UnitedMail

October 2019

Data-Security in the Digital Age

The importance of dependable data-security at a time when data is vital and breaches are frequent

Table of Contents

Abstract

Between February 2018 and March 2019, the American Medical Collection Agency suffered a breach that impacted over 20 million customers. The medical data and financial information, including bank account details of those 20 million people, collected under the American Medical Collection Agency were accessed in a targeted breach that left Retrieval-Masters Creditors Bureau Inc., the parent company, filing for Chapter 11 bankruptcy. During the same time period, car manufacturer Toyota suffered a breach that affected over 3 million people, and social media platform Evite suffered a breach of their own that impacted over 10 million. This isn't a new phenomenon either. Yahoo might still have to pay out customers affected by breaches occurring as far back as 2012, and a Marriott data breach made headlines just last year when hundreds of millions of people had their passport and credit card numbers stolen. In 2017, Equifax was investigated by the Federal Trade Commission for a massive data breach that targeted the personal information of over 140 million accounts. With rising economic tensions and pressures, we can safely say that everyone who stores data is a potential target, but that doesn't mean there aren't steps that can be taken to prevent these data breaches.

What We'll Cover

First, we will discuss the largest data breaches in further detail, and the impacts of thereof, both for the involved companies and their customers. Next, we will go into detail about the symptoms of vulnerable data storage. Finally, we will go over the steps that can be taken to prevent these data breaches from occurring in the first place.

Overview:

- Data Breaches
- Data Vulnerability
- Data Security

Data Breaches

Yahoo! - The Widest-Scale Breach to Date

Back in 2016, Yahoo! finally reported that its 3 billion accounts had been hacked between 2013 and 2014. During these two security breaches, unprecedented in scale, account holders' names, birthdates, email addresses, and passwords were accessed and circulated.

Although Yahoo! only reported the first announced breach in 2016, the breach had occurred in late 2014. This breach affected over 500 million Yahoo! users. A previous breach, occurring around August 2013, was reported at the end of 2016. Initially believed to have affected a still-unprecedented 1 billion or so Yahoo! users, the company later confirmed in 2017 that all 3 billion of its user accounts were impacted.

At the time, both breaches were considered the most wide-scale breaches ever uncovered. Yahoo! as a company may never be unseated in its record of the sheer number of people affected. Information accessed includes not just names, email addresses, and telephone numbers, but personal information like security questions and answers, dates of birth, and passwords.

A lawsuit about this breach is going to cost Yahoo!. Many of the billions of individuals impacted can be eligible for compensation thanks to a class-action lawsuit. Anyone with evidence of identity theft damage might be entitled to $375 per person.

The Aadhaar Database - Biggest Breach of Citizen Data

In India, the Aadhaar government ID database suffered multiple breaches that compromised the records of all 1.1 billion registered citizens. This unprecedented breach of citizen data allowed anyone willing to pay a nominal fee to access the information of any of the 1.1 billion users. While exploiting various security glitches and oversights, criminals sold access to the database at a rate of Rs 500 rupees for 10 minutes of access.

These data breaches cost organizations in India about ₹12.8 crore on average, or around $1.8 million, between July 2018 and April 2019, according to a security report sponsored by IBM. The unprecedented per-capita cost per lost or stolen record was ₹5,019, or about $150 per record.

First American Financial Corp - Hundreds of Millions of Title Insurance Records

Real estate title insurance giant First American Financial Corp leaked hundreds of millions of documents related to mortgage deals as far back as 2003. Some 800 million records, including bank account numbers, bank statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and driver's license images, were available without authentication to anyone with an internet connection and access to any web browser.

First American Financial Corp reported almost $6 billion in revenue in 2018, it is perhaps the largest provider of title insurance and settlement services to the real estate and mortgage industries. As such, countless hundreds of millions of records exist in their data archives, much of it personal, financial, and sensitive. It's now confirmed that almost 900 million files accrued over the past decade and a half were made vulnerable. Much of the information was exploitable, including wire transactions listing bank account numbers.

It isn't currently known whether or not this information was exploited by anyone for nefarious purposes, nor if the information was mass-downloaded, only that the information was openly available, easy to access, and readily exploitable.

