Recent *Major* Data Breaches

Data breaches continue to be a significant concern for individuals and organizations alike. Here's a summary of some notable data breaches and cybersecurity incidents reported in late 2024 and early to mid-2025:

Major Data Breaches (Late 2024 - Mid-2025):

- **"Largest Breach Ever" (Potentially Surveillance Related):** In early June 2025, a massive dataset containing roughly 4 billion records was discovered unsecured online by cybersecurity researchers. This data, primarily consisting of Chinese citizens, includes personal information like full names, dates of birth, phone numbers, financial data (card numbers, debt, savings, spending habits), and more. Researchers believe it could be part of a surveillance effort. (Reported June 2025)
- **AT&T Data Leak (Re-packaged):** Data from a 2021 AT&T breach, affecting 70 million customers, was re-released in June 2025. This new release directly links Social Security numbers and birth dates to individual users, making it more impactful. (Reported June 2025)
- **LexisNexis Risk Solutions:** In December 2024, data broker LexisNexis Risk Solutions experienced a breach that stole personal information of over 364,000 individuals. (Reported May 2025)
- **Cartier and The North Face:** Luxury brand Cartier and outdoor apparel retailer The North Face both reported data breaches in early June 2025 and late May 2025, respectively, impacting customer personal information.
- **Coinbase:** The cryptocurrency exchange Coinbase reported two data breaches in May and June 2025. One incident was tied to bribed customer support agents, affecting 69,461 customers. (Reported May/June 2025)

- **Lee Enterprises:** Publishing giant Lee Enterprises notified nearly 40,000 people about a February 2025 ransomware attack that stole their personal information.(Reported June 2025)
- **PowerSchool:** A major K-12 education tech provider, PowerSchool, suffered a data breach in December 2024 affecting 62.4 million students and 9.5 million educators. They paid a ransom, but hackers resumed extortion attempts as of May 2025. (Reported May 2025)
- **Yahoo! (Historical but impactful):** While older (2013-2016), the Yahoo! data breach, which compromised 3 billion accounts, is still frequently cited as one of the largest in history due to its sheer scale.
- **Indian Council of Medical Research:** In 2023, around 815 million Indian citizens may have had their COVID test and other health data exposed in a breach.
- **Apria Healthcare:** US healthcare company Apria Healthcare notified almost 1.9 million customers in late 2024 that their personal data may have been compromised.
- **Union Health System, Inc.:** This Indiana-based healthcare company disclosed a data breach affecting an estimated 262,831 individuals. (Reported April 2025)
- **Yale New Haven Health System:** This healthcare system experienced a data security incident that may have affected approximately 5.6 million patients.(Reported April 2025)
- **New York University (NYU):** NYU experienced a major data breach in March 2025 that exposed the personal information of over 3 million applicants. (Reported April 2025)
- **SpyX Stalkerware App:** This app suffered a massive data breach exposing personal information of nearly 2 million individuals,

including iCloud usernames and passwords stored in plain text. (Reported April 2025)

- **Jaguar Land Rover (JLR):** JLR reportedly suffered a data breach in March 2025, with a hacker claiming to have exposed 700 internal documents, including development logs, source code, and employee credentials. (Reported April 2025)
- **Gravy Analytics:** In January 2025, Gravy Analytics suffered a significant data breach that exposed the personal information of millions of people worldwide. (Reported Feb 2025)
- **Globe Life Inc.:** This insurance company disclosed a breach affecting approximately 850,000 individuals, including names, Social Security numbers, and health information. (Reported Jan 2025, initially detected mid-2024)
- **Community Health Center, Inc. (CHC):** A non-profit healthcare provider in Connecticut, CHC, suffered a significant data breach in January 2025, impacting over one million individuals. (Reported Feb 2025)
- **HCF Management:** This operator of long-term care facilities suffered a data breach in 2024 that came to light in January 2025, affecting thousands of patients. (Reported Feb 2025)
- **Wolf Haldenstein (Law Firm):** This law firm experienced a substantial data breach in January 2025, impacting approximately 3.4 million individuals. (Reported Feb 2025)
- **Change Healthcare:** In 2024, Change Healthcare, a key player in healthcare technology, suffered a significant data breach that exposed sensitive patient and operational data for potentially 190 million people. This is considered one of the biggest US medical data breaches in history.

- **Snowflake Data Platform:** In May 2024, a significant data breach involving the cloud data platform Snowflake was uncovered, affecting various organizations.
- **UK Ministry of Defence (MoD) and MediSecure:** Both the UK MoD and Australian e-prescription service MediSecure experienced breaches between September and November 2024, with unauthorized access to employee emails through phishing scams.

Key Trends and Observations:

- **Healthcare Sector continues to be a major target:** Numerous healthcare organizations, from large systems to smaller clinics, have been impacted by breaches, exposing sensitive patient data.
- **Third-Party and Supply Chain Risks:** Many breaches originated from vulnerabilities in third-party vendors or supply chain partners, highlighting the interconnectedness of cybersecurity risks.
- **Ransomware and Phishing Remain Prevalent:** Ransomware attacks continue to cause significant disruption and data theft, while phishing remains a primary tactic for gaining initial access.
- **Misconfigured Databases and Weak Credentials:** Unsecured databases and the use of weak or compromised credentials are still common causes of data exposure.
- **Increased Sophistication of Attacks:** Threat actors are employing increasingly sophisticated methods, including the use of AI to automate phishing campaigns and exploiting zero-day vulnerabilities.

It's crucial for individuals and organizations to remain vigilant, implement strong security measures, and stay informed about the latest threats.

Authors Note. This list was compiled with the assistance of Google's Gemini, an AI agent.