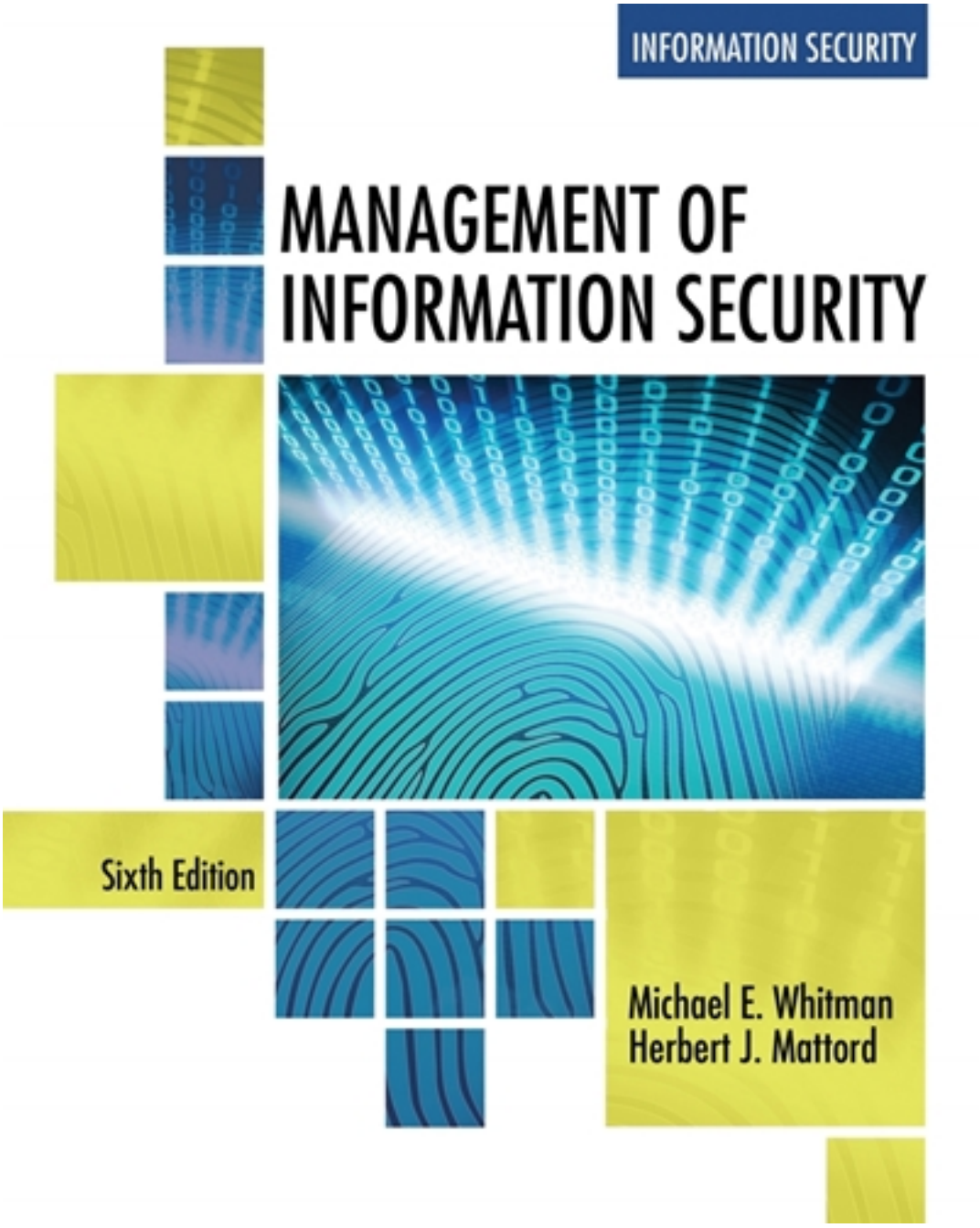
Test Bank for Management of Information Security 6th Edition by Whitman

CLICK HERE TO ACCESS COMPLETE Test Bank



Test Bank

TRUE/FALSE

1 : Ethics carry the sanction of a governing authority.
A : true
B : false

Correct Answer : B

2 : The Secret Service is charged with the detection and arrest of any person who commits a U.S. federal offense relating to computer fraud, as well as false identification crimes.
A : true
B : false

Correct Answer : A

3 : ?Deterrence is the best method for preventing an illegal or unethical activity. _____
A : true
B : false

Correct Answer : A

4 : ISACA is a professional association with a focus on authorization, control, and security. _____
A : true
B : false

Correct Answer : B

5 : Information ambiguation occurs when pieces of nonprivate data are combined to create information that violates privacy. _____
A : true
B : false

Correct Answer : B

6 : The Gramm-Leach-Bliley (GLB) Act, also known as the Financial Services Modernization Act of 1999, contains a number of provisions that affect banks, securities firms, and insurance companies. _____
A : true
B : false

Correct Answer : A

7 : To protect intellectual property and competitive advantage, Congress passed the Entrepreneur Espionage Act (EEA) in 1996.? _____
A : true
B : false

Correct Answer : B

8 : A(n) compromise law specifies a requirement for organizations to notify affected parties when they have experienced a specified type of loss of information. _____

A : true
B : false

Correct Answer : B

9 : It is the responsibility of InfoSec professionals to understand state laws and bills. _____
A : true
B : false

Correct Answer : B

10 : ?Due diligence requires that an organization make a valid and ongoing effort to protect others. _____
A : true
B : false

Correct Answer : A

11 : InfraGard began as a cooperative effort between the FBI’s Cleveland field office and local intelligence ?professionals.? _____
A : true
B : false

Correct Answer : B

SHORT RESPONSE

12 : Describe the foundations and frameworks of ethics.

