SpinOne

The Cost of Data Breach – Calculate the ROI of Backup and Disaster Recovery

- Common cybersecurity misconceptions
- Causes of data loss
- The cost of a data breach
- The ROI of cloud-to-cloud backup

Your data has become more valuable than ever before! With the rising cost and value of your data, there are also numerous threats to that data across the board. This can include the ever-growing threat of malware such as ransomware and other cybersecurity threats, or it could be the threat posed each and every day from end-users who may mistakenly delete business-critical data.

The cost of a data breach is rising exponentially. Even with a single data breach or data loss event, the ROI of backup and recovery software proves to be well worth the cost. Why is the cost of data breach so enormous? Why are backups critically important to your business continuity? Let’s look at the cost of a data breach and calculate the ROI of backup and disaster recovery software.

SpinOne

Contents

01

CYBERSECURITY MISCONCEPTIONS

SaaS Data Protection Guide

What businesses get wrong about data security

Today, data has often been described as the most valuable asset your business holds. This is because data is at the heart of most business activities. With online sales and e-commerce driving most industries, data is central to business success or failure.

When you think about the complex technologies, infrastructure, and cloud solutions that we invest in, their purpose is to support, transmit, and store your business-critical data. The value of your data cannot be emphasized enough. All too often, you hear of companies that were so focused on growing their business and reaping the rewards of success, they failed to properly think about protecting their data.

Data protection is just as important to think about in cloud environments as it is on-premises. You may have migrated at least part of your data to the cloud. Do you have a backup solution to protect your data there? Many businesses may fail to back up their business-critical cloud infrastructure as they may mistakenly view data protection as an unnecessary expenditure on a solution that is not needed. Many may be under the impression that cloud environments are immune to data loss. This is simply not the case. Consider the recent Amazon data loss event where a large chunk of customer data was lost.

Another misconception, especially among small to mid-sized businesses, is they may not be a target of a cyber attack due to their small size in comparison with other targets of attackers. However, this type of mindset is extremely unwise as attackers are targeting a wide range of business sizes and industries. In 2019, there has been an uptick in coordinated ransomware attacks that have targeted hospitals, schools, media outlets, and public offices.

So far, we have spoken in general about the value of your data and the threat from data breach. What are the underlying causes of a data breach?

Causes of Data Breach

Data Breach can be the result of many different kinds of events. However, the three most common causes of a data breach are:

- Malicious cybersecurity or criminal attack
- System glitch
- Human error

Ransomware can render your data useless

Any of these events can lead to grave consequences for your business's financials and customer confidence. What are those costs?

THE COST OF DATA BREACH

How Much Does a Data Breach Cost a Company?

Let's take a look at the question – how much does a data breach cost a company? While this can be answered in general terms, let's look at real data breach numbers and what it could wind up costing you and your business. Each year, IBM Security releases a study called the Cost of a Data Breach Report. This year's report contains some alarming numbers when it comes to what data breach can actually cost your business.

The average cost of a data breach includes the following global averages:

