Brandon Creech

November 22, 2024

# Data Breaches

## Introduction

In today's online world, the functionality of technology in our daily lives has become fundamental to our desires. However, increasing dangers and malicious cybercriminals online highlight the importance of security and how vigilance remains a virtue. Despite preventative efforts, anyone can become a victim of data breaches when their personal information is in possession of a company for their security. To put it simply, data breaches are a method of attack for cybercriminals in which they breach security infrastructures of a company in order to take the personal information of the customers the company swore to protect. This unauthorized access proves to be deadly as it costs countless companies millions upon million dollars lost. A lot of times these incidents happen not only because of how clever the cybercriminal is, but also because of weaknesses found within the company, whether that is the security infrastructure itself or employee knowledge. Data breaches can arise many ways, such as through phishing or malware for example, where emails and files can be served as bait to take an innocent person's personal information. Once a data breach has been committed, the personal information of customers is no longer safe which is why data breach remains to be one of the deadliest forms of cyberattacks in recent decades.

## Facts and Figures

To better understand the consequences data breaches can have on both companies and customers, let's look at the facts and figures surrounding data breaches. Firstly, we can say that overall, data breaches are currently trending in the wrong direction. We are facing an insurgency in security incidents that has caused alarms to be raised in IT infrastructure. Take a look at the chart to the right by IT Governance USA; companies are starting to experience an increased likelihood of security incidents involving data being breached. This means that customer personal information is becoming more frequently compromised and likely to become compromised. The technology world is becoming far less secure to the point that we can't trust our personal information in someone else's hands. If we look back at the historical data of data breaches, 2005 marked the year of the first recorded data breach that "exposed more than one million records" (Sobers 2024). Now put this fact into perspective, if we consider the increasing frequency of security incidents coupled with the number of records being exposed, we are looking at a dangerous future in which data breaches are more frequent and the number of records being exposed ever increase. Numerous companies have already reported historical numbers of records being exposed this year. For example, Dell, a highly renown technology company, reported a data breach in which 49 million records were exposed in this cyberattack.

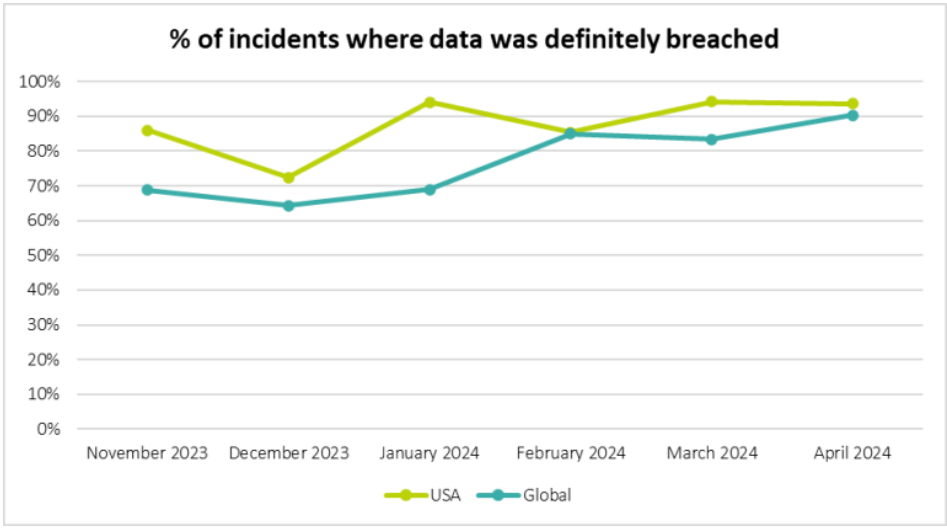


*Figure 1 - Source: IT Governance USA*

Dell was also not aware of the activities until after the fact of what happened (Bluefin 2024). I consider this an important thing to consider for a specific reason: cybercriminals are becoming more sophisticated in their attacks in recent years, which means that they are starting to develop tactics that let them be able to slip under the radar. This is a bad recipe if you combine this with other reasons that data breaches can happen such as weak security infrastructure or employee inadequacy. We are looking at a deadly future in the technology world not just for these companies, but also the customers as their trust are put into the hands of the companies to secure their data. As quoted by VentureBeat, "consumer confidence in online organizations' ability to protect their data is misaligned with reality" (Sevilla 2022). With data breaches becoming increasingly deadly, it is hard to trust them now when anyone has the possibility to be a victim of a data breach.

However, there is news about data breaches that shows efforts are being put in to mitigate the losses associated with them. Although it is hard to predict the chances of a data breach happening, companies are able to put forth the effort that both reduces the personal information exposed and scale of the data breach overall. Judgment can be made by the two following charts by HIPAA Journal that shows the rapid escalation of large-scale data breaches in the healthcare industry, but then take a dip this year. While

