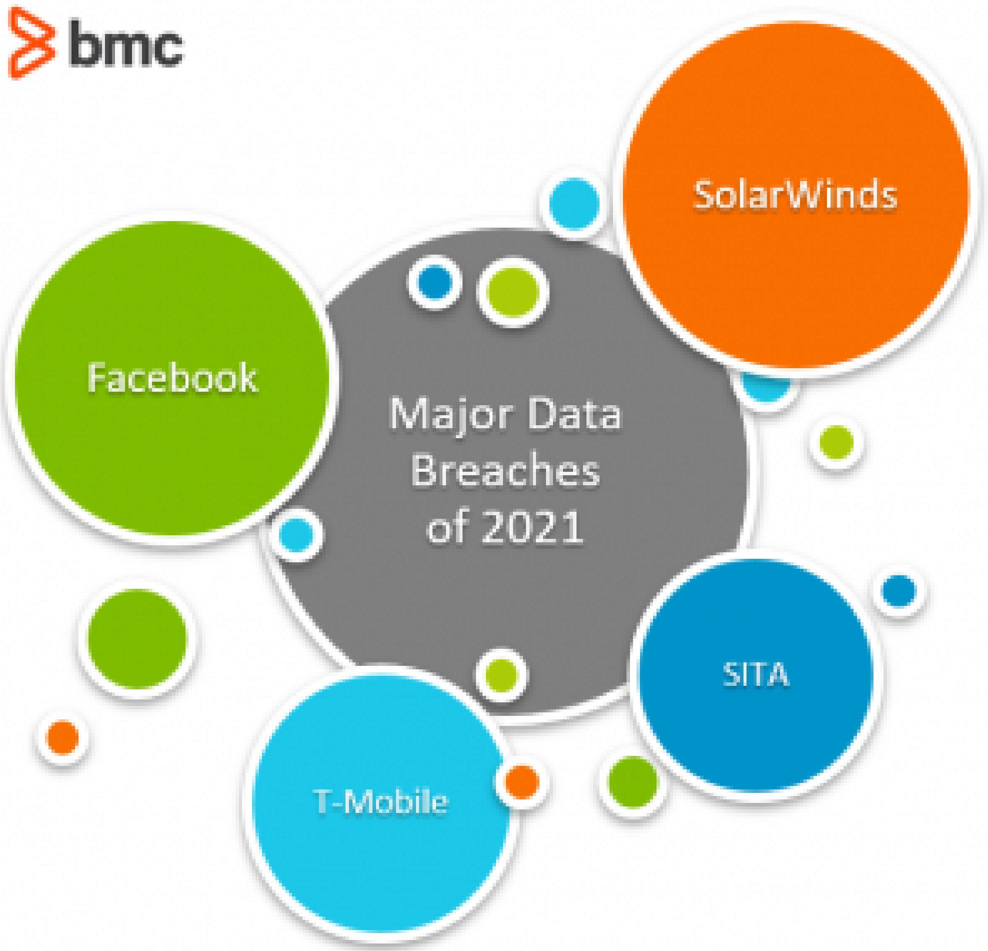
WORST DATA BREACHES OF 2021: 4 CRITICAL EXAMPLES

Consumers rely on businesses to deliver customized services in exchange for their personally identifiable information. Consumers participate in this exchange through trust and reliance upon the service provider to protect their sensitive information.

This information—in the wrong hands—has the potential to inflict tangible losses to both parties.

Business organizations therefore invest significant resources to protect consumer data as part of regulatory compliance objectives and a defense mechanism against growing security threats. The threats, however, are growing in sophistication, defeating some of the most technologically advanced enterprises to compromise valuable consumer data.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)



What is a data breach?

A data breach occurs when information is accessed and taken from a system without the consent of the operator. Bad actors seek to obtain sensitive data, and once acquired, they can often sell it to the highest bidder. Usually, the target is personal identification information (PII).

There are many ways for a data breach to happen, from old-fashioned hardware theft to cleverly engineered AI phishing scams. Information theft is so profitable, in fact, that it is worth the time for criminals to continue to innovate new ways to steal that data. This is why every year we see an uptick in data breaches, especially targeting well-known and otherwise trusted organizations.

(Understand information security in detail.)

4 Major Data Breaches from 2020-2021

This year was no different: a diverse range of organizations with a vast pool of end-users fell prey to cybersecurity incidents.