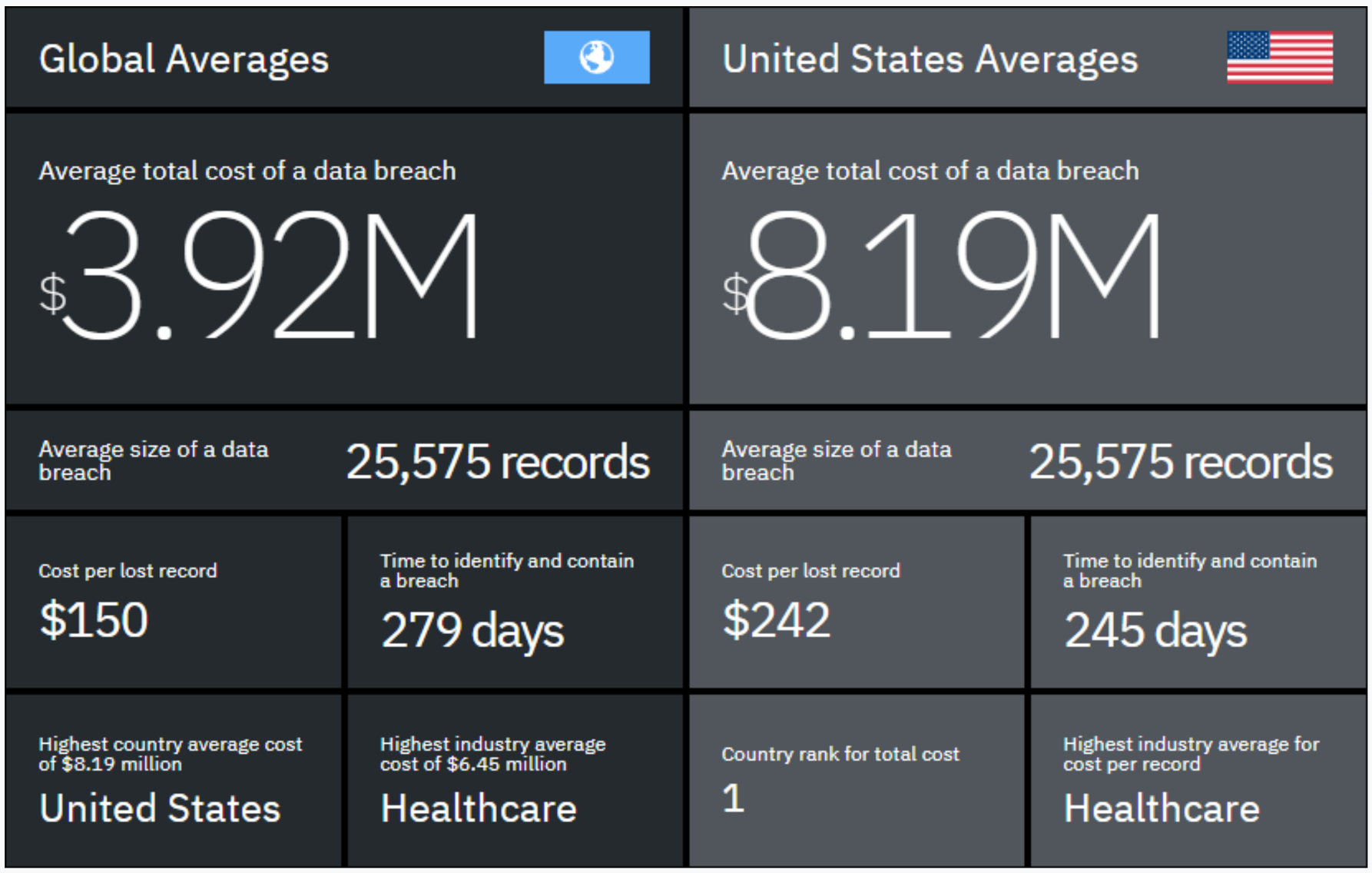
- $3.92 million average total cost of a data breach
- Average size of a data breach - 25,575 records
- Cost per lost record $150

More specifically, the United States saw the highest cost of a data breach in 2019, with the following:

- $8.19 million average total cost of a data breach
- Average size of a data breach - 25,575 records
- Cost per lost record $242

Healthcare was the highest industry average for cost per record and highest industry average:

- $6.45 million – average cost of healthcare data breach



IBM Security Cost of Data Breach in 2019 (Image courtesy of IBM)

Where Data Breach Costs Come From

When you examine where the costs come from in the case of a data breach where data is lost or stolen, there are many different areas where your business can be affected by a data breach, including long-term effects that need to be considered.

Lost Customers

One of the major factors that costs your business in the event of a data breach event is lost customers. When the news of a breach makes headlines, regardless of whether or not the breach is your fault, this can leave consumers who may have been future customers wary of doing business with you. Current customers whose data may have been lost or stolen will most likely no longer have confidence in your business handling their data.

Long-Term Effects

Keep in mind these types of costs can remain long term, lasting even years down the road. Some 22 percent of data breach costs can happen in year two, after the breach. And an 11 percent cost of breach can happen more than two years afterwards! The effects are long lasting!

Legal and Other Fees

Additional costs of data breach can result from legal fees, third-party security firms, and internal time and administrative effort spent “cleaning up” after a data breach event.

Fines

Let’s also not forget very recent GDPR fines and penalties that can cost businesses more than the actual data breach event. GDPR fines and penalties can cost a business significantly. GDPR fines consist of up to 10 million euros or 2% of its entire global turnover of the preceding fiscal year, whichever is higher.