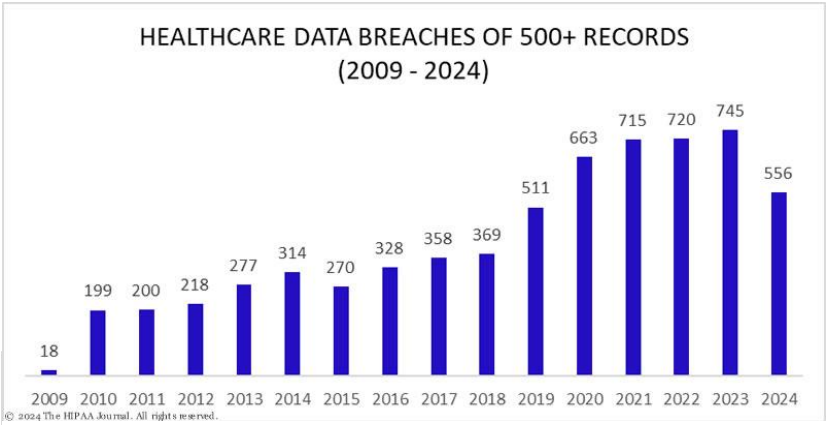

*Figure 3 - Source: HIPAA Journal*

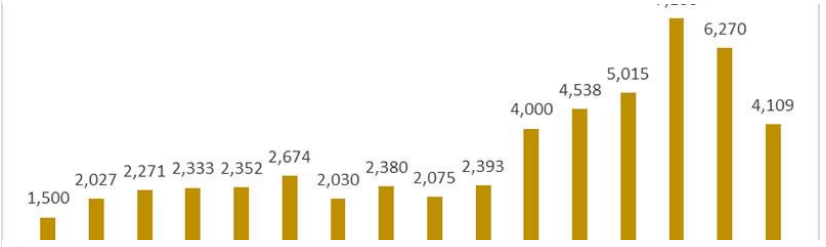

*Figure 2 - Source: HIPAA Journal*

it is important to note that this is just a small blip on the damage data breaches causes annually, we can recognize that it is possible for companies to act in mitigating the damage data breaches can cause overall.

Next, there are plenty of ways that companies are addressing data breaches. Companies have looked towards multiple sectors of their security to help mitigate data breaches. One way is through allocating funds towards increasing security budget, which means many implementations can be done towards improving security such as better infrastructure, employee training, and detection programs that can stop malicious forces swiftly. Respondents from IANS and Artico Search have reported an increased average of 6% in security budgets in 2023. While this may be important in addressing data breaches, Nick Kakolowski, the Senior Research Director of IANS, believes this will not be enough to deal with the threats that exist (Help Net Security 2023). Other companies are taking measures that involved changing their current system of security and reforming it for the sake of improvement. Such companies are reforming their systems, in which approximately 63 percent of companies are now using a biometric system or are planning to (Sobers 2024).

## Moving Forward

Considering the facts given from the statistics, how companies are handling data breaches, and the current trends of security. It is hard to judge exactly of what direction these companies heading into. On one hand, statistics have gone down a year, signaling a potential sign of improvement in security and reassurance for customers on data protection. However, on the other hand, statistics still remain historical in data breach financial loss and some customers

still have trust issues over personal data handling. Cybercriminals also find new ways to infiltrate data infrastructure, which means that surprises can be brought up to these companies. One thing is for certain, as long as technology continues to evolve, data breaches will always remain a constant threat in the cyber world.

## Conclusion

In conclusion, companies will always be in a war against cybercriminals over data breaches. Data breaches will never be able to go away. Protection of customer data is top priority, but the constant threat and financial loss from data breaches will always reside over companies. The best that companies can do is to improve security infrastructures by maximizing their budget. This means investing in costs that help stop or prevent data breaches such as employee training or reforming into a biometric system. Implementing these tactics may not stop data breaches altogether, but it can help reduce the losses and stop them from creating further damage after it has happened. Data breaches are hard to overcome but having resilience can help both companies and customers in the long run.

## Summary

- Data breaches remain a consistent threat to the cyber world, both companies and customers alike.
- Although statistics have went down a year, it can not be undermined that it still remains historical, and that customer data security is top priority.
- Data breaches cannot be stopped. But they can be mitigated and stopped swiftly after they have happened through various tactics companies have developed.

- Companies and customers alike will always be in a constant war against cybercriminals and data breaches.

## Glossary

- **Data breach –** A breach of infrastructure in a company in order to steal personal information.
- **Cybercriminal –** A criminal that does malicious activity online.
- **Infrastructure –** The technical dealings within a company consisting of fortified firewalls, systems, and employees that all work together to stop and prevent malicious activity.
- **Phishing –** Used commonly in data breaches, it is a method of scamming that cybercriminals use to steal personal information by using bait links.

**References**

*Data Breaches and Cyber Attacks – USA Report 2024*. IT Governance USA Blog. (2024, June 19). https://www.itgovernanceusa.com/blog/data-breaches-and-cyber-attacks-in-2024-in-the-usa

Sobers, R. (2024, November 15). *82 Must-Know Data Breach Statistics [updated 2024]*. Varonis. https://www.varonis.com/blog/data-breach-statistics

*The Biggest Data Breaches of the Year (2024)*. Bluefin. (2024, July 10). https://www.bluefin.com/bluefin-news/biggest-data-breaches-year-2024/

Alder, S. (2024, October 24). *Healthcare Data Breach Statistics*. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Sevilla, G. (2022, December 13). *33% Of Consumers Are Victims of Data Breaches on Companies That Are Tasked with Keeping Their Data Safe*. EMARKETER. https://www.emarketer.com/content/33-of-consumers-victims-of-data-breaches-on-companies-that-tasked-with-keeping-their-data-safe

*Cybersecurity Budgets Show Moderate Growth*. Help Net Security. (2023, September 27). https://www.helpnetsecurity.com/2023/09/29/cybersecurity-budgets-growth/