Chapter 2 Answers to Review Questions and Exercises

Review Questions

1. What is the difference between criminal law and civil law?Answer:Civil law embodies a wide variety of laws pertaining to relationships between and among individuals and organizations. Criminal law addresses violations harmful to society and is actively enforced and prosecuted by the state.
2. What is tort law and what does it permit an individual to do?Answer:Tort law is a subset of civil law that allows individuals to seek recourse against others in the event of personal, physical, or financial injury. It is not prosecuted by the state.
3. What are the three primary types of public law?Answer:The three primary examples of public law are criminal, administrative, and constitutional law.
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?Answer:The National Information Infrastructure Protection Act of 1996amended the Computer Fraud and Abuse Act of 1986, modifying several sections of the previous act and increasing the penalties for selected crimes. The act was then further modified by the PATRIOTAct of 2001 and USA PATRIOTImprovement and Reauthorization Act of 2005.
5. What is the USA PATRIOT Act? When was it initially established and when was it significantly modified?Answer:The USA PATRIOTAct was initially enacted in 2001 as a mechanism to provide the United States with a means to investigate and respond to the 9/11 attacks on the New York World Trade Center. It was modified by the USA PATRIOT Improvement and Reauthorization Act of 2005, which became law in 2006.Some aspects of the law have been updated as recently as 2015.
6. What is privacy in the context of information security?Answer:In the context of information security, privacy is an individual's right to guard personalinformation from unauthorized use. It is also defined as the "state of being free from unsanctioned intrusion," which means that information can be gathered and used only if the individual providing the information agrees to the manner in which it will be used.
7. What is another name for the Kennedy-Kassebaum Act (1996), and why is it important to organizations that are not in the health care industry?Answer:The Kennedy-Kassebaum Act is also known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is important to organizations that are not in the health care industry because it limits what information is collectable from individuals' health records. It also allows individuals to be informed of how their information is being used and who is accessing it.
8. If you work for a financial service organization (such as a bank or credit union), which law from 1999 affects your use of customer data? What other effects does it have?Answer:The Gramm-Leach-Bliley (GLB) Act of 1999 affects how financial service organizations use customer data. It provides that all financial institutions must disclose privacy policies, describe how they share nonpublic personal information, and describe how customers can place requests to not have their information shared. It also requires organizations to create and disseminate a privacy policy to the customers which is to be distributed annually with all revisions and updates.
9. Which 1997 law provides guidance on the use of encryption?Answer:The Security and Freedom through Encryption Act of 1997 provides rules and guidelines on the

proper use of encryption. The act provides proper uses and situations in which encryption can legally be used and situations in which it cannot legally be used.

10. What is intellectual property? Is it offered the same protection in every country? What laws currently protect intellectual property in the United States and Europe?Answer:Intellectual property is any material or words created by individuals on their own free time or at any time, depending on the policy their employers issue. Any country in the world may have its own definition of "intellectual property." Therefore, intellectual property is difficult to protect worldwide. Currently, the U.S. copyright law ensures intellectual property in the United States, and Europe has the European Council Cyber-Crime Convention.
11. What is a policy? How does it differ from a law?Answer:A policy is a formalized description of acceptable and unacceptable employee behavior, which, when properly defined and enforced, functions the same way as laws within the organization. Unlike with law, however, ignorance is an acceptable defense, so steps must be taken to assure that policy is communicated, understood, and accepted by employees.
12. What are the three general categories of unethical and illegal behavior?Answer:The three general categories of unethical and illegal behavior that organizations and society should seek to eliminate are those arising from ignorance, those resulting from accident, and those that are intentional.
13. What is the best method for preventing illegal or unethical behavior?Answer:The best method for preventing illegal or unethical behavior is deterrence. Deterrents include laws, policy, and technical controls.
14. Of the professional organizations discussed in this chapter, which has been in existence the longest time? When was it founded?Answer:The Association forComputing Machinery (ACM) has been in existence for the longest time, having been founded in 1947.
15. Of the professional organizations discussed in this chapter, which is focused on auditing and control?Answer:The Information Systems Audit and Control Association (ISACA) focuses on auditing and control as well as other topics often associated with InfoSec.
16. What is the stated purpose of the SANS organization? In what ways is it involved in professional certification for InfoSec professionals?Answer:SANS is dedicated to the protection of information and systems by promoting GIAC certifications and requiring members to agree to its code of ethics.
17. Which U.S. federal agency sponsors the InfraGard program? Answer:The Federal Bureau of Investigation's National Infrastructure Protection Center sponsors the InfraGard program.
18. Which U.S. federal agency has taken control of the overall National Infrastructure Protection mission?Answer:The Department of Homeland Security has taken over control of the overall NIP mission.
19. What is due care? Why would an organization want to make sure it exercises due care in its usual course of operations?Answer:Due care is a company taking measures to make sure that every employee knows what is acceptable and what is not, and that every employee knows the consequences of illegal or unethical actions. In its usual course of operations, a company employs due care to protect itself against liability resulting from illegal or unethical actions by any employee.

20. What should an organization do to deter someone from violating policy or committing a crime?Answer:Successful deterrence requires the institution of severe penalties of which people are aware, the feeling by people that there is a realistic probability of apprehension, and an expectation that penalties will be enforced.

Exercises

Student answers to the following exercises will vary.

1. The $(ISC)^2$ has several certifications. Use a Web browser connected to the Internet to read about the $(ISC)^2$ certifications. What does "CISSP" stand for? Using the Internet, find out which continuing education is required for the holder of a CISSP to remain current and in good standing.
2. Use a Web browser connected to the Internet to explore the career options in cybersecurity at the U.S. National Security Agency. For what kind of InfoSec jobs does the NSA recruit? What qualifications do the jobs you found call for?
3. Using the resources available in your library, find out what laws your state has passed to prosecute computer crime.
4. Using the Web, go to *www.eff.org*. What are the current top concerns of this organization?
5. Using the ethical scenarios presented in this chapter, consider each scenario and note your response. Bring your answers to class to compare them with those of your peers.