2010 Annual Study: Global Cost of a Data Breach

Regulatory compliance surpassing data protection as main driver of data breach costs, leading IT organizations to sometimes pay more

A benchmark study of 154 global companies about the financial impact, customer turnover and preventive solutions related to breaches of sensitive data

May 2011

Research conducted by
Ponemon Institute, LLC

Ponemon INSTITUTE

Symantec

Executive Summary

Symantec Corporation and the Ponemon Institute proudly present *2010 Annual Study: Global Cost of a Data Breach*, the second annual study analyzing the cost of data breach incidents for companies in five countries: the United States, the United Kingdom, Germany, France and Australia (all converted into U.S. dollars).

This year's study analyzes the actual data breach experiences of 154 global companies from 17 different industry sectors. The 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 mean to organizations in an evolving data protection environment.

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

This year, multiple factors apparently confirm that regulatory compliance is surpassing data protection as the main driver of data breach companies' data breach costs – and, in some cases, may lead companies to pay more than they would otherwise. We base our conclusion on key findings, including:

- Breach costs correspond with national data protection priorities, especially regulatory compliance
- Generally, costs are highest and rising the fastest for high-risk breach types targeted by laws and regulations and are lowest and rising the slowest, or even shrinking, for breach types not involving them
- Across the board, companies are becoming more proactive in the face of worsening data breach threats
- Lost business and/or ex-post response are increasingly becoming the main components of data breach costs in all countries surveyed

We analyzed these findings in light of a number of milestones in 2010 for global data protection and the fight against cyber attacks and data breaches. Governments took decisive steps to strengthen data privacy oversight while high-profile incidents continued to make headlines and damage lives and businesses. IT and IT security, and especially data protection, for the first time have become top headline material in the global media. The issues even helped decide national elections in Germany in 2009 and Australia in 2010. These trends reflect the intensity of IT implementation challenges, regulatory requirements and data security threats companies worldwide face today.

As a result of these pressures, and responding to public demand, all countries studied have made improving cybersecurity a national priority. Germany, the United Kingdom and Australia gave their national data privacy offices additional powers. All governments surveyed except the United Kingdom introduced legislation to improve their powers to protect sensitive data. The U.S. Congress introduced numerous bills that made further progress toward a national data breach notification law. German lawmakers introduced draft legislation designed to improve data protection for employees. Australia and France, two countries without data breach notification laws, introduced landmark draft legislation that would eventually create them.

All these discussions about data breach prevention and notification are taking place while broader economic and technological trends are making data protection – and its absence during a breach – even more relevant. The stumbling global economy has forced many companies to reduce costs and improve efficiencies, leading to increased use of outsourcers, mobile technologies and application delivery models such as cloud computing. A major side effect of moving so much data 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.

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

Key Report Findings

Overall Findings

Average data breach costs overall increased in all five countries: The average organizational cost of a data breach this year increased to $4 million, up 18 percent from 2009. Actual costs varied widely by country but last year's relative rankings remained unchanged. The United States had the most expensive average cost of $7.2 million. Germany came in second with $4.7 million. The United Kingdom and France had nearly identical average costs at $3.1 million apiece. Australia had the cheapest average cost of $2 million.

Data breaches in 2010 cost an average of $156 per compromised record, up $14 (10 percent) from 2009. The United States had the highest cost per compromised record, $214, followed by Germany at $191. The other countries had substantially lower costs – France at $136, Australia at $123 and the United Kingdom with the lowest at $114.

Breach costs correspond with national data protection priorities, especially regulatory compliance: 2010 marked the first time that regulatory compliance surpassed data breach mitigation as the main driver behind U.S. companies' implementation of encryption technologies (and, by extension, other data protection technologies). In Britain, defending against malicious or criminal attacks and lack of internal preparedness and expertise appear to drive costs. German breach cost trends may indicate that the strengthened federal data protection law is working, while in France regulatory compliance appears to drive spending. Finally, protecting brand and reputation appears to drive spending in for Australian companies.

