The purpose of the term project is to analyze a cybersecurity incident or issue to explore the reasons and circumstances that caused the incident/issue, examine the actors involved, and provide recommendations to prevent similar incidents or mitigate the issue in the future. Below are some resources to browse through for some topic inspirations: https://nakedsecurity.sophos.com/ https://cyware.com/category/breaches-and-incidents-news https://threatpost.com/ https://www.securitymagazine.com/topics/2236-cyber-security-news Structure: The final report must follow the structure of sections outlined below: 1. Introduction 2. Case Description 3. Case Analysis 4. Recommendations 5. Conclusion 6. References Introduction The introduction should provide a brief overview of the case and topic and inform the reader of the core issue of the case. It is recommended to add the introduction during the final stages of writing the report. 2. Case Description After settling on a case, research as much relevant information as possible to describe as many case details you can find. The purpose of this section is to outline the following: What exactly happened? - Chronologically outline the event Who were the actors involved? What was the method, or strategy of the attack? This step is fundamental because the following analysis and recommendation will depend on the information you present here. You should use at least three different credible sources, including: Academic publications, established news papers and magazines, professional blogs, white papers, etc. (Wikipedia is not a credible source, but a good point to start to check the references used there). The case description must include: Background information on the organization involved Timeline of events. 3. Case Analysis The analysis is the core part of your term project. In this section you will identify and analyze the attackers’ strategies and exposed vulnerabilities to explore the circumstances that lead to the security incident. Based on your case description you should: Identify the vulnerabilities exposed in the case: What was the problem? Analyze the reasons for the vulnerabilities, such as human error, neglect by management, technological failure, zero-day etc. Which pillar or the CIA Model was compromised and how? The case analysis must include: a. Analysis of the vulnerabilities exploited b. Analysis of the threat agents and attack vectors c. Analysis of the management response 4. Recommendations The recommendations section is a response to your analysis and outlines security measures which help to reduce the problems that caused the breach. Therefore, it is essential that you focus on the security measures for the security issues you discussed in the analysis. For example, if the problem of your case was an exploited Wi-Fi connection, provide recommendations on strengthening Wi-Fi connections. I suggest to refer to the NIST framework or further NIST guidelines for specific security recommendations. The recommendations must include: Improving security measures Improving management Conclusion In the conclusion you can wrap-up your report by summarizing the most important points of your case. The conclusion is also the place where you can include your opinion on the case. 6. References Use APA-Style references and citations throughout your paper. All your references used must be from credible sources. Formal Requirements: The report must be: 12pt font Times New Roman Double-spaced 1 inch margins At least 8 pages (not counting title page and reference pages) No more than 1 direct quote. APA-Style citations and references At least 6 credible resources