Chapter 3 Study Guide

Indicate whether the statement is true or false.

1. The Computer Security Act of 1987 is the cornerstone of many computer-related federal laws and enforcement efforts; it was originally written as an extension and clarification of the Comprehensive Crime Control Act of 1984,

a. True

b. False

2. Cultural differences can make it difficulty to determine what is ethical and is not ethical between cultures, except when it comes to the use of computers, where ethics are considered universal.

a. True

b. False

3. The Council of Europe Convention on Cyber-Crime has not been well received by advocates of intellectual property rights because it de-emphasizes prosecution for copyright infringement, but has been well received by supporters of individual rights in the U.S.

a. True

b. False

4. The Department of Homeland Security (DHS) works with academic campuses nationally, focusing on resilience, recruitment, internationalization, growing academic maturity and academic research.

a. True

b. False

5. Laws, policies and their associated penalties only provide deterrence if offenders fear the penalty, expect to be caught, and expect the penalty to be applied if they are caught.

a. True

b. False

6. Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident.

a. True

b. False

7. Due care and due diligence require that an organization make a valid effort to protect others and continually maintain this level of effort, ensuring these actions are effective.

a. True

b. False

8. Unethical and illegal behavior is generally caused by ignorance (of policy and/or the law), by accident, and by inadequate protection mechanisms.

a. True

b. False

Chapter 3 Study Guide

9. The United States has implemented a version of the DMCA law called the Database Right, in order to comply with Directive 95/46/EC.

a. True

b. False

10. The key difference between laws and ethics is that ethics carry the authority of a governing body and laws do not.

a. True

b. False

11. The NSA is responsible for signal intelligence, information assurance products and services, and enabling computer network operations to gain a decision advantage for the US and its allies under all circumstances.

a. True

b. False

12. For policy to become enforceable it only needs to be distributed, read, understood, and agreed to.

a. True

b. False

13. Key studies reveal that legal penalties are the overriding factor in leveling ethical perceptions within a small population.

a. True

b. False

14. Since it was established in January 2001, every FBI field office has established an InfraGard program to collaborate with public and private organizations and the academic community.

a. True

b. False

15. The difference between a policy and a law is that ignorance of a law is an acceptable defense.

a. True

b. False

16. Criminal laws addresses activities and conduct harmful to society and is categorized as private or public.

a. True

b. False

17. The Secret Service is charged with safeguarding the nation’s financial infrastructure and payments systems to preserve the integrity of the economy.

a. True

b. False

18. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality’s ethical behavior violates the ethics of another national group.

a. True

b. False

Chapter 3 Study Guide

19. In the context of information security, confidentiality is the right of the individual or group to protect themselves and their information from unauthorized access.

a. True

b. False

20. Employees are not deterred by the potential loss of certification or professional accreditation resulting from a breach of a code of conduct as this loss has no effect on employees' marketability and earning power.

a. True

b. False

21. The Department of Homeland Security is the only U.S. federal agency charged with the protection of American information resources and the investigation of threats to, or attacks on, the resources.

a. True

b. False

Indicate the answer choice that best completes the statement or answers the question.

22. Which of the following acts is also widely known as the Gramm-Leach-Bliley Act?

a. Financial Services Modernization Act

b. Communications Act

c. Computer Security Act

d. Health Insurance Portability and Accountability Act

23. The Council of Europe adopted the Convention of CyberCrime in 2001 to oversee a range of security functions associated with _____ activities.

a. online terrorist b. electronic commerce

c. cyberactivist d. Internet

24. What is the subject of the Computer Security Act?

a. Federal Agency Information Security

b. Telecommunications Common Carriers

c. Cryptography Software Vendors

d. Banking Industry

25. What is the subject of the Sarbanes-Oxley Act?

a. Banking b. Financial Reporting

c. Privacy d. Trade secrets

26. According to the National Information Infrastructure Protection Act of 1996, the severity of the penalty for computer crimes depends on the value of the information obtained and whether the offense is judged to have been committed for each of the following except _____.

a. for purposes of commercial advantage b. for private financial gain

c. to harass d. in furtherance of a criminal act

Chapter 3 Study Guide

27. _____ law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.

a. Public b. Private

c. Civil d. Criminal

28. Which of the following acts is a collection of statutes that regulate the interception of wire, electronic, and oral communications?

a. Electronic Communications Privacy Act

b. Financial Services Modernization Ac

c. Sarbanes-Oxley Act

d. Economic Espionage Act

29. Which of the following acts defines and formalizes laws to counter threats from computer related acts and offenses?

a. Electronic Communications Privacy Act of 1986

b. Freedom of Information Act (FOIA) of 1966

c. Computer Fraud and Abuse Act of 1986

d. Federal Privacy Act of 1974

30. Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage _____.

a. with intent b. by accident

c. with malice d. with negligence

31. Which of the following countries reported the least tolerant attitudes toward personal use of organizational computing resources?

a. Australia b. United States

c. Singapore d. Sweden

32. Laws and policies and their associated penalties only deter if which of the following conditions is present?

a. Fear of penalty

b. Probability of being caught

c. Probability of penalty being administered

d. All of the above

33. The _____ attempts to prevent trade secrets from being illegally shared.

a. Electronic Communications Privacy Act

b. Sarbanes-Oxley Act

c. Financial Services Modernization Act

d. Economic Espionage Act

34. The Privacy of Customer Information Section of the common carrier regulation states that any proprietary information shall be used explicitly for providing services, and not for any _____ purposes.

a. troubleshooting b. billing

c. customer service d. marketing

Chapter 3 Study Guide

35. The _____ of 1999 provides guidance on the use of encryption and provides protection from government intervention.

a. Prepper Act
b. Economic Espionage Act
c. USA PATRIOT Act
d. Security and Freedom through Encryption Act

36. The Health Insurance Portability and Accountability Act Of 1996, also known as the _____ Act, protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.

a. Gramm-Leach-Bliley b. Kennedy-Kessebaum
c. Privacy d. HITECH

37. Criminal or unethical _____ goes to the state of mind of the individual performing the act.

a. attitude b. intent
c. accident d. ignorance

38. The National Information Infrastructure Protection Act of 1996 modified which Act?

a. USA PATRIOT Act
b. USA PATRIOT Improvement and Reauthorization Act
c. Computer Security Act
d. Computer Fraud and Abuse Act

39. The Computer _____ and Abuse Act of 1986 is the cornerstone of many computer-related federal laws and enforcement efforts.

a. Violence b. Fraud
c. Theft d. Usage

40. _____ law comprises a wide variety of laws that govern a nation or state.

a. Criminal b. Civil
c. Public d. Private

41. The _____ defines stiffer penalties for prosecution of terrorist crimes.

a. USA PATRIOT Act b. Sarbanes-Oxley Act
c. Gramm-Leach-Bliley Act d. Economic Espionage Act