COSC2539 Assignment 1

Overview:

This assignment aims to evaluate students' understanding of cybersecurity principles through various tasks, including analysis, technical skills, and synthesis of academic literature.

Understanding the Assignment:

- **Objective**: To apply theoretical knowledge in practical cybersecurity scenarios.
- **Key Areas**: Cyber threats, encryption, cipher analysis, public-key cryptography, and academic synthesis.

Specific Instructions:

Exercise 1: Cyber Threats and the CIA Triad [20 Marks]

- **Knowledge Required**: Understanding of cyber threats and the CIA triad.
- **Steps**:
    1. Identify two potential cyber threats for Papaya Inc.
    2. Analyze their impact on the CIA triad.
    3. Recommend security mechanisms to mitigate these threats.
    4. Write a 300-500 word analysis.

Exercise 2: Symmetric Encryption in Practice [20 Marks]

- **Knowledge Required**: Symmetric encryption standards and command-line encryption tools.
- **Steps**:
    1. Discuss a standard type of symmetric encryption for secure document communication.
    2. Provide step-by-step command-line instructions to encrypt a file.
    3. Write a 300-500 word explanation.

Exercise 3: Deciphering a Simple Substitution Cipher [15 Marks]

- **Knowledge Required**: Frequency analysis technique for cipher decryption.
- **Steps**:
    1. Create a frequency analysis table.
    2. Decrypt the provided ciphertext.
    3. Document the decryption process, hypotheses, and trials.
    4. Show all steps and justifications.

Exercise 4: Public-Key Cryptography Demonstration [25 Marks]

- **Knowledge Required**: Public-key cryptography and OpenSSL functionality.
- **Steps**:
    1. Record a technical demonstration using OpenSSL or a similar tool.
    2. Cover key concepts of public-key cryptography.
    3. Discuss each step of the demonstration.
    4. Upload the video demonstration to Canvas.

Exercise 5: Academic Article Synthesis [20 Marks]

- **Knowledge Required**: Ability to synthesize information from academic literature.
- **Steps**:
    1. Select two academic articles reviewed over the past four weeks.
    2. Identify and discuss the connection between the two articles.
    3. Ensure proper IEEE citations.
    4. Write a 100-300 word synthesis.

Guide for excercise 1

Sample:

Papaya Inc., a leading global producer of papaya fruit with a flourishing online sales platform, must prioritize cybersecurity to protect its business operations and customer data. In the realm of cybersecurity, two predominant threats that pose significant risks to the company are phishing attacks and ransomware.

Phishing attacks, a prevalent form of cybercrime, involve malicious actors posing as legitimate entities to deceive employees into divulging sensitive information. Such attacks directly undermine the **confidentiality** aspect of the CIA triad. Confidentiality is crucial for Papaya Inc., as it involves protecting customer information and proprietary business data from unauthorized access. A successful phishing attack can lead to significant data breaches, eroding customer trust and potentially resulting in substantial financial losses and legal ramifications.

Another formidable threat is ransomware, a type of malware that encrypts a victim's files, demanding a ransom to restore access. This directly impacts the **availability** of data, a core component of the CIA triad, by denying access to critical business and customer information. In the case of Papaya Inc., where online sales are vital, ransomware can disrupt sales operations, lead to revenue loss, and damage the company's reputation. Additionally, ransomware can compromise the **integrity** of the company’s data. The alteration or potential loss of data during such attacks can result in mistrust in the accuracy and reliability of the company's information systems.

To mitigate these threats, Papaya Inc. must implement robust security mechanisms. For countering phishing, the company should invest in advanced email filtering technologies to

detect and prevent phishing emails from reaching employees. Regular cybersecurity training for employees is essential to raise awareness about recognizing and appropriately responding to phishing attempts. Implementing strong authentication protocols, such as two-factor authentication, can also significantly reduce the risk of unauthorized data access.

Regarding ransomware, Papaya Inc. should deploy state-of-the-art antivirus and anti-malware software to detect and neutralize threats. A comprehensive data backup strategy is imperative. Regular backups, preferably off-site or in a cloud environment, can ensure data recovery in the event of a ransomware attack, minimizing downtime and loss. Additionally, keeping all systems and software up to date with the latest security patches can prevent attackers from exploiting known vulnerabilities.

In conclusion, by proactively addressing these cybersecurity threats through strategic measures, Papaya Inc. can safeguard its digital assets, maintain customer trust, and ensure the continuity of its online business operations. This proactive approach to cybersecurity will not only protect the company from immediate threats but also fortify its resilience against evolving cyber threats in the digital landscape.

To approach this task effectively, I followed a structured method:

1. **Understanding the Context**: I first understood Papaya Inc.'s context as a global papaya producer with a significant online presence. This helped in identifying relevant cyber threats.
2. **Identifying Relevant Threats**: Based on the context, I chose phishing and ransomware as the most pertinent threats, considering their commonality and potential impact on online businesses.
3. **Analyzing Impact on the CIA Triad**: I then analyzed how these threats affect the three components of the CIA Triad: Confidentiality, Integrity, and Availability. This step involved thinking through the consequences of these threats on Papaya Inc.'s operations and data.
4. **Recommending Mitigation Strategies**: After identifying the threats and their impacts, I suggested specific, actionable security measures that Papaya Inc. could implement to mitigate these risks.
5. **Writing Style**: The writing was kept concise, clear, and focused on the task objectives. I ensured that the response was within the specified word limit, providing enough detail to be informative but concise enough to maintain clarity and focus.
6. **Ensuring Relevance and Accuracy**: Throughout the response, I maintained relevance to the company’s context and ensured that the information was accurate and reflective of current cybersecurity best practices.

This approach ensured a comprehensive, clear, and informative response, tailored to the specific needs and context of Papaya Inc.

To ensure the confidentiality of the document your business manager intends to send from an unsecured location in New Zealand, the use of AES (Advanced Encryption Standard) is recommended. AES is a widely recognized symmetric encryption standard adopted by the U.S. government and is known for its reliability and security.

Guide for exercise 2 and 3

[ ] ↳ *2 cells hidden*