Equifax - A Targeted Hack Affecting Millions

Of similar exploitability, Equifax compromised the information of some 140 million accounts. Equifax is one of the top credit reporting companies in the United States, many Americans who had requested or received a credit report were potentially vulnerable. Information, including names, social security numbers, birthdates, and addresses, was hacked and circulated on the internet. It is reported that the company was aware of its online portal's security vulnerabilities before the massive data breach.

Those who incurred expenses in order to remedy their own personal fallout from the breach are entitled to compensation up to $20,000 per person. Others can also be compensated for the time they took in dealing with the breach. Impacted individuals can claim time lost at $25 per hour up to $500.

The Litany of Vulnerable Data Instances

The preceding instances might be the biggest examples of breaches and various types thereof, but they do not come close to encompassing the sheer number of breaches plaguing today's data-driven economies. There is a growing litany of instances of vulnerable data in terms of both the negligent availability of sensitive data and targeted attacks.

For example, JPMorgan Chase, the largest bank in the United States, experienced a major cyberattack in 2014. The personal data of 76 million households and over 7 million small businesses were breached. Vital information like social security numbers and bank accounts largely remained safe, but other incredibly sensitive personal account information, like addresses and buying and selling habits, became compromised. The issue cost the company not just credibility, but $250 million pledged to address the issues.

No one is immune. Even social media giant Facebook has some familiarity with data breaches. More than 540 million records concerning Facebook users were publicly exposed on Amazon's cloud computing service when two third-party Facebook app developers posted those records, allowing them to be easily accessed by almost anyone. Facebook is even under federal criminal investigation for deals it struck with electronics manufacturers to access user data, and it has been hit a series of security breaches over the past year.

Marriott leaked passport information and credit card details of millions of customers, and the American Medical Collection Agency leaked healthcare information for 20 million people. The list of data breaches is too exhaustive to enumerate in complete detail and more and more instances of vulnerable data and targeted hacks are added to that list each year. These leaks and attacks are ongoing, and the only way to prevent them is to understand the conditions that allow them to occur.

Data Vulnerability

Understanding the conditions that make data vulnerable is vital to understand the steps needed to keep it safe. Companies that need to keep large backlogs of user/client data — healthcare companies and insurance companies being prime examples — are inherently at risk of attacks and leaks. These massive stores of information are sensitive and easy to mismanage.

In the various aforementioned instances of data breaches, there exists a clear commonality of lax security and negligent oversight. Following is two examples detailing two specific situations of companies leaving data open to attack.

The Aadhaar Issues

A government utility provider called Indane was used to access customer information and verify customers via an unsecured endpoint. It was leaking data of all persons with an Aadhaar, exposing their names, bank details, and more personal info.

The only required input was an Aadhaar ID, which is just a 12-digit number. All anyone needed to access this sensitive information was 12 numbers. This means that anyone with a random number generator and enough time could brute force their way into countless user profiles.

What's worse, the Indane endpoint didn't just supply data about the utility provider's customers, but anyone with an Aadhaar. The user data wasn't kept in distinct silos with restricted needs-based access but was instead accessible freely to anyone with an internet connection.

Worse still, the flaw was understood by Indian authorities at the time, but they let it persist. They knew the system was flawed, the data was vulnerable, and the issue needed to be addressed, but instead, they denied the issues.

Marriott's Data Management Mess

Marriott's Starwood brands, which include the Westin, Sheraton, St. Regis, and W hotels, suffered another known lack of security. Before Marriott purchased Starwood, these Starwood brand hotels used a network that had already been compromised in 2014. Marriott purchased Starwood in 2016, and,

after two years, the former Starwood hotels still hadn't been migrated to Marriott's own reservation system and were still using inherently flawed IT infrastructure from Starwood.

What's surprising isn't that the attack happened in the first place — we know all too well that these attacks are common — it's that it went undetected for four years. It was only detected by chance by Infosecurity software that flagged unusual database queries. But it was too little too late.

Data Security

Learning from the mistakes of others is the first step in understanding how best to protect customer and client data from being mismanaged and wrongfully accessed. Data breaches are common, but not all attacks are successful. Avoiding the pitfalls of these other companies is a great way to shore up your company's data defenses.

