Mini Research Project:
Case Study of a Recent Real-World Data Breach / Hack

Objective:

The goal of this research project is to give the students an opportunity to independently investigate a recent real-world case of *data breach* or *hack* using the knowledge acquired in the course. In particular, the student is expected to find and research various online sources in order to gain in-depth understanding of the given breach/hack, including: when and how the breach/hack occurred, who the main stakeholders of the breach/hack were, what the most significant consequences and lessons of the breach/hack are, etc. The findings of the research will be submitted to the course instructor for evaluation in the form of a written report.

Timeline & Deliverable:

- ***September 11***: The student receives an email from the course instructor with the name of a specific real-world data breach or hack which he/she is supposed to independently investigate, as well as a few initial references pertaining to this incident.

- ***October 28***: The student submits a written report on his/her main findings about the given incident. The first page of the report should provide some general coverage of the incident, while the reminder of the report should give very specific answers about the following:

  1) **Was this incident a hack or a breach?** Justify your answer!
  2) Who are the main 'stakeholders' in this incident (who is the adversary & who is the victim)? *Note: In cases when there are multiple adversaries and/or victims, they all have to be clearly enlisted.*
  3) When did the incident happen? When was it discovered?
  4) Which vulnerability in the target system was exploited by the adversary during the incident?
  5) How, exactly, did the adversary exploit the vulnerability? What was the main attack vector? *Note: For an exhaustive list of attack vectors see: https://www.upguard.com/blog/attack-vector*
  6) What did this breach/hack target in terms of CIA?
  7) What has been the actual loss suffered by the victim due to the incident (monetary, functional, reputational, …)? *Note: In most cases the victim suffers a combination of different types of loss, and they all should be enlisted. Also, if there are multiple victims, the losses of each particular victim should be specified.*
  8) How did/can the victim ensure that the same type of breach/hack does not happen again?
  9) Was the adversary prosecuted, and if so what were the penalties (if known)?
  10) What can other similar potential victims learn from this incident?

  The list of all researched references should be included in the report. The minimum acceptable number of references is 10!

  The report will be evaluated for the following:

  1) **Clarity of communication** (Does the provided information render a clear understanding of the incident? Are the report's organization and grammar satisfactory?)
  2) **Completeness** (Is all relevant information included in the report?)
  3) **Correctness** (Is the information provided in the report actually correct?)