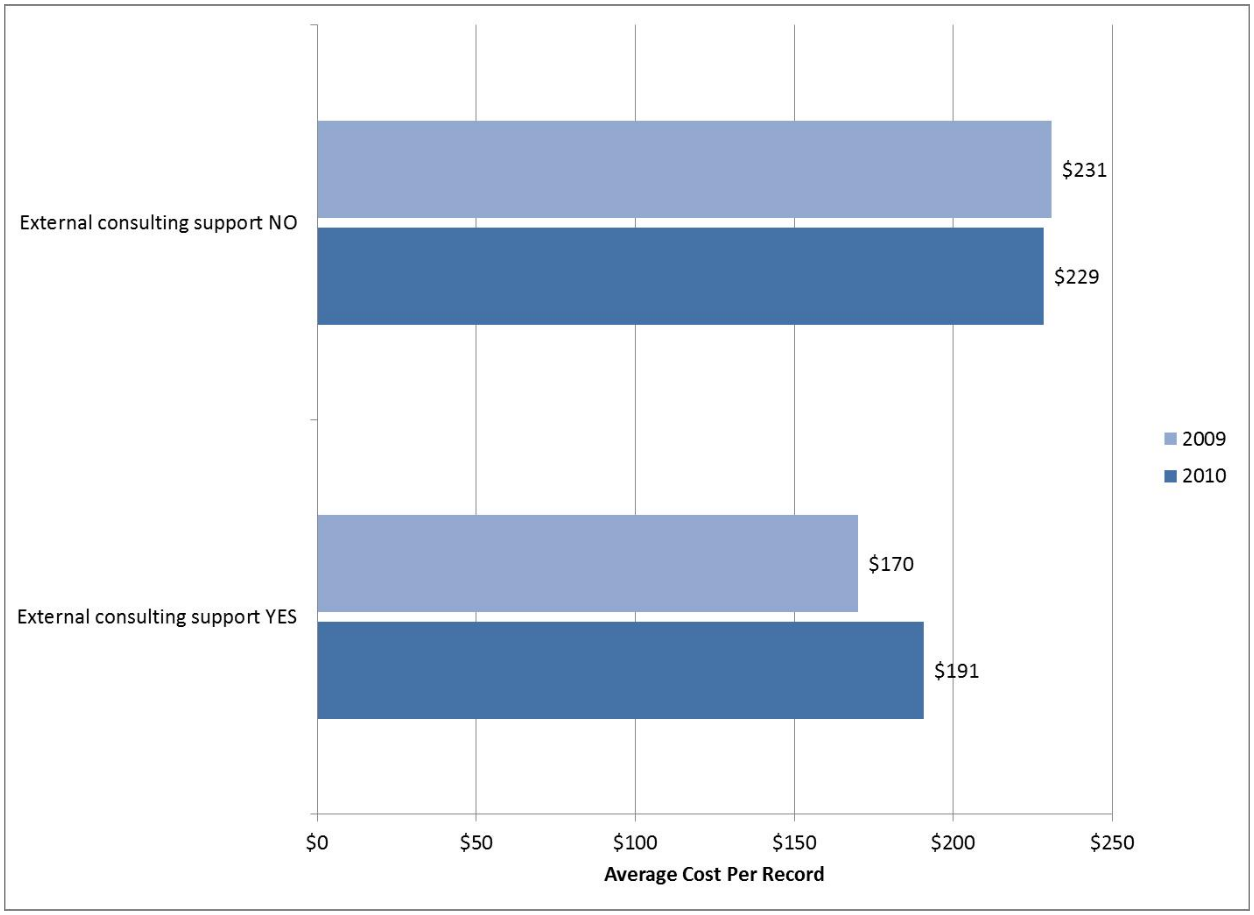


Figure 16: Cost per record of data breaches when outside consultants are involved with response, 2009-10

Report Conclusions

Taken together, this year's results suggest that data breaches remain a persistent threat with which the wide majority of companies already have unfortunate experience. Organizations are responding by locking down their IT systems to prevent breaches and taking proactive steps to act quickly and competently when breaches occur. Despite these positive steps, they still face increasing challenges from their own people, equipment and outsourcing partners.

The data security threat landscape continues to worsen and data breach costs continue to rise. Malicious or criminal attacks increased in both frequency and severity to further cement their position as a primary data breach cause.

One of the biggest obstacles companies may now be facing is regulatory pressure from industry and government. The notable increase in companies responding quickly to breaches, despite the additional cost, may reflect pressure companies feel to comply with commercial regulations and state and federal data protection laws. The federal government and attorneys general in some states, such as Massachusetts, can sue companies for negligence if the government officials believe the companies are not responding to a data breach sufficiently fast. More companies could be spending more than necessary to respond quickly to breaches to avoid possible regulatory scrutiny and penalties. We will closely watch this issue in future reports.

We base our conclusion on additional key findings, including:

- For the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least common one
- Organizations are more proactively protecting themselves from malicious attacks
- Companies' investments in finding and remediating data breaches may be paying off
- For the third straight year, direct costs accounted for a larger proportion of overall data breach costs

The increase in quick responders and CISO leadership and the declines in breaches related system failures, lost or stolen devices and third-party mistakes may point to organizations taking data breach threats and regulatory compliance requirements more seriously. The rise in CISO leadership and decline in use of external consulting support may indicate organizations' drive to move quickly; organizations may prefer to rely on internal experts out of a belief that hiring external consultants could slow breach response.