Generally, costs are highest and rising the fastest for high-risk breach types targeted by laws and regulations and are lowest and rising the slowest, or even shrinking, for breach types not involving them: The highest costs in 2010 belonged to breach types that reflect failure to address the most prominent and dangerous data breach causes: malicious or criminal attacks, lost or stolen devices and third-party mistakes, along with overall lack of preparedness that can lead a company to become a first-time breach victim (first-timer). The opposite was also true: companies that avoided problems and had sufficient internal expertise and preparation (CISO leadership and quick response) to meet compliance demands fared better.

Across the board, companies are becoming more proactive in the face of worsening data breach threats: The willingness for companies in Australia, France and the United States to pay more – sometimes much more – for activities such as quick response and external consulting support may indicate that organizations are spending more on expertise to shore up their compliance (and thus avoid much greater expenses). The most frequent breach attributes overall are CISO leadership, external consulting support and above-average security posture – all of which reflect proactivity on the parts of their organizations. Taken together, these figures may indicate more organizations are taking more proactive steps to thwart hostile attacks in the worsening threat environment.

Lost business and/or ex-post response are increasingly becoming the main components of data breach costs in all countries surveyed: All countries except the United States reported higher spending on lost business than last year. All countries except Australia reported higher spending on ex-post response. Notification costs stayed flat in most countries surveyed, while detection and escalation costs varied.

The cost of lost business means consumers are concerned about how well organizations safeguard personal data. 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 detection and escalation and/or ex-post response could reflect increased compliance activities, as those two stages often require more investment than the notification process.

Manual, policy and training-oriented options remained the most popular post-breach preventive and remediation measures in most countries surveyed: Noticeable changes, however, are that American and French companies started relying more on encryption and other technological solutions. Germany kept its traditional preference for technological solutions but, for the first time, endpoint security solutions have overtaken expanded use of encryption as the most popular measure. Even though organizations still far prefer using traditional approaches, this year's figures may indicate companies are starting to see more value in technology that can help prevent and mitigate data breaches and meet compliance requirements.

Findings by Breach Type – Cause

Malicious or criminal attacks are still the most dangerous cause of data breaches: Malicious or criminal attacks remained the most common and expensive breach cause in all surveyed countries except Australia, where both breach cost and frequency dropped. The high cost may reinforce the extreme danger hostile breaches pose.

Breaches involving third-party mistakes by outsourcers are still a major worry and expense in all five countries: In Australia, third-party mistakes remain the expensive breach cause and, for the first time, are the most frequent cause and most expensive breach type overall. Our results may indicate that compliance with data protection regulations are slowly raising breach costs involving outsourced data in France and Germany but dramatically raising them in the United States. The marked drop in cost of third-party breaches among U.K. companies may indicate that organizations feel confident in securing outsourced data.

Breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat in all five countries: 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. German respondents found device-oriented breaches to be one of the top new data protection threats they face, with frequency rising and costs up from last year. In France, Australia and the United Kingdom, these breaches may reflect anxiety about insecure use of mobile technologies.

