ITBU 313: Introduction to Cyber Security, Homework 02

Chapter 14, *Computer Security, Principles and Practices*

Readings

Read chapter 14 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. Managing the security of computer and information systems involves answering three questions. What are they?
2. The book notes that managing IT infrastructure is a "cyclical process." What does this mean?
3. What is the intent of the *organizational security policy*?
4. List the four approaches to identifying and mitigating risks to an organization's IT infrastructure.
5. You have recommended for your organization to use the *combined approach* to develop a security policy, and your manager has asked you to justify your recommendation. What would you say?
6. What do we mean when we say that the initial step in establishing a security policy is to *establish the context*?
7. What is an *asset* with respect to the security policy? Give an example of assets in four different asset classes.
8. What is the connection between a *threat* and an *vulnerability*? Be specific.
9. The book gives the following formula as one means of calculating risk:

$$Risk = ThreatProbability \times ThreatCost \tag{1}$$

   Explain this formula and use it to calculate a (hypothetical) risk.
10. What is the difference between quantitative risk assessment and qualitative risk assessment?
11. List the five alternatives for risk management.