Companies' investments in finding and remediating data breaches may be paying off as well. The cost of lost business continues to drop as companies aggressively spend more on detection, escalation and ex-post response, largely on legal defense costs to avoid successful class-action lawsuits by breach victims.

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

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

Suggested Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organizations 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 organization 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 centralized management of IT security solutions so they can automatically enforce IT security best practices throughout their organizations. Such capability enables enterprises to align information protection with corporate security policies and regulatory or business-partner mandates. It also enables organizations to implement technology with minimal or no user disruption, encouraging user compliance and acceptance.

Next Steps

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

- Vet and evaluate the security posture of third parties before sharing confidential or sensitive information. Pick responsible vendors that can guarantee data protection through encryption and appropriate procedures and controls. Also, ensure that third parties protect data on their employees' mobile devices.

- Ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for extensive business travelers. Also, consider implementing inventory control, anti-theft devices and data loss prevention (DLP) policies, practices and technologies.

- Take as slow, thoughtful an approach to data breach response as possible, given federal and state legal requirements applicable to location, industry and circumstances of the breach. Prepare in advance as much as possible to enable quick and cost-effective response.

- Improve IT security posture by upgrading technology and procedures to reflect current best practices and the preventive solutions discussed above.

- Develop and practice a crisis management plan that clearly defines roles, duties, procedures and timelines.

- Establish an organizational structure that allows the CISO or other security/privacy leaders to take charge and ensure the detection and notification process is handled appropriately. When in doubt about legal requirements or the technical aspects of responding to data breaches, seek the counsel of external consultants and legal and technology experts to help ensure improved results.

- To minimize customer turnover (churn), develop a proactive communications outreach plan that clearly defines the issue and root cause of the breach incident. Whenever feasible, take steps that minimize potential harm to data breach victims. For instance, consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.

- Finally, perform a post-mortem a few months after the incident to objectively evaluate the adequacy and effectiveness of the overall response. At this point, it may make good sense to consider buying insurance products to defray future data breach costs.

About the Ponemon Institute

The Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company-identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About Symantec Corporation

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

Appendix A – Study 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 U.S. organizations 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 studies. The Ponemon Institute invited more than 400 organizations to participate; all invited organizations were known to have experienced a breach involving the lost or theft of customer or consumer data sometime in 2010. Fifty-one U.S. companies completed all parts of the benchmark study. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the data breach process, as well as the underlying costs associated with information loss.

- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

- Unmeasured factors: To keep the study concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

- Estimated cost results. The quality of study research is based on the integrity of confidential responses received from companies. While reliability checks were incorporated into the benchmark study process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique rather than the company's detailed actual cost data could create significant bias in presented results.

Benchmark Methods

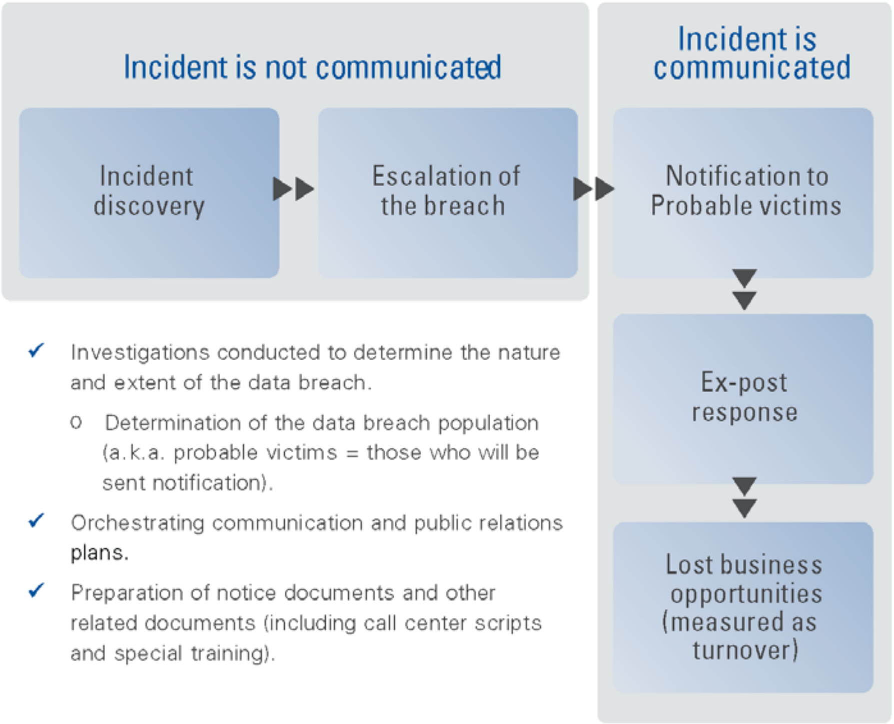
The benchmark study instrument was designed to collect descriptive information about the costs incurred either directly or indirectly concerning the breach event. Typically, the point-person for each study was privacy, data protection or compliance professionals responsible for managing the data breach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

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

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

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

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


Incident is not communicated
Incident discovery
Escalation of the breach
Incident is communicated
Notification to Probable victims
Ex-post response
Lost business opportunities (measured as turnover)

- ✓ Investigations conducted to determine the nature and extent of the data breach.
  - o Determination of the data breach population (a.k.a. probable victims = those who will be sent notification).
- ✓ Orchestrating communication and public relations plans.
- ✓ Preparation of notice documents and other related documents (including call center scripts and special training).

Figure 17: Visual representation of benchmark cost categories