Law and Ethics

1. What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?
   1. Evidence Circumstance Doctrine
   2. Exigent Circumstance Doctrine
   3. Evidence of Admissibility Doctrine
   4. Exigent Probable Doctrine
2. What category of law deals with regulatory standards that regulate performance and conduct? Government agencies create these standards, which are usually applied to companies and individuals within those companies?
   1. Standards law
   2. Conduct law
   3. Compliance law
   4. Administrative law
3. If an organization were to monitor their employees' e-mail, it should not:
   1. Monitor only a limited number of employees.
   2. Inform all employees that e-mail is being monitored.
   3. Explain who can read the e-mail and how long it is backed up.
   4. Explain what is considered an acceptable use of the e-mail system.
4. Computer-generated evidence is considered:
   1. Best evidence
   2. Second hand evidence
   3. Demonstrative evidence
   4. Direct evidence
5. Which of the following would be less likely to prevent an employee from reporting an incident?
   1. They are afraid of being pulled into something they don't want to be involved with.
   2. The process of reporting incidents is centralized.
   3. They are afraid of being accused of something they didn't do.
   4. They are unaware of the company's security policies and procedures.
6. The copyright law ("original works of authorship") protects the right of the owner in all of the following except?
   1. The public distribution of the idea
   2. Reproduction of the idea
   3. The idea itself
   4. Display of the idea
7. Why would a memory dump be admissible as evidence in court?
   1. Because it is used to demonstrate the truth of the contents.
   2. Because it is used to identify the state of the system.
   3. Because the state of the memory cannot be used as evidence.
   4. Because of the exclusionary rule.
8. Concern that federal agencies were not protecting information obtained about US citizens caused Congress to enact a law known as the:
   1. Computer Security Act of 1987
   2. Computer Fraud and Abuse Act of 1986
   3. Brooks Act of 1975
   4. The Privacy Act of 1974
9. Which of the following rules is less likely to allow computer evidence to be admissible in court?
   1. It must prove a fact that is material to the case.
   2. Its reliability must be proven.
   3. The process for producing it must be documented.
   4. The chain of custody of evidence must show who collected, secured, controlled, handled, transported and tampered with the evidence.
10. What rule is concerned with the legality of how the evidence was gathered?
    1. Exclusionary rule
    2. Best evidence rule
    3. Hearsay rule
    4. Investigation rule
11. One of the offences an individual or company can commit is decompiling vendor code. This is usually done in the hopes of understanding the intricate details of its functionality. What best describes this type of non-ethical engineering?
    1. Inverse engineering
    2. Backward engineering
    3. Subvert engineering
    4. Reverse engineering
12. To be admissible in court, computer evidence must be which of the following?
    1. relevant
    2. decrypted
    3. edited
    4. incriminating
13. Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the \_\_\_\_\_ Amendment. Private citizens are not subject to protecting these amendment rules of others unless they are acting as police agents.
    1. First
    2. Second
    3. Third
    4. Fourth
14. Where can the phrase "Discourage unsafe practice" can be found?
    1. Computer Ethics Institute commandments
    2. (ISC)2 Code of Ethics
    3. Internet Activities Board's Ethics and the Internet (RFC1087)
    4. CIAC Guidelines
15. What is defined as inference of information from other, intermediate, relevant facts?
    1. Secondary evidence
    2. Conclusive evidence
    3. Hearsay evidence
    4. Circumstantial evidence
16. Which of the following best defines a Computer Security Incident Response Team (CSIRT)?
    1. An organization that provides a secure channel for receiving reports about suspected security incidents.
    2. An organization that ensures that security incidents are reported to the authorities.
    3. An organization that coordinates and supports the response to security incidents.
    4. An organization that disseminates incident-related information to its constituency and other involved parties.
17. In addition to Human Resources, with what company function must the collection of physical evidence be coordinated if an employee is suspected?
    1. legal
    2. Industrial Security
    3. public relations
    4. computer security
18. Which of the following is an example of an active attack?
    1. Traffic analysis
    2. Masquerading
    3. Eavesdropping
    4. Shoulder surfing
19. Since disks and other magnetic media are only copies of the actual or original evidence, what type of evidence are they are often considered to represent?
