Chapter 10 - Management & Incidents

**1. In what ways is denial of service (lack of availability for authorized users) a**

**vulnerability to users of single-user personal computers?**

**2. Identify the three most probable threats to a computing system in an office**

**with fewer than ten employees. That is, identify the three vulnerabilities most**

**likely to be exploited. Estimate the number of times each vulnerability is**

**exploited per year. Justify your estimate.**

**3. Perform the analysis of Exercise 2 for a computing system located in a large**

**research laboratory.**

**4. Perform the analysis of Exercise 2 for a computing system located in the**

**library of a major university.**

**5. What is the value of your own personal computer? How did you derive that**

**number? Does it cover the cost to recover or recreate all the data you have on it?**

**6. List three factors that should be considered when developing a security plan.**

**7. Investigate your university’s or employer’s security plan to determine whether**

**its security requirements meet all the conditions listed in this chapter. List any**

**that do not. When was the plan written? When was it last reviewed and updated?**

**8. State a security requirement that is not realistic. State a security requirement**

**that is not verifiable. State two security requirements that are inconsistent.**

**9. Cite three controls that could have both positive and negative effects.**

**10. For an airline, what are its most important assets? What are the minimal**

**computing resources it would need to continue business for a limited period (up to**

**two days)? What other systems or processes could it use during the period of the**

**disaster?**

**11. Answer Exercise 10 for a bank instead of an airline.**

**12. Answer Exercise 10 for an oil drilling company instead of an airline.**

**13. Answer Exercise 10 for a political campaign instead of an airline.**

**14. When is an incident over? That is, what factors influence whether to continue the**

**work of the incident handling team or to disband it?**

**15. List five kinds of harm that could occur to your own personal computer. Estimate**

**the likelihood of each, expressed in number of times per year (number of times could**

**be a fraction, for example, 1/2 means could be expected to happen once every two**

**years). Estimate the monetary loss that would occur from that harm. Compute the**

**expected annual loss from these kinds of harm.**

**16. Cite a risk in computing for which it is impossible or infeasible to develop a**

**classical probability of occurrence.**

**17. Investigate the computer security policy for your university or employer. Who**

**wrote the policy? Who enforces the policy? Who does it cover? What resources does**

**it cover?**

**18. If you discover an unusual situation at your university or employer, to whom**

**should you report it? Can you report something any time day or night?**

**19. List three different sources of water to a computing system, and state a control for**

**each.**

**20. You discover that your computing system has been infected by a piece of**

**malicious code. You have no idea when the infection occurred. You do have backups**

**performed every week since the system was put into operation but, of course, there**

**have been numerous changes to the system over time. How could you use the**

**backups to construct a “clean” version of your system?**