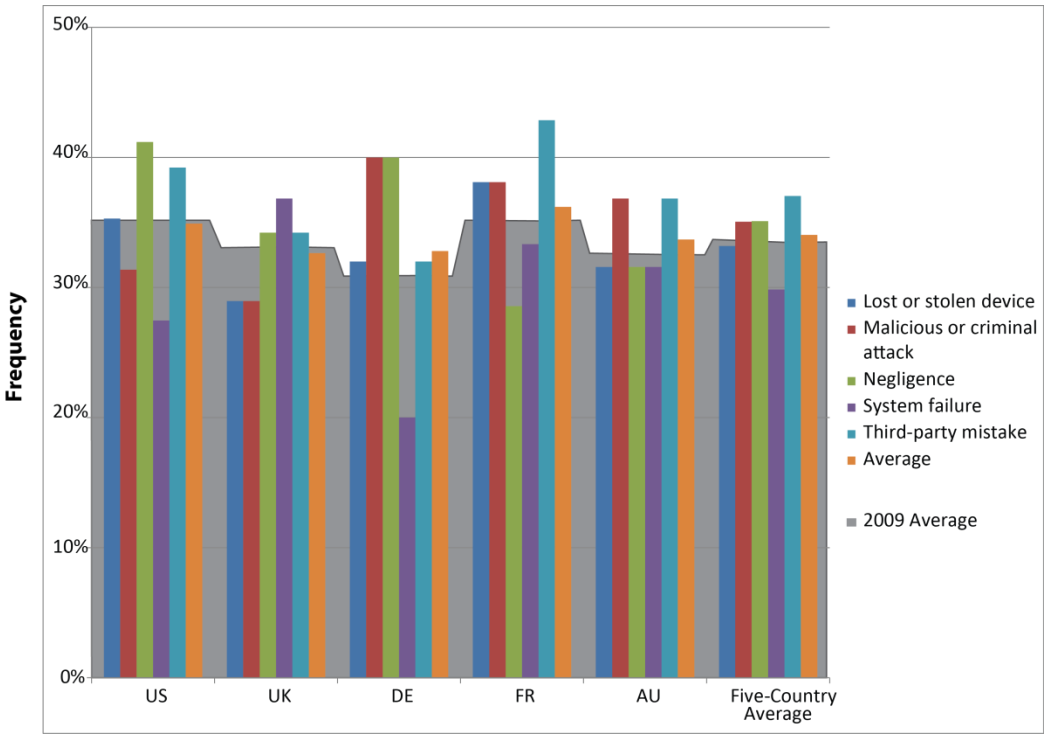

Figure 1: Frequency of data breaches by cause, 2009-10

Negligence is generally becoming more common and expensive: Australia, Germany and the United States all saw the frequency and cost of negligent breaches rise, sometimes sharply. These figures may indicate that employee and partner compliance remains an ongoing challenge. Costs rose sharply in Great Britain but the frequency fell.

Systems failures are becoming more prevalent but less worrisome: Every country surveyed save the United States reported more breaches due to systems failures. France, Australia and the United States all saw cost increases, while Germany and the United Kingdom saw their costs drop. Companies' increasing focus on data breach mitigation and regulatory compliance may be encouraging them to discover more systems failures behind data breaches – especially because systems failure costs were consistently among the lowest in this study.

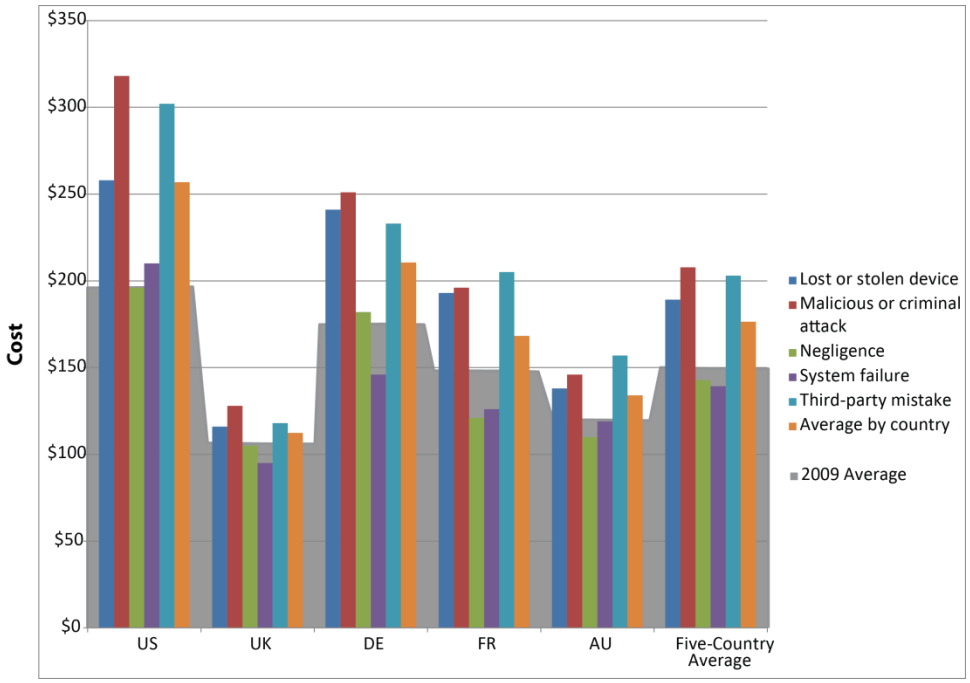

Figure 2: Average cost per record of data breaches by cause, 2009-10

Findings by Breach Type – Response

First-time breach victims are becoming more rare but still pay some of the highest costs: Breach costs for first-time victims were either the highest (France and the United States) or one of the highest (Germany and the United Kingdom) of all breach types. First-time Australian victims paid substantially less than data breach veterans. First timers saw sharp declines in Australia, France and Great Britain even as they remained the most common breach type in Germany and the least common in the United States. Increased compliance activities and prior breach victims may explain frequency rates, while experience may help companies manage costs better over time.

