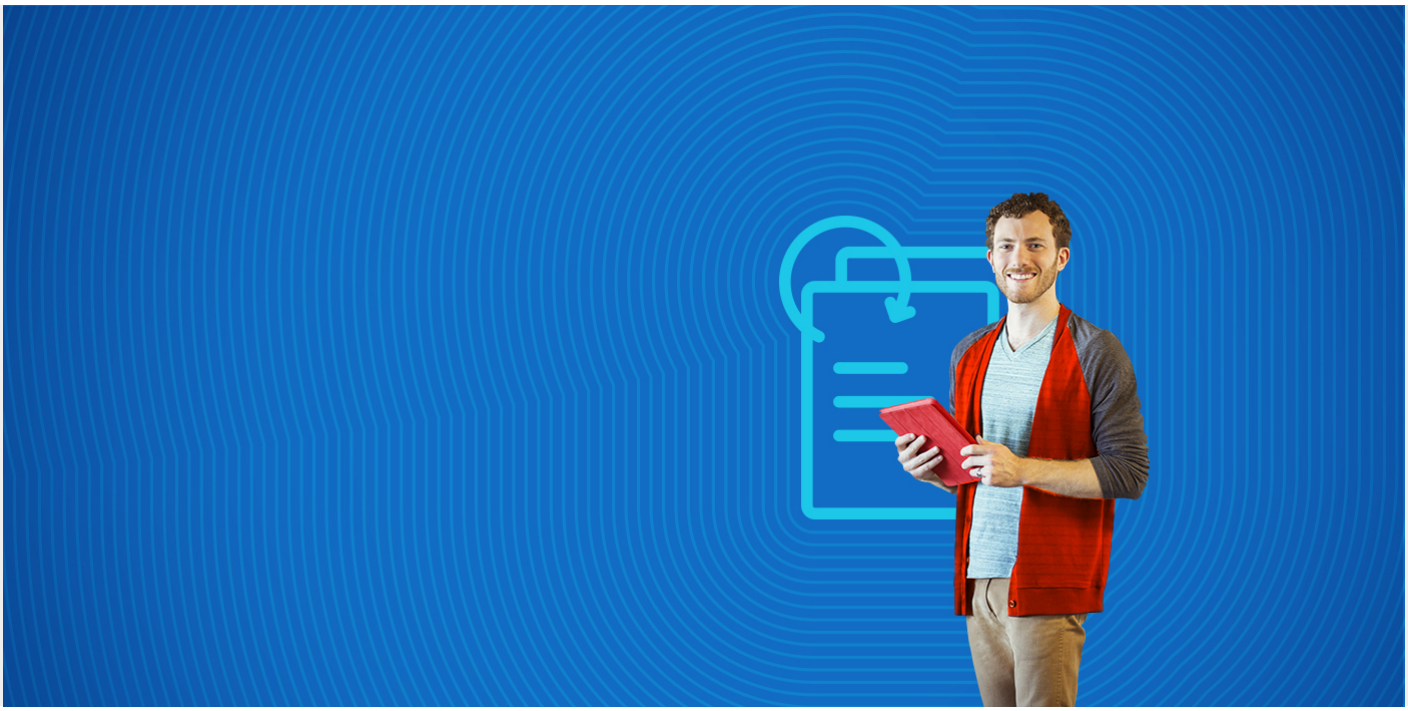
DATA BREACHES: 5 CRITICAL EXAMPLES



Consumers rely on businesses to deliver customized services in by leveraging their personally identifiable information. Consumers participate in this exchange through trust and reliance upon the service provider to protect their sensitive information, which 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 defense mechanism against the growing security threats. The threats however, are growing in sophistication, defeating some of the most technologically advanced enterprises to compromise valuable consumer data.

The year 2018 was no different as a diverse range of organizations with a vast pool of end-users falling prey to cybersecurity incidents. Many of these high-profile data breaches took place months or years before 2018, but were only discovered or revealed to the general public last year. The following list contains top 5 biggest data breaches of 2018, 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.