    1. Hearsay
    2. Irrelevant
    3. Incomplete
    4. Secondary
20. The ISC2 Code of Ethics does not include which of the following behaviors for a CISSP:
    1. moral
    2. ethical
    3. legal
    4. control
21. What is the primary goal of incident handling?
    1. Successfully retrieve all evidence that can be used to prosecute
    2. Improve the company's ability to be prepared for threats and disasters
    3. Improve the company's disaster recovery plan
    4. Contain and repair any damage caused by an event.
22. Which of the following would best describe secondary evidence?
    1. Oral testimony by a non-expert witness
    2. Oral testimony by an expert witness
    3. A copy of a piece of evidence
    4. Evidence that proves a specific act
23. Which of the following statements regarding trade secrets is false?
    1. For a company to have a resource qualify as a trade secret, it must provide the company with some type of competitive value or advantage.
    2. The Trade Secret Law normally protects the expression of the idea of the resource.
    3. Many companies require their employees to sign nondisclosure agreements regarding the protection of their trade secrets.
    4. A resource can be protected by law if it is not generally known and if it requires special skill, ingenuity, and/or expenditure of money and effort to develop it.
24. Computer crime is generally made possible by which of the following?
    1. the perpetrator obtaining advanced training & special knowledge
    2. victim carelessness
    3. collusion with others in information processing
    4. system design flaws
25. Which of the following statements is not from the (ISC)2 Code of Ethics?
    1. All information systems security professionals who are certified by (ISC)2 shall observe all contracts and agreements, express or implied.
    2. All information systems security professionals who are certified by (ISC)2 shall render only those services for which they are fully competent and qualified.
    3. All information systems security professionals who are certified by (ISC)2 shall promote and preserve public trust and confidence in information and systems.
    4. All information systems security professionals who are certified by (ISC)2 shall think about the social consequences of the program they write.
26. Which category of law is also referenced as a Tort law?
    1. Civil law
    2. Criminal law
    3. Administrative law
    4. Public law
27. Which of the following outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations?
    1. The Computer Security Act of 1987.
    2. The Federal Sentencing Guidelines of 1991.
    3. The Economic Espionage Act of 1996.
    4. The Computer Fraud and Abuse Act of 1986.
28. In order to preserve a proper chain of custody of evidence:
    1. Evidence has to be collected following predefined procedures in accordance with all laws and legal regulations.
    2. Law enforcement officials should be contacted for advice on how and when to collect critical information.
    3. Verifiable documentation indicating the sequence of individuals who have handled a piece of evidence should be available.
    4. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.
29. Which of the following provides for data collection limitations, the quality of data, specifications of the purpose for data collection, limitations of data use, participation by the individual on whom the data is being collected, and accountability of the data controller?
    1. 1980 Organization for Economic Cooperation and Development (OECD) Guidelines
    2. 1974 U.S. Privacy Act
    3. 1970 U.S. Fair Credit Reporting Act
    4. 1973 U.S. Code of Fair Information Practices
30. Which of the following groups represents the leading source of computer crime losses?
    1. hackers
    2. industrial saboteurs
    3. foreign intelligence officers
    4. employees
31. Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:
    1. the company is not a multi-national company.
    2. they have not exercised due care protecting computing resources.
    3. they have failed to properly insure computer resources against loss.
    4. the company does not prosecute the hacker that caused the breach.
32. Which of the following logical access exposures involves changing data before, or as it is entered into the computer?
    1. Data diddling
    2. Salami techniques
    3. Trojan horses
    4. Viruses
33. Which of the following placed requirements of federal government agencies to conduct security-related training, to identify sensitive systems, and to develop a security plan for those sensitive systems?
    1. 1987 U.S. Computer Security Act
    2. 1996 U.S. Economic and Protection of Proprietary Information Act
    3. 1994 U.S. Computer Abuse Amendments Act
    4. 1986 (Amended in 1996) U.S. Computer Fraud and Abuse Act
34. A copy of evidence or oral description of its contents; not reliable as best evidence is what type of evidence?
    1. Direct evidence
    2. Circumstantial evidence
    3. Hearsay evidence
    4. Secondary evidence
35. Once evidence is seized, a law enforcement officer should emphasize which of the following?
    1. chain of command
    2. chain of custody
    3. chain of control
    4. chain of communications
36. Which of the following statements pertaining to the (ISC)2 Code of Ethics is incorrect?
    1. All information systems security professionals who are certified by (ISC)2 recognize that the Internet is a privilege and must be protected.
