<table>
<tr><th colspan="3">King Saud University
College of Computer and Information Sciences
Computer Science Department</th></tr>
<tr><td>CSC 429: Computer Security</td><td>Course Project</td><td>1st Semester, 1446– Fall, 2024</td></tr>
</table>

Course Project: Comprehensive Analysis of a Major Cybersecurity Incident

Project Objective:

This course project aims to deepen your understanding of high-profile cybersecurity incidents, analyze their root causes and impacts, and explore preventive measures. Through this project, you will apply theoretical knowledge to real-world scenarios, working collaboratively to identify solutions that strengthen organizational resilience against cyber threats.

Project Scope and Deliverables:

1. **Team Formation and Incident Selection:**
    - Form teams of 3 students.
    - Each team will select one cybersecurity incident from the list provided below.
    - Ensure that each team chooses a different incident to provide a variety of case studies across the class.
2. **Project Components:** The project will be split into two main deliverables:

    A. Incident Analysis Report (Individual Component):
    - Each team will write a 1,500 to 2,000-word report analyzing their chosen incident, covering:
        - **Introduction:** Overview of the incident and the entities affected.
        - **Timeline of Events:** A detailed timeline showing how the incident unfolded.
        - **Attack Methodology:** Describe the techniques and tactics used by attackers.
        - **Root Causes and Vulnerabilities:** Identify and analyze the specific security weaknesses exploited.
        - **Impact Analysis:** Discuss financial, reputational, operational, and legal impacts.
        - **Lessons Learned:** Key insights that could help organizations prevent or mitigate similar attacks.

    B. Group Presentation (Collaborative Component):
    - Each team will present their chosen incident which should include:
        - **Summary of the Incident:** Highlight the key elements of the incident.
        - **Incident Analysis:** Summarize attack methods, root causes, and impacts.
        - **Comparative Insights:** If relevant, compare the incident with similar types of attacks and highlight patterns.
        - **Mitigation Strategies:** Recommend security best practices and solutions based on lessons learned from the incident.
        - Use visual aids (e.g., slides, infographics, timelines) for clarity.
3. **Deliverables Summary:**

   - **Report:** Analysis of the incident (due by **23 Nov 2024**).
   - **Group Presentation:** Summary and recommendations (due by **27 Nov 2024**).
4. **Incident Options (Choose One Per Team):**
   - Target Data Breach (2013)
   - Sony Pictures Hack (2014)
   - Equifax Data Breach (2017)
   - WannaCry Ransomware Attack (2017)
   - Yahoo Data Breach (2013-2014)
   - Marriott Data Breach (2018)
   - NotPetya Attack (2017)
   - SolarWinds Supply Chain Attack (2020)
   - Colonial Pipeline Ransomware Attack (2021)

Grading Criteria:

- **Report (50%):** Depth of research, clarity of analysis, and critical thinking.
- **Group Presentation (50%):** Cohesion, quality of content, presentation style, and effectiveness of visual aids.

Additional Notes:

- **Research Sources:** Utilize credible sources such as academic journals, news articles, official reports, and industry analyses.
- **Format:** All written components should be submitted as PDFs, and presentations should use PowerPoint or similar software.
- **Citation:** Ensure accurate and consistent citation of all sources.
- **You must use at least 5 references.**