5 Major Data Breaches from 2018

Facebook

Impact: Personally identifiable information including social media activities of 87 million users compromised.

Revealed: September 2018

Story: The incident involved the data analytics firm Cambridge Analytica capturing Facebook user

information through a login API. When users agreed to login via Facebook to a Cambridge Analytica survey app, the analytics firm cleverly confirmed end-user consent to access and use end-user information. While Facebook likes to call this deceptive marketing and misuse of data, valuable personal information of Facebook users was compromised outside of their actual knowledge and approval. Facebook itself remained unaware of Cambridge Analytica's misuse of customer data and responded with strengthened privacy policies, banning of apps accessing end-user information without true consent as well as explanation to the general public and government officials. The incident reflects upon the vulnerability of large companies and Internet services in controlling and preventing misuse of customer data.

Marriot Starwood Hotel

Impact: 500 million guests lost personal information including passport numbers, bank card data, reservation details and contact information.

Revealed: November 2018

Story: Large hotel chains such as Marriott Starwood thrive on their ability to serve their guests with luxury hospitality services. Customers pay significant amounts to ensure their stay is comfortable and secure, and share all necessary information such as bank card and identification details that allow the brand to charge its customers and secure its business. However, Marriott recently discovered anomalous behavior around its guest information databases that traced back to 2014. According to reports, customer information was breached, encrypted and attempted to remove from Marriott servers altogether. The issue was discovered only in September 2018, and disclosed to general public by the end of November 2018.

Newegg

Impact: Credit card information of 50 million users.

Revealed: September 2018.

Story: The Newegg incident is an example of financially motivated organized cybercrime. A cybercrime underground ring called Magecard was able to compromise the Newegg website with malicious code. The group was also responsible for other high-profile attacks on popular online websites including those of British Airways, Feedify and Ticketmaster. The credit card information of customers purchasing online was then compromised and the financial data was available to cybercriminals. The company suggested that only a limited number of users may have been affected, but the incident exposes vulnerabilities in online shopping services. Similar to the attack on the British Airways website, hackers were able to route users to a malicious domain impersonating the legitimate brands. Information around the true financial losses to end-users was not reported, but the victims were advised to follow proactive security measures. These may include the hassle of replacing credit cards and keeping an eye out for suspicious transactions on their accounts.

Aadhaar

Impact: ID database including biometrics and sensitive personally identifiable information of 1.1 billion citizens in India compromised and up for sale less at less than $10 according to reports.

Revealed: January 2018

Story: Following years of criticism around the vulnerabilities of the worlds largest biometric identification system, hackers were able to compromise Aadhaar data and sell it for a few dollars on Whatsapp. The data was sold the software patch that can be used anywhere in the world to generate legitimate Aadhaar identification numbers. The incident follows a series of security compromises taking place earlier, including the data being leaked on government websites. The sheer scale of ID database management systems and the associated complex infrastructure systems make it particularly challenging to protect against cybercriminals using sophisticated attack mechanism to exploit the security loopholes.

Exactis

Impact: Sensitive information of 340 million users, including businesses and consumers was compromised. Two terabytes of data was somehow transferred to public servers, although the company did not disclose how much of that information was accessed or compromised to third-parties. Reports suggest that the breach compromised practically "every US citizen". The company now faces lawsuit against the attack.

Revealed: June 2018.

Story: The data broker and aggregation firm Exactis collects individual records ranging from personally identifiable information to marketing and behavioral information. The comprehensive information was exposed within public domain as discovered by a security researcher Vinny Troia. The compromised data did not contain credit card information or social security numbers, therefore reducing the severity of impact to the victims. However, the security reports suggest that the data records spanned 400 variables including characteristics such as favorite pets and recreational activities. The incident highlights how relatively small organizations are able to maintain large database repositories on the cloud infrastructure, and may be prone to large scale data breaches due to inadequate security systems and policies in place.

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.