Quick response to breaches can save – or cost – a lot: Rapid reaction to data breaches (within 30 days) became more prevalent in all countries except the United Kingdom. Our results suggest that in the United States and France, moving too quickly through the data breach process may cause cost inefficiencies for organizations. In Germany and Australia, taking take longer to respond may cause inefficiencies. Interestingly, U.K. quick responders switched camps, paying much more instead of less. The notable increase in quick response, despite higher costs, may reflect pressure companies feel to comply with commercial regulations and state and federal data protection laws.

External consulting support is losing popularity in most countries surveyed: Fewer U.S. organizations are using external consulting support, even though such support lowers data breach costs. Fewer British and German organizations are engaging external consulting support to respond to breaches. Despite paying much more, more French organizations favor it. External consulting support remained the most expensive breach response attribute for Australian companies. Companies' concern about data breaches and regulatory compliance may drive some of them to acquire expert guidance from external sources, even if that significantly increases their costs.

CISO leadership for breach response saves money but still gets mixed reviews: More companies in Australia, France and the United States are trusting CISOs to better manage data breaches and reduce costs. Somewhat counterintuitively, CISO leadership is becoming much less popular with British companies – despite dramatically lowering breach costs and the fact that CISOs' strategic emphasis complements the high priority British organizations put on regulatory compliance and data breach mitigation. Increased compliance demands on organizations may be raising CISO-related costs in Germany, which may in turn be hurting their popularity. While CISOs' specialized expertise helps keep breach costs down, CISO-related costs are rising as organizations race to keep pace with escalating data protection threats and increased compliance demands.

Above-average security postures are common and cost-effective: Not surprisingly, organizations with a more favorable security posture (Security Effectiveness Score (SES) above the median) experienced lower average costs than those with a less favorable posture (SES below the median). Our research suggests that companies may exceed the SES median as they strengthen their IT security posture to meet regulatory compliance requirements.