As we can see with the ease of access in the case of Aadhaar ID information, keeping data separate and keeping access needs-based is a great way to start. The Aadhaar breach also readily illuminates another problem: unauthenticated access.

Unauthenticated access is poor security 101. The ability for anyone to simply generate a random string of 12 numbers and potentially access private information is something that should never have been allowed in the first place. Ideally, passwords should be required, and they should never be stored as plain text, and never on the same server as user or other log-in credentials information. Two-factor authentication is also a golden rule for data security.

Comprehensive monitoring is key. As we saw with the Marriott breach, which went undiscovered for four years, the security monitoring was simply not enough. Data protection and security should be a top priority for businesses that store sensitive information. It's not just a matter of trust, as we've seen the costs of repair can far exceed the costs of maintenance, so to speak. No one wants to open themselves up to legal action and compensation.

Knowing who to trust is also vital. As we saw with the Indian government, trusting Indane with Aadhaar information was a big mistake. And this is nothing new. Even when companies do everything right, and grant needs-based access to third-party collaborators, advertisers, or processors, those clients need to

be trustworthy themselves in order to be certain that the data turned over to them remains in safe hands. It is up to companies to do their due diligence to make sure that other companies they work with are equally trustworthy. Luckily, new regulations are making it more and more difficult for companies to fall victim to leaks and attacks. Better still, many companies elect to go above and beyond standard guidelines and additionally obtain further security licensure such as HITRUST CSF and SOC 2 Type 2 certification.

General guidelines, such as those set forth by HIPAA, are often too broad to be effective for the array of varied companies called on to follow these guidelines. Companies whose only benchmark for data security is loose guidelines like this are left without specific direction. Even successfully following these guidelines and frameworks does not guarantee the level of data security necessary in fields associated with high volumes of data and/or sensitive data. The need for specific, standardized, and proven data-security certification has never been greater, and the value of loose guidelines and unchecked standards has never been more inadequate. Furthermore, there is no legitimacy nor guarantee of data-protection in a company claiming to be HIPAA "certified," as no such process for certification nor status of certification exists.

On the other hand, HITRUST offers a third-party assessment (HITRUST CSF or Health Information Trust Alliance Common Security Framework) that actually does certify companies as meeting data-security protection standards through rigorous testing. HITRUST CSF certified companies are tested in the spirit of HIPAA guidelines (and additionally incorporating NIST, ISO, PCI, FTC Red Flag and COBIT guidelines/frameworks), but in a way that offers companies an actual path to certification. Companies who take steps to become officially certified are making large financial investments in order to ensure the safety and security of their customer and client data.

Similarly, SOC 2 Type 2 certification requires companies to comply with standard operating procedures for organizational oversight, the management of data to and from vendors, the minimization of risk, and a high standard of regulatory oversight. It is critical for anyone with sensitive data of any kind, large amounts of user data, personal information, or anyone who wants to keep their data protected from lapses and breaches to ensure that they are working only with companies that are officially certified by a rigorous third-party assessment such as SOC and HITRUST CSF.

Conclusion

Data leaks and attacks are common and disastrous. In an age where data is vital for businesses, the stakes have never been higher. Industry giants are not immune, suffering some of the largest hacks ever uncovered. Billions of people have had their data breached over the last decade, and reports aren't slowing.

There are common qualities of vulnerable data. Expert criminals are primed to take advantage of every security inadequacy from poorly authenticated log-ins to data made accessible by negligent partner companies.

The best way to ensure your data is safe is to make sure access is restricted, authenticated, and monitored, and assure that any shared data is in the hands of businesses and organizations that adhere to strict guidelines of data security and management. The best way to do that is to check that they are certified by trustworthy data security certification sources such as HITRUST CSF and SOC 2 Type 2.

References

https://www.natlawreview.com/article/licensed-your-state-s-insurance-commissioner-comprehensive-data-security

https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

https://www.bloomberg.com/news/articles/2019-06-17/american-medical-collection-agency-parent-files-for-bankruptcy

https://www.marketwatch.com/story/773-million-email-addresses-exposed-in-mega-data-breach-heres-how-to-see-if-yours-is-one-of-them-2019-01-18

https://www.infosecurity-magazine.com/news/twothirds-of-firms-have-suffered/

https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html