How are GDPR fines determined? If there is a punishable situation in a company, that is revealed through proactive inspection activities. Was the company negligent in protecting the data of is customers? Was there gross mismanagement or lack of proactive protection of the data?

So, keep in mind that on top of the cost of the actual breach itself, your business can potentially be at risk of GDPR fines if subject to the purview of the EU. Considering the potential cost of data breach, it is absolutely necessary for your business to think about how data is protected.

One eye-opening aspect when looking at the cost of data breach is that cloud migration and housing your data in the cloud can actually increase data breach costs. This is due to the additional complexity that housing data in the cloud brings to your infrastructure.

In addition, misconceptions concerning the protection of your cloud data as mentioned above as well as a lack of processes and solutions in the cloud to protect your data can lead to greater data breach costs.

02

THE ROI OF CLOUD-TO-CLOUD BACKUP

SaaS Data Protection Guide

It's better to be safe than sorry

Let’s focus on data loss as a result of a data breach. After looking at actual numbers making up the cost of a data breach resulting in lost or stolen data in 2019, your business would see an immense ROI for a backup and recovery software solution protecting your data.

If your business has migrated business-critical data and services to Software-as-a-Service environments such as Google G Suite and Microsoft Office 365, you need to have an effective cloud-based backup service in place to protect this data in the cloud. The fine print included in most public cloud vendor SLAs points to the fact that your data is your responsibility, not theirs.

Cloud-based backup solutions allow you to make use of a DR-as-a-Service configuration for protecting your business-critical data. Cloud-based backups allow you to have an effective way to protect your SaaS data such as Google G Suite and Office 365 by copying your data to a protected cloud environment for the purposes of backup.

This helps to ensure that your backup data is protected from accidental deletion or encryption by malware. The only access to your backup data is for the purpose of recovery in times of disaster, including ransomware attacks that render your business data useless.

03

MAKE THE RIGHT CHOICE

SaaS Data Protection Guide

SpinOne – The Best Cloud-to-Cloud Backup Option

When choosing a cloud backup solution, you want to make sure your data is stored outside of the cloud environment you are protecting. This helps to make sure that in the event your production cloud vendor is having issues, your backup data is still accessible. This is in harmony with the 3-2-1 backup best practice methodology. Its core principle is based on the fact that you never want to have your backups housed in the same environment as your production data.

To follow this principle, if you are using Office 365, you would want to have your backups housed in a different public cloud outside of Microsoft's public cloud infrastructure is perhaps Google or Amazon. This helps to diversify where your data is housed.

As an example of a cloud-to-cloud backup solution that allows you to diversify where your data is stored, SpinOne provides great options to store your backups in different cloud environments than where your data is stored. You can choose from Amazon AWS, Google GCP, or Microsoft Azure as the target for your backups.

Along with offering options on where to store your data, you get all the options needed to protect critical data in the cloud including automated backups, unlimited retention, encrypted backups, granular restores, data migration, and data downloads.

SpinOne provides backups and cybersecurity for Software-as-a-Service environments like G Suite and Office 365

Aside from backing up your data, SpinOne offers a full cybersecurity suite of functionality to protect your SaaS environments from the cybersecurity threats that lead to data breach in the first place.

Whatever solution you choose to backup and protect your data, backups are essential to being able to successfully recover from data breach events leading to data loss. Having cybersecurity protection to go along with effective backups can literally save your business millions along with the untold losses in customer confidence that can lead to years of losses as a result.

In the case of SpinOne, how does the cost of a breach ($242 per record in the US) compare with the cost of backing up your data?

- Google G Suite - $3 user/month
- Office 365 - $3 user/month

The cost pales in comparison to the costs of data breach.

Concluding Thoughts

The cost of data breach is real. Your business could stand to lose millions initially and even more than that over time. Fines levied by GDPR and other compliance regulations can add to the cost of data breach significantly. Worst of all, customer confidence can be lost forever.

The ROI on your investment in effective data protection can be achieved very quickly, especially if you suffer a data breach. By using both good backups of your environments, including cloud, along with cybersecurity protection, you can offset many of the costs that otherwise could be detrimental to your business.

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)