• Be specific and the policy should be applicable to each and every employee: The policy should be specific and should relate to every employee in the organization, irrespective of the employee’s position. An organization should take action if any employee violates the rules.

• Terms that are specific should be bold, underlined, or italicized: Specific and technical terms that let the employee understand the policy clearly should be brought to notice by making them bold, underlined, or italicized.

• Apply provisions that allow for updates to the policy: An organization should make provisions for updating policies.

• Policies should adhere to local laws: Policies should relate to local laws, as an organization can involve law enforcement when an employee violates certain rules that are also laws.

Chapter Summary

■ The term corporate espionage is used to describe espionage conducted for commercial purposes on companies and governments, and to determine the activities of competitors.

■ Personal relations, disgruntled employees, and easy money are the main motives behind corporate spying.

■ The major techniques used for corporate spying are hacking, social engineering, dumpster diving, and phone eavesdropping.

■ Steps to prevent corporate espionage are understanding and prioritizing critical assets, defining acceptable level of loss, controlling access, baiting, detecting moles, profiling, monitoring, and analyzing signatures.

■ Netspionage is defined as network-enabled espionage in which knowledge and sensitive proprietary information are stored, transmitted, and obtained via networks and computer systems.

Review Questions

1. What are the reasons behind corporate espionage?

2. What type of information do corporate spies look for?

3. What are the different techniques of spying?

4. What are the techniques for securing the confidential data of a company from spies?

5. What are the steps to prevent corporate espionage?