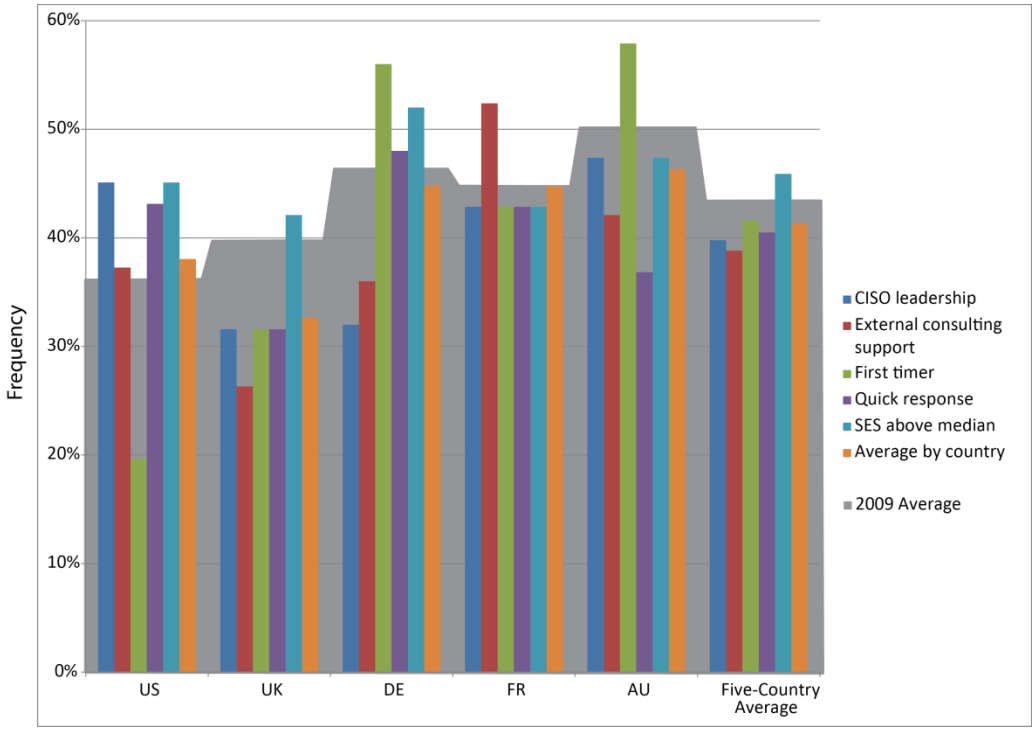

Figure 3: Frequency of data breaches by response attribute, 2009-10

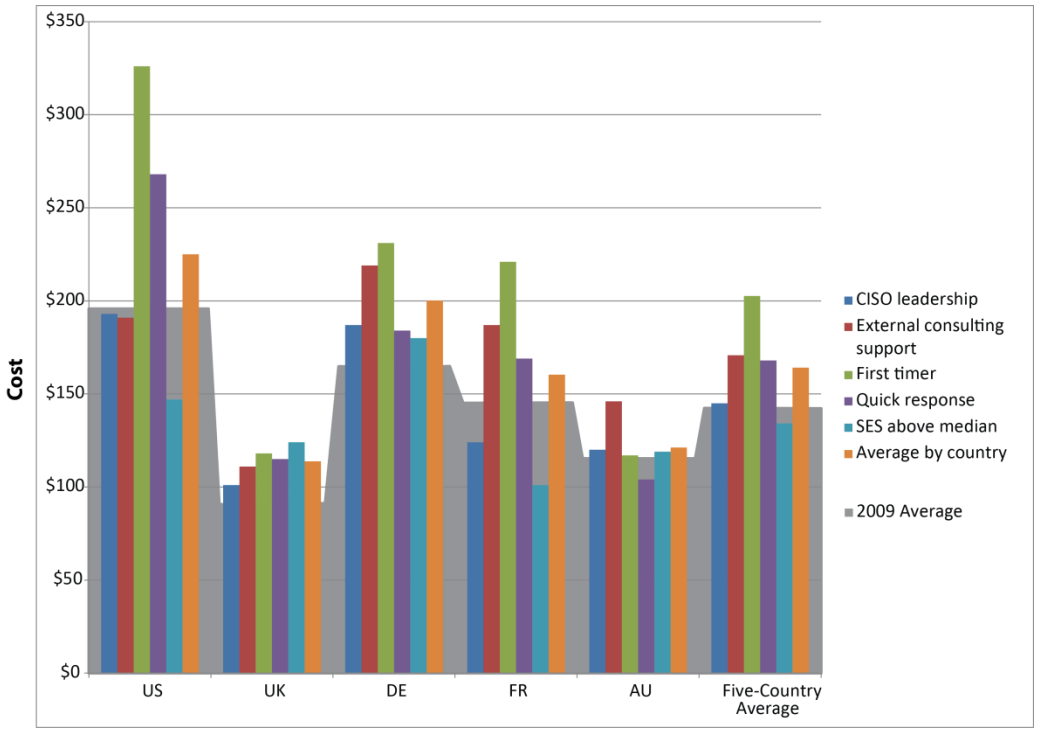

Figure 4: Average cost per record of data breaches by response attribute, 2009-10

Next Steps

Whether or not they have yet had a data breach, companies should also consider the following best practices:

- Pick responsible vendors and other third parties that can guarantee data protection through encryption and appropriate procedures and controls. Also, ensure that third parties protect data on staff mobile devices.
- Encrypt portable data-bearing devices. Consider implementing inventory control, anti-theft devices and data loss prevention (DLP) policies, practices and technologies.
- Take as thoughtful an approach to data breach response as possible. 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.
- Develop and practice a crisis management plan that clearly defines roles, duties, procedures and timelines.
- Empower CISOs or other security/privacy leaders to appropriately lead detection and notification processes. When in doubt, acquire counsel from external legal or technology experts to help improve breach response.

Study Overview & Methodology

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. 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. We believe the findings of this study are important because they can be generally applied to global organizations that experience large data breaches (between 1,000 and 100,000 compromised records).

Fieldwork for this research commenced in April 2010 and continued until January 2011. All organizations voluntarily agreed to participate with the promise of complete confidentiality and anonymity.