how to calculate the cost of a data breach
introduction

We see it time and time again: a well-known brand’s security is compromised. Millions of consumer records are exposed. The public becomes frantic. As brands, we watch from the sidelines, thankful that it wasn’t us – then we move on.

We think the unthinkable will never happen to our company. But in an age when so much sensitive information is housed, managed, and exchanged online, a data breach isn’t unthinkable at all.

Just last year, 50% of American adults had their private information exposed. And this threat is only growing.

In order to prepare your brand for these situations, you’ll need to first understand how much a data breach – defined as the loss of employee, customer, or other confidential information – would cost your company. While estimating the full impact of a data breach is no easy feat, putting together this estimate is crucial in allocating budget for crisis management planning.

In this report, we outline what your data breach cost estimate should encompass.

In 2014, 50% of American adults had their private information exposed.

Source: The New York Times
data breach costs: industry estimates

Many people underestimate the cost of a data breach, but its effects can be truly devastating. One estimate puts the overall cost of cybercrime against U.S.-based companies at a staggering $300 billion each year.

When it comes to calculating the cost of an individual data breach, there are two well-recognized models: The Ponemon Institute and the Verizon Data Breach Investigations Report.

The Ponemon Institute's 2015 Cost of Data Breach Study puts the average cost of a data breach in the U.S. at $6.5M. This is about $217 per record lost. Regulated industries have substantially higher costs – in healthcare, for example, the cost of a lost record is $398.

The Verizon Report, on the other hand, put estimated costs at $0.58 per record. This is significantly lower than the Ponemon Institute's estimation. They take a tiered approach, estimating the cost of a data breach as falling within a range of values.

At 100K records lost, the cost is between $366K and $614K; at 1M records lost, the cost is between $892K and $1.78M; and at 10M records lost, the cost is between $2.13M and $5.24M.

Both models put the direct cost of a data breach well into the millions. But this is really just the tip of the iceberg.

the costs companies don’t know about

When calculating the cost of a data breach, you need to take into account the damage caused from social media backlash and long-term media coverage. In the age of social, the price paid for negative public sentiment and damaged reputation can far surpass that of the actual crime itself. Your crisis will travel across dozens of digital channels, countries, and headlines, picking up more steam (and comments) as it goes along. In just a few hours, it’ll make an impression on billions of customers across the globe.

Even once your data breach has been resolved and the court fees settled, your crisis will live on. Once your reputation has been tarnished due to a data breach, it’s an uphill battle to prove to your scorned customers that you’ll ameliorate the situation. That you’ll do a better job of protecting their private information. That they can trust you again.

As a result, your business will lose current customers, as well as confidence from prospective customers. The Ponemon study found that the average cost of lost business (e.g., costs from customer turnover and increased activities to acquire new customers) was $1.57 million. A recent Deloitte study echoed those findings – 59% of consumers would be less likely to buy from a company that they knew had experienced a breach.
how to calculate the cost of a data breach

When calculating the cost of a data breach, there are two main categories: short-term and long-term. The former refers to costs occurring during the actual data breach. Long-term costs are ones that are ongoing for weeks, months, and even years.

In both categories, it is important to include both direct costs – the actual cash outlays your company is paying – and indirect costs, such as employee time or loss of future revenue.

The goal in these calculations is not to arrive at exact figures, but rather to determine ballpark values and shed light on areas of cost you perhaps hadn’t considered. This exercise will better inform your crisis management, as well as security software purchases.

SHORT-TERM COSTS OF A DATA BREACH

DIRECT COSTS
Detection
When your company is hacked or records have been stolen, the first order of business is determining the source of the leak, where the responsibility lies, and how it can be stopped. This often involves engaging forensic experts to determine the cause of the data breach, which can run anywhere from $200 to $2,000 an hour. Additional costs can include immediate hardware or software purchases to ensure there are no continuing vulnerabilities.

Escalation
Once the information is no longer directly compromised, additional costs will involve the escalation and notification of the proper individuals in your company. While these costs are for the most part internal, contracted companies may assist in this dissemination of information.

