Agpoon, Claire 2-20-24 IAS1

BSIT 3-A Mr. Gabriel Thomas Torneros

**The Yahoo Hacks (2013 & 2014):**

In 2013 and 2014, Yahoo suffered two major data breaches that had severe consequences for millions of users. The first breach compromised over 1 billion Yahoo accounts, including names, dates of birth, security questions, contact details, and passwords. The second breach affected 500 million accounts.

The data breaches highlighted the serious implications of password and security question reuse. Additionally, outdated encryption methods used by Yahoo failed to protect user data adequately, making it vulnerable to attackers.

## ****Equifax Data Breach (2017):****

One of the most extensive data breaches in history occurred in 2017, affecting Equifax, a major credit reporting agency. The breach exposed sensitive personal information, such as social security numbers, dates of birth, addresses, driver’s license numbers, and more, of over 143 million customers.

Attackers had access to Equifax’s systems for 76 days before being discovered. The breach cost the company $1.4 billion in recovery efforts. The attack was facilitated by an XXE vulnerability in the company’s customer complaints web portal, left unpatched due to internal failures. Lack of proper segmentation and authentication mechanisms also enabled attackers to access data and credentials without detection.

## ****LinkedIn Data Breach (2021):****

In June 2021, LinkedIn, the renowned professional networking platform, faced a significant data-related issue affecting a massive 700 million users, which constituted over 90 percent of its user base. A hacker, identifying themselves as “God User,” utilized data scraping techniques to exploit not only LinkedIn’s API but also that of other websites. Subsequently, the hacker disclosed a first information data set of approximately 500 million customers, followed by the announcement of selling the complete database of 700 million users.

LinkedIn contended that no sensitive or private personal data had been exposed, and they characterized the incident as a violation of their terms of service rather than a data breach.

## ****Twitter Breach (2022):****

In 2022, Twitter encountered a major data breach involving excessive data exposure. The breach began with attackers selling the information of 5.4 million users on a hacking forum. Subsequently, in January 2023, the attackers scraped the public and private data of 400 million additional users and sold it on the dark web.

The flaw in Twitter’s systems allowed attackers to verify if email IDs and phone numbers were linked to specific Twitter accounts. This breach left numerous users, including high-profile individuals such as celebrities, politicians, and activists, vulnerable to social engineering, targeted phishing attacks, identity theft, and other cyber threats.

## Sony

In April 2011, Sony had a cybersecurity breach. Hackers compromised 77 million PlayStation gaming console user accounts, gaining access to their names, addresses and other sensitive data.

This was a big blow for the gaming community, but it wouldn’t be the last blow to Sony. In 2014, hackers erased data from its systems and stole — and shared with the world — prerelease movies and celebrities’ private information.

### **2013 - Cyber Attacks on the Singaporean Government**

[**Anonymous**](https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/), perhaps one the more iconic hacking groups in the world from the early 2000s, was linked to several security events in the news around this time. The group, an international hacktivist group which started in 2003 and was responsible for several high-profile cyber attacks against governments and large organizations, initiated a series of cyber attacks on the Singaporean government in 2013. One reason for the attacks was purportedly Singapore’s web censorship regulations, particularly on news outlets. [**James “The Messiah” Raj**](https://www.todayonline.com/singapore/suspected-messiah-hacker-charged-court), an Anonymous representative, was eventually later charged that year in a Singapore court.

### **2013 - Adobe**

Despite being one of the most recognizable names in software, Adobe announced in October 2013 that its system was massively hacked.

[**Over 38 million users and over 152 million breached records were involved**](https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online)in the incident. To perform the hack, the perpetrators took advantage of Adobe’s poor encryption practices, but that’s not all: Hackers were also able to obtain over [**40 GB of source code**](https://techcrunch.com/2013/10/03/adobe-gets-hacked-product-source-code-and-data-for-2-9m-customers-likely-accessed/) for three Adobe programs: Acrobat, ColdFusion, and ColdFusion Builder.

Adobe was eventually [**fined $1 million**](https://news.softpedia.com/news/adobe-fined-1-million-for-2013-hack-that-affected-millions-of-users-510256.shtml?utm_source=dlvr.it&utm_medium=twitter) for the said incident.