CISC 181 Lab 11 Data Breaches

In this lab I want you to do web searches to investigate issues with the storage of large amounts of data online. Specifically, find **four** examples **in the last four years** (so no earlier than November 2017) of major data breaches in user/customer/taxpayer data security at a large company or government agency **involving at least 1 million records**. Do not include the Microsoft Exchange Server breach, as it is already described in the Notes 11 slides. For each data breach, give:

* (4 × 1 marks) The name and home page address (URL) of the company or government agency. If the company or agency no longer exists, as might happen, for example, if the company is no longer in business, make a note of that instead of giving a URL.
* (4 × 1 marks) The date on which the security breach was discovered OR made public.
* (4 × 2 marks) A brief description of the breach and what data was, or may have been, stolen. Include details like number of accounts affected, the type of data stolen and, if known, the way in which the thieves gained access to the data.
* (4 × 1 marks) Your web source(s) for the information (one or more URLs).

(That is 20 marks in total.) **Make sure all URLs in your submission are active links** for the benefit of the TAs, please.

**Type your solutions into the space below and on extra pages if needed**. Save and submit your completed Lab 11.docx file by the deadline.

**Example 1:**

* Alibaba (<https://www.alibaba.com/>)
* November 2019
* A developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers from the Alibaba Chinese website. They took roughly 1.1 billion pieces of user data in total
* <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

**Example 2:**

* Facebook (<https://www.facebook.com>)
* April 2019
* Two datasets containing roughly 533 million users phone numbers, account names and Facebook ID’s were posted to the internet
* <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

**Example 3:**

* Cam4 (<https://www.cam4.com>) 🡪 NSFW
* March 2020
* Adult video site had it’s Elasticsearch server breached, exposing roughly 10.9 billion records. The breached records contained full names, email addresses, sexual orientation, chat transcripts, email correspondence transcripts, password hashes, IP addresses, and payment logs.
* <https://www.upguard.com/blog/biggest-data-breaches>

**Example 4:**

* LinkedIn (<https://www.linkedin.com>)
* June 2021
* Data associated with roughly 700 million users was posted for sale on the Dark Web, with data including email addresses, full names, phone numbers, geolocation records, LinkedIn username and profile URL’s, personal and professional experience, gender, and other social media accounts and details
* <https://www.upguard.com/blog/biggest-data-breaches>