Notification
The next step in the face of a data breach is external communications. Depending on the size of your company, a PR firm or communication specialist may be hired to assist. Other costs include mailings to notify impacted customers, outsourcing and training hotline support to answer any questions, and website alteration to add FAQ pages and contact information. Charges for notification costs vary by type, but can range between $0.50 to $5.00 per record.
INDIRECT COSTS

During the time of a data breach, it’s most likely that many teams will drop their day-to-day work to help in mitigating the effect of the breach. In this case, the employees’ time and the work they are forgoing is a significant, yet often overlooked, cost. Normal business could be stopped for weeks at a time. In particular, the precious time of executives and C-suite individuals is often required for press conferences and outreach, as well as overseeing preventive activities. The loss in employee time can be converted to dollars lost with a simple equation:

\[
\begin{align*}
\text{Days Lost} & = \frac{\text{Hours Spent Away from Normal Work}}{8 \text{ Hours per Workday}} \\
\text{Dollars Lost} & = \frac{\text{Days Lost} \times \text{Average Salary}}{260 \text{ Work Days per Year}}
\end{align*}
\]

Depending on the severity and cause of the breach, individuals may be let go from the company, generating increased recruitment and training costs, which can be sizable depending on seniority.

LONG-TERM COSTS OF A DATA BREACH

DIRECT COSTS

Customer Cost
Your company will owe customers reimbursement of any fraudulent credit card charges or other expenses made in their name, as well as fees to cancel cards and recover their information. Depending on the severity of the breach, your company may also need to provide free credit monitoring subscriptions or identity protection, which can cost between $8 to $12 per month, per victim.

Legal Costs
When customer data is compromised, legal action is sure to follow. Companies must be prepared to address lawsuits including negligence, failure to protect data, and violations of various state and federal laws. In addition, depending on the industry, your company may also be facing compliance fines, especially in the financial or healthcare industries. If the data breach originated from inside your company or there was negligence involved, an internal investigation or audit from a third party may also be necessary.

Reputation Costs
In order to preserve and rebuild brand equity following a data breach, your company may need to activate additional marketing and communications campaigns. Costs surrounding these activities include continued support from a PR or advertising agency, media spend (particularly digital), and discounts on future products or services.
INDIRECT COSTS

Indirect costs are likely to include a continuation of the costs taken on during the crisis itself, such as loss of employee time and deferring of business as usual. These activities will gradually decrease depending on the size of the crisis and amount of resources hired outside of the company. Continued internal communication and investigation will also be necessary in order to follow up on items that may have been deferred during the crunch time of the crisis (such as cost tracking).

One particularly damaging aspect of a data breach is decrease in future revenue due to loss of customers. This is seen in two forms: turnover of existing customers, especially those who were directly affected by the breach, and loss of future customers. The more press and media coverage on the crisis, the larger these numbers will be. The Ponemon Institute found that companies in certain industries – i.e., health, pharmaceutical, financial services, and service organizations – are more susceptible to customer turnover and have churn rates as high as 6.1%.

Today, the loss of current and future customers is particularly exacerbated by social media, as individuals are able to share their stories and voice their frustrations on a much larger scale than ever before. In fact, negative sentiment around a brand will increase 35% during a data breach (Sprinklr, 2015). Weaving a social media management strategy into your overall crisis management plan will assist in mitigating this loss in revenue.

THE IMPORTANCE OF PLANNING

Data breaches can be one of the most costly types of crises to hit your business. Making governance and compliance a priority in your day-to-day operations and ensuring you have proper infrastructure across all aspects of your business will help you prepare against such an event – saving your brand millions in the long run. And most importantly, it’ll help you maintain trust with your customers.
Sprinklr is the most complete enterprise social technology in the world, purpose-built for global brands to drive business outcomes and manage customer experiences across all touch points. Called “the most powerful technology in the market” by Forrester Research, Sprinklr's fully integrated social media management software powers more than four billion social connections across 77 countries. Headquartered in New York City with more than 900 employees globally, Sprinklr is revolutionizing customer engagement for more than 1,000 top enterprise brands, including IHG, Intel, Microsoft, Samsung, and Virgin America, and partners like Deloitte, Accenture, R/GA, Golin, and AKQA. For more information, visit sprinklr.com or tweet us @sprinklr.