ECCS 3411 - Computer Security **Project 1**

Title: Understanding Real-World Cyber-Attacks and Analyzing the Societal and Ethical Impact of Cybersecurity Solutions: A Case Study Approach

Objectives:

- Enhance students' understanding of cybersecurity threats and incidents by analyzing a real-world cyber-attack case study.
- Explore how specific security solutions have been implemented to prevent cyber-attacks and discuss their effectiveness in mitigating risks.
- Evaluate the societal impact of cybersecurity solutions, considering global, economic, environmental, and societal contexts.
- Analyze ethical issues related to the cyber-attack and the implemented security solutions, presenting judgments adhering to professional codes of conduct.

Assignment Overview:
1. Select a Case Study:

- Choose a well-documented real-world cyber-attack case study from a reliable source. Examples include the WannaCry ransomware attack, Stuxnet, or the SolarWinds supply chain attack.

2. Introduction:

- Provide a brief overview of the chosen cyber-attack, including the date, entities involved, and the initial impact.
- Identify the societal need for cybersecurity solutions, emphasizing the potential consequences of cyber-attacks on individuals, organizations, and critical infrastructure.

3. Attack Analysis:

- Explore the technical aspects of the attack, including attack vectors, vulnerabilities exploited, malware or tools involved, and the attack's progression and timeline.
- Discuss the specific security solutions that were in place (or should have been in place) to prevent or mitigate the attack.

4. Impact Assessment:

- Assess the overall impact of the cyber-attack, including global, financial (and broader economic), environmental, and societal consequences such as,
  - disruption to operations,
  - damage to the organization's reputation, and
  - legal and regulatory implications.
- Analyze the effectiveness of the implemented security solutions in mitigating the impact of the attack.

5. Ethical Implications:

- Analyze the ethical issues related to the cyber-attack, such as the motivations of the attackers, the potential harm caused to individuals and society, and the responsibilities of organizations to protect user data.
- Discuss the ethical considerations surrounding the implemented security solutions, such as privacy concerns, potential biases, and the impact on individual freedoms.
- Present judgments on the ethical dilemmas involved, adhering to professional codes of conduct such as the ACM Code of Ethics and Professional Conduct or the IEEE Code of Ethics.

6. Security Recommendations:

- Based on your analysis, propose security recommendations for preventing similar cyber-attacks in the future.
- Discuss the ethical implications of your recommendations, ensuring they align with professional codes of conduct.

7. Conclusion:

- Summarize key findings and emphasize the importance of cybersecurity measures in today's digital landscape.
- Discuss the role of engineering solutions in meeting societal needs and the importance of considering broader contexts in cybersecurity decision-making.
- Reiterate the ethical responsibilities of cybersecurity professionals and the importance of ethical considerations in developing and implementing security solutions.

Submission Guidelines:

- Include proper citations for sources used.
- Use visuals (charts, graphs) to enhance the presentation of information.
- Due March 5th, Wednesday (hard copy submission).

Evaluation Criteria:

- Thoroughness of the analysis.
- Clarity and coherence of writing.
- Proper citation of sources.
- Critical thinking and insights into the ethical implications.
- Practicality and relevance of security recommendations.
- Consideration of global, economic, environmental, and societal contexts.
- Depth and quality of ethical analysis and judgments.