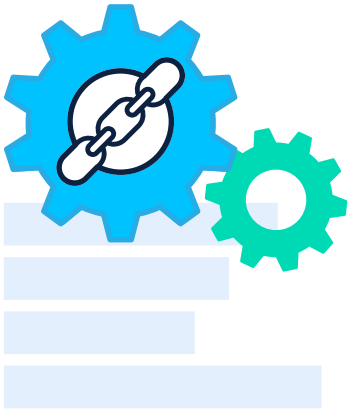
verbit

The Shocking Costs of Data Breaches

With a 10% rise in data breaches, ensure you're protected

Data breaches are on the rise. Major companies like **Facebook, Audi, Android and Microsoft are among the high profile victims this**[1] year alone. Now more than ever, it's essential to realize what's at stake when businesses fail to invest in their own security or vet that of their vendors. The numbers may be frightening, but there are simple ways to minimize these risks.

By the Numbers: The Impact of Data Breaches



The cost of an **average data breach[2] in 2021 increased 10% over last year, adding up to $4.24 million**. For some companies, the costs are far higher. The expenses fall into several categories, including:

- Lost business: **This factor accounts for around 40% of the total costs[3] related to a data breach**. Businesses may lose revenue because their system is down after the incident or due to customer turnover. Then, there are the added costs of attracting new customers following bad press related to a breach.
- Fines: Companies that fail to comply with data security regulations may face hefty fines. For example, the Federal Trade Commission, the Consumer Financial Protection Bureau and several state regulators fined Equifax after the credit reporting agency failed to take appropriate action to remedy known security risks. **The agreed-upon amount is $575 million[4] but could eventually reach $700 million.**

- Monitoring after a breach: Credit monitoring for victims can become a company's responsibility following a breach. **Premium monitoring can cost between $8.99 and $35.95[5] per month for each affected person.**
- Investigations: Following a breach, companies may hire investigators to identify the cause and prevent future incidents. **Those costs can amount to more than $100,000**.
- Loss of consumer trust: **Companies can permanently lose more than 40% of their customers[6] because of a data breach**. The tarnished reputation can extend for years, especially in high-profile cases.
- Stock decline: Stock prices for companies tend to dip after data breaches. **Macy's stock value dropped 11%[7] when it announced that it was a victim of a sophisticated cyber attack.**

The Human Cost of a Data Breach

Consumers face real consequences when companies don't protect their data. Given these high stakes, it's no wonder that people are likely to hold a grudge when a provider fails to maintain proper security.

- Identity theft: It's one of the most common consequences of a data breach. When credit reporting agency Equifax fell victim, they exposed Social Security numbers, home addresses and birthdates of **nearly 150 million Americans**.
- Credit card fraud: Target suffered a data breach that exposed over **41 million customer payment accounts**. The attack allowed hackers to commit credit card fraud and other scams on the retail giant's customers.
- Phishing scams: A Marriot International data breach exposed information including passport numbers, mailing addresses, email addresses, flight departures and arrivals and phone numbers for **up to 500 million guests**. The attack exposed customers to social engineering and phishing attacks.
- Blackmail: AdultFriendFinder sustained a data breach that exposed user data for **412 million accounts**. Because of the nature of this website, hackers could blackmail users with the threat of exposing embarrassing or reputation-ruining information.

Outside Vendors: Security is Only as Strong as its Weakest Link

Consumers who learn of a data breach will blame the company they have a relationship with, not the vendor, even if that third party is at fault. Given that the average company in 2020 used 80 Software as a Service (SaaS) apps[8], there are many players handling each company's data making security vetting practices critical.

Protecting Businesses Using Outside Vendors

- Look for **Service Organization Control 2 (SOC 2) compliance**. The American Institute of Certified Public Accountants (AICPA) created these standards to evaluate third-party vendors and determine if they adequately protect the information that they receive from clients.

As Verbit handles sensitive information contained in transcription work, among other services, its leaders take significant privacy measures to ensure all data and information contained in these transcripts remains secure. Sensitive information is regularly shared in legal proceedings, business meetings and university classrooms. When producing and obtaining transcripts in these scenarios, SOC 2 Type II and HIPAA compliance must be met. Verbit provides top-level security and meets these standards to offer clients peace of mind.

verbit

To learn more about how to implement Verbit's technology, including captioning and transcription solutions, in order to offer accessibility and meet legal requirements, reach out. If you're using automated or free transcription tools, your data is likely not secure and exposing it will cost you. Protect your data and **contact Verbit**.