Correct Answer : Normative ethics—The study of what makes actions right or wrong, also known as moral theory—that is, how should people act?Meta-ethics—The study of the meaning of ethical judgments and properties—that is, what is right?Descriptive ethics—The study of the choices that have been made by individuals in the past—that is, what do others think is right?Applied ethics—An approach that applies moral codes to actions drawn from realistic situations; it seeks to define how we might use ethics in practice.Deontological ethics—The study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences; also known as duty-based or obligation-based ethics. This approach seeks to define a person’s ethical duty.

13 : Discuss the three general categories of unethical behavior that organizations should try to control.

Correct Answer : Ignorance:Ignorance of the law is no excuse, but ignorance of policies and procedures is. The first method of deterrence is education. Organizations must design, publish, and disseminate organizational policies and relevant laws, and employees must explicitly agree to abide by them. Reminders, training, and awareness programs support retention, and one hopes, compliance.?Accident:Individuals with authorization and privileges to manage information within the organization have the greatest opportunity to cause harm or damage by accident. The careful placement of controls can help prevent accidental modification to systems and data.?Intent:Criminal or unethical intent refers to the state of mind of the individual committing the infraction. A legal defense can be built upon whether the accused acted out of ignorance, by accident, or with the intent to cause harm or damage. Deterring those with

criminal intent is best done by means of litigation, prosecution, and technical controls. Intent is only one of several factors to consider when determining whether a computer-related crime has occurred.

14 : Laws and policies and their associated penalties only deter if three conditions are present. What are these conditions?

Correct Answer : Fear of penalty—Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.Probability of being caught—There must be a strong possibility that perpetrators of illegal or unethical acts will be caught.Probability of penalty being administered—The organization must be willing and able to impose the penalty.

15 : Briefly describe five different types of laws.

Correct Answer : 1. Civil law embodies a wide variety of laws pertaining to relationships between and among individuals and organizations.2. Criminal law addresses violations harmful to society and is actively enforced and prosecuted by the state.3. 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.4. Private law regulates the relationships among individuals and among individuals and organizations, and encompasses family law, commercial law, and labor law.5. Public law regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

16 : The penalty for violating the National Information Infrastructure Protection Act of 1996 depends on the value of the information obtained and whether the offense is judged to have been committed for one of three reasons. What are those reasons?

Correct Answer : For purposes of commercial advantageFor private financial gainIn furtherance of a criminal act

17 : The Computer Security Act charges the National Bureau of Standards, in cooperation with the National Security Agency (NSA), with the development of five standards and guidelines establishing minimum acceptable security practices. What are three of these principles?

Correct Answer : Standards, guidelines, and associated methods and techniques for computer systemsUniform standards and guidelines for most federal computer systemsTechnical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systemsGuidelines for use by operators of federal computer systems that contain sensitive informationin training their employees in security awareness and accepted security practiceValidation procedures for, and evaluation of the effectiveness of, standards and guidelinesthrough research and liaison with other government and private agencies

18 : Describe the Freedom of Information Act. How does its application apply to federal vs. state agencies?

Correct Answer : All federal agencies are required under the Freedom of Information Act (FOIA) to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public

access laws that should be consulted for access to state and local records.

19 : What is a key difference between law and ethics?

Correct Answer : The key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not.

20 : A key difference between policy and law is that ignorance of policy is a viable defense. What steps must be taken to assure that an organization has a reasonable expectation that policy violations can be appropriately penalized without fear of legal retribution?

Correct Answer : Policies must be:Effectively writtenDistributed to all individuals who are expected to comply with themRead by all employeesUnderstood by all employees, with multilingual translations and translations for visually impaired or low-literacy employeesAcknowledged by the employee, usually by means of a signed consent formUniformly enforced, with no special treatment for any group (e.g., executives)

MULTIPLE CHOICE

21 : Which of the following ethical frameworks is the study of the choices that have been made by individuals in the past?
A : Applied ethics
B : Descriptive ethics
C : Normative ethics
D : Deontological ethics

Correct Answer : B

22 : Which of the following is the study of the rightness or wrongness of intentions and motives as opposed to the rightness or wrongness of the consequences (also known as duty- or obligation-based ethics)?
A : Applied ethics
B : Meta-ethics
C : Normative ethics
D : Deontological ethics

Correct Answer : D

23 : Which ethical standard is based on the notion that life in community yields a positive outcome for the individual, requiring each individual to contribute to that community?
A : utilitarian
B : virtue
C : fairness or justice
D : common good

Correct Answer : D

24 : There are three general categories of unethical behavior that organizations and society should seek to eliminate. Which of the following is NOT one of them?
A : ignorance
B : malice

C : accident
D : intent

Correct Answer : B

25 : Which of the following is the best method for preventing an illegal or unethical activity? Examples include laws, policies, and technical controls.
A : remediation
B : deterrence
C : persecution
D : rehabilitation

Correct Answer : B

26 : Which of the following is NOT a requirement for laws and policies to deter illegal or unethical activity?
A : fear of penalty
B : probability of being penalized
C : probability of being caught
D : fear of humiliation

Correct Answer : D

27 : Which of the following organizations put forth a code of ethics designed primarily for InfoSec professionals who have earned their certifications? The code includes the canon: Provide diligent and competent service to principals.
A : $(ISC)^2$
B : ACM
C : SANS
D : ISACA

Correct Answer : A

28 : Which subset of civil law regulates the relationships among individuals and among individuals and organizations?
A : tort
B : criminal
C : private
D : public

Correct Answer : C

29 : Which of the following is NOT used to categorize some types of law?
A : constitutional
B : regulatory
C : statutory
D : