Lab Assignment 01: Threat Actors and Information Security Practices

Overview:
This lab assignment is designed to deepen your understanding of the key concepts introduced in Chapter 1: Introduction to Information Security. Through independent research and analysis, you will explore real-world applications of security principles, emerging threat actors, and current cybersecurity strategies and frameworks. Due 06/17 @ 11:59pm

Objectives:

- Apply the CIA triad to real-world security incidents.
- Identify and analyze different types of threat actors and their motivations.
- Research current industry standards, frameworks, and regulatory measures.
- Evaluate the impact of vulnerabilities and attack vectors.

Instructions:

Complete the following sections using credible academic, industry, or government sources. Cite all sources at the end of the document.

Lab Tasks:

1. Real-World Breach Analysis

   Choose a real-world data breach or cybersecurity incident from the last five years. Identify how each component of the CIA triad (Confidentiality, Integrity, Availability) was impacted. Describe the threat actor(s) involved and their likely motivations.

2. Threat Actor Deep Dive

   Choose one threat actor category (e.g., hacktivists, nation-state actors, insiders) and conduct a detailed investigation. Include examples of known incidents, typical techniques used, and countermeasures organizations implement to protect against them.

3. Frameworks and Compliance

   Select one security framework (e.g., NIST Cybersecurity Framework, ISO/IEC 27001, or PCI DSS) and explain its core components. Discuss how this framework supports an organization's ability to defend against modern threat actors.

4. Vulnerability Research

   Research a recent zero-day vulnerability. Explain how it was discovered, what systems were affected, and how the vulnerability was mitigated. Include a discussion of potential attack vectors and the importance of early detection.