The following list contains some of the top data breaches of the past year or so, in terms of number of consumers affected, impact in the industry, criticality, and nature of consumer data compromised as well as the acknowledged security stature of the affected business organization.

SolarWinds

Impact: Thousands of large private companies and high-security governmental departments were left vulnerable to Russian hackers.

Revealed: December 2020

Story: SolarWinds is a major US company that provides IT software to 33,000 customers, including large corporations and government entities. Hackers added malicious code to one of their software systems, which then transferred to every customer during a regular system update. The malicious code allowed hackers to install even more malware and ultimately spy on companies and organizations, including the U.S. Department of Homeland Security and the Treasury Department.

SITA

Impact: Frequent flyer data from numerous airlines worldwide were exposed.

Revealed: March 2021

Story: Hackers accessed data through the company SITA's Horizon Passenger Service System. Not all affected airlines utilize SITA's system, but their frequent flyer information was accessible due to their connection through the Star and Oneworld Alliance.

Facebook

Impact: The personal information of 533 million Facebook users was found posted online by a hacker, including names, birthdays, phone numbers, locations, and email addresses.

Revealed: April 2021

Story: According to Facebook, the stolen data had been originally scraped a few years ago due to a vulnerability that the company patched in 2019. Cybercriminals could use the exposed data to impersonate people to both:

- Gain access to even more sensitive information
- Convince people to hand over login information, orchestrating very convincing phishing scams

The data was posted on a hacking forum for free, allowing almost anyone to access it. The breach affected people from 106 different countries.

T-Mobile

Impact: Compromised the personally identifiable information of more than 50 million previous and current customers.

Revealed: August 2021

Story: A 21-year-old hacker by the name of John Binns accessed T-Mobile's servers and pulled the personal data from millions of previous and current customers. A breach of this magnitude at a phone company is particularly troubling—so, so many two-factor authentication checks for other services go through one's mobile phone.

What to do in the event of a data breach?

The way things are going, the question is not if a breach will happen, but when. Data theft is incredibly lucrative and that makes it a worthwhile endeavor for bad actors to continue to innovate how it is done.

Of course, there are many things an organization should do if there is a breach on their end, including:

- Informing your customers of the breach and its included risks
- Providing some harm mitigation, such as free credit monitoring

As an individual, once you catch wind of a breach that may have affected you, there are a few things you can do to protect yourself from further risk.

Monitor your correspondence

When a company's data is compromised, they might reach out to inform users of the situation. Be sure to verify via the organization's secure website or a direct telephone call that the information in the email is correct and not a phishing scam.

It is also important to monitor any unfamiliar communications or unexpected bills that might come your way. Be extra wary when responding to requests for information or password resets.

Confirm what data was stolen

All data breaches expose users to potential hazards, but some data is more sensitive than others. For example:

- Email addresses and telephone numbers can open the victim to phishing scams and access to login information.
- A stolen social security number can cause a lot more damage—loans and mortgages could be taken out in your name, without your knowledge.

Verify what information was stolen so you can take the correct measures to protect yourself.

Keep an eye on your financial accounts

Pay attention to your bank and credit card statements to make sure there are no unfamiliar charges posted to them. Many providers allow you to set up alerts to new activity, which will help you stay on top of things as they occur.

Activate fraud alerts

A fraud alert can let lenders know that you are a potential victim of fraudulent activity. This will put a note on your credit reports and ensure that lenders contact you before any line of credit is opened in your name. If you initiate an alert with any of the big three credit reporting agencies (TransUnion, Experian, or Equifax) it will translate to the other two and stay active for 90 days.

Regularly check your credit report

Whether you do so through one of the big three, or if you utilize Annualcreditreport.com for free, it is a good idea to monitor your credit report on a regular basis. This is especially true if you know you may have been the victim of a breach so you can keep an eye out for any unusual activity.

From an Internet consumer perspective, it is important to understand the risks associated with performing transactions, sharing information, or even browsing social media online. It is recommended not to rely on the Internet companies as your last line of defense, but to personally walk the extra mile in protecting your online presence and watching out for any suspicious activity associated with your online or financial accounts.

Related reading

- BMC Security & Compliance Blog
- DataOps Explained: Understand how DataOps leverages analytics to drive actionable business insights
- What Is Threat Remediation? Threat Remediation Explained
- DevSecOps: Combining Development, Security & Operations
- Data Ethics for Companies
- Top IT Security, InfoSec & CyberSecurity Conferences To Attend