Post-Class Quiz: Legal, Regulations, Compliance & Investigation Domain

1. Laws and regulations are sources of what type of requirements?
    A. Directive
    B. Preventive
    C. Corrective
    D. Security policy

2. Copyright provides what form of protection:
    A. Protects an author's right to distribute his/her works.
    B. Protects information that provides a competitive advantage.
    C. Protects the right of an author to prevent unauthorized use of his/her works.
    D. Protects the right of an author to prevent viewing of his/her works.

3. What is the difference between a patent and a trade secret?
    A. Trade secret has no expiration date.
    B. Trade secret is a formal protection that provides a set of exclusive rights.
    C. Patent is recognized world-wide.
    D. There is no difference.

4. Due care is defined as:
    A. The prudent management and execution of security responsibilities.
    B. The minimum and customary practice of responsible protection of assets.
    C. Employment of reasonable security controls.
    D. Diligent care for the safety and security of employees.

5. The standard of proof in a criminal case is:
    A. Probable cause.
    B. Preponderance of evidence.
    C. Fair and impartial
    D. Beyond a reasonable doubt.

6. Computer crime has been difficult to define because:
    A. Laws are slow to keep up with technology.

B. It is difficult to identify computer criminals.

C. Many crimes are victimless

D. Most computer criminals are juveniles.

7. Primary factor to be considered when deciding to proceed with an investigation are:

A. Information dissemination, costs, investigative control.

B. Legal issues, publicity, time.

C. Likelihood of prosecution, availability of FBI, costs.

D. Manpower, evidence, investigative control.

8. The admissibility rule requires that evidence must be excluded if:

A. It is not pertinent.

B. It is not legally obtained.

C. It is not sufficient.

D. It is not relevant.

9. Chain of custody is primarily used to:

A. Protect evidence in a secure storage location.

B. Fix responsibility for protecting evidence.

C. Protect and account for evidence.

D. Ensure that the evidence is returned to the victim in good condition.

10. The $(ISC)^2$ Code of Ethics calls for security professionals to abide by the highest standard of:

A. Legal and ethical behavior.

B. Professional conduct.

C. Moral, legal, ethical behavior.

D. Ethical behavior.

11. What is another name for tort law?

A. Criminal

B. Administrative

C. Napoleonic

D. Civil

12. A unique packaging method or symbol is a:

A. Trade secret.

B. Patent.

C. Trademark.

D. Copyright.

13. One problem not associated with investigating Internet-based computer crime is:

A. Jurisdiction

B. Data diddling.

C. Evidence rules

D. Skill of investigators.

14. Privacy issues deal with all of the following except:

A. Gathering information

B. Dissemination of information

C. Accuracy of information

D. Proliferation of information

15. The Best Evidence Rule is designed to:

A. Ensure that only relevant material is presented in court.

B. Rank the importance of evidence according to veracity

C. Deter any alteration of evidence.

D. Require expert testimony to introduce electronic evidence.

16. Which is not a common form of evidence:

A. Direct

B. Conclusive

C. Real

D. Documentary

17. Why is computer crime difficult to investigate:

A. Privacy laws protect people from being investigated.

B. Computer crime investigations require special techniques and tools.

C. Criminals can spoof their address.

D. The police have no jurisdiction over the Internet.

18. Discs and other media that are copies of the original are considered:

A. Primary evidence

B. Reliable evidence

C. Hearsay evidence

D. Conclusive evidence.

19. Privacy laws generally include which of the following provisions:

A. Individuals have the right to remove data that they do not wish disclosed.

B. Government agencies must ensure that their data is accurate.

C. Government agencies must provide assess to all other government agencies.

D. Government agencies may not use data for a purpose other than that for which it was initially collected.

20. One reason that successful computer crime prosecution are so difficult is:

A. There is no reliable way to capture electronic data

B. Evidence in computer crime cases does not follow the Best Evidence Rule.

C. Computer crimes do not fall into traditional categories of crimes.

D. Wiretapping is difficult to do legally.

21. Which is not a unique issue when investigating and prosecuting computer crimes:

A. Investigators and prosecutors have a compressed time frame.

B. The information is “intangible”.

C. An expert of specialist may be required.

D. It is a simple matter to extract the data needed for the investigation.

22. Which of the following is not a component of “chain of evidence”:

A. Location evidence obtained.

B. Time evidence obtained.

C. Who discovered the evidence.

D. Identification of person who left the evidence.

23. Evidence may be not detected through:

A. Out of band communications

B. Accidental discovery

C. Audit trail review

D. Real-time intrusion monitoring.

24. During a preliminary investigation, you should not:

A. Inspect the damage.

B. Correct the damage.

C. Interview witnesses.

D. Inspect logs.

25. A Search and Seizure Team would not have as a member:

A. Information security representative.

B. Upper management representative.

C. Legal representative.

D. Technical representatives.