    2. All information systems security professionals who are certified by (ISC)2 shall provide diligent and competent service to principals.
    3. All information systems security professionals who are certified by (ISC)2 shall discourage such behavior as associating or appearing to associate with criminals or criminal behavior.
    4. All information systems security professionals who are certified by (ISC)2 shall promote the understanding and acceptance of prudent information security measures.
37. Which of the following is NOT defined in the Internet Activities Board (IAB) Ethics and the Internet (RFC 1087) as unacceptable and unethical activity?
    1. uses a computer to steal
    2. destroys the integrity of computer-based information
    3. wastes resources such as people, capacity and computers through such actions
    4. involves negligence in the conduct of Internet-wide experiments
38. Which of the following is NOT part of the (ISC)2 Code of Ethics?
    1. Not use a computer to harm people or interfere with other people's computer work.
    2. Execute responsibilities in a manner consistent with the highest standards of their profession,
    3. Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with resulting investigations.
    4. Not misuse the information in which they come into contact during the course of their duties, and they shall maintain the confidentiality of all information in their possession that is so identified.
39. The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?
    1. Writing computer viruses.
    2. Monitoring data traffic.
    3. Wasting computer resources.
    4. Concealing unauthorized accesses.
40. Due care is not related to:
    1. Good faith
    2. Prudent management
    3. Profit
    4. Best interest
41. Evidence life cycle does not include which of the following?
    1. Protection
    2. Identification
    3. Recording
    4. Destruction
42. Which of the following categories of hackers poses the greatest threat?
    1. Disgruntled employees
    2. Student hackers
    3. Criminal hackers
    4. Corporate spies
43. When should a post-mortem review meeting be held after an intrusion has been properly taken care of?
    1. Within the first three months after the investigation of the intrusion is completed.
    2. Within the first week after prosecution of intruders have taken place, whether successful or not.
    3. Within the first month after the investigation of the intrusion is completed.
    4. Within the first week of completing the investigation of the intrusion.
44. Under United States law, an investigator's notebook may be used in court in which of the following scenarios?
    1. When the investigator is unwilling to testify.
    2. When other forms of physical evidence are not available.
    3. To refresh the investigators memory while testifying.
    4. If the defense has no objections.
45. This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks the user needs to fulfill. What best describes this scenario?
    1. Excessive Rights
    2. Excessive Access
    3. Excessive Permissions
    4. Excessive Privileges
46. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called:
    1. alteration.
    2. investigation.
    3. re-direction.
    4. enticement.

1. Something that is proprietary to that company and importance for its survival and profitability is what type of intellectual property law?
   1. Trade Property
   2. Trade Asset
   3. Patent
   4. Trade Secret
2. Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?
   1. Direct evidence
   2. Circumstantial evidence
   3. Conclusive evidence
   4. Corroborative evidence
3. Supporting evidence used to help prove an idea or point is described as? It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.
   1. Circumstantial evidence
   2. Corroborative evidence
   3. Opinion evidence
   4. Secondary evidence
4. Which of the following exceptions is less likely to make hearsay evidence admissible in court?
   1. Records are collected during the regular conduct of business.
   2. Records are collected by senior or executive management.
   3. Records are collected at or near the time of occurrence of the act being investigated.
   4. Records are in the custody of the witness on a regular basis.
5. To understand the 'whys' in crime, many times it is necessary to understand MOM. Which of the following is not a component of MOM?
   1. Opportunities
   2. Methods
   3. Motivation
   4. Means
6. Which of the following is from the Internet Activities Board (IAB) Ethics and the Internet (RFC 1087)?
   1. Access to and use of the Internet is a privilege and should be treated as such by all users of the systems.
   2. Users should execute responsibilities in a manner consistent with the highest standards of their profession.
   3. There must not be personal data record-keeping systems whose very existence is secret.
   4. There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used or made available for another purpose without their consent.
7. In the US, HIPAA addresses which of the following?
   1. Availability and Accountability
   2. Accuracy and Privacy
   3. Security and Availability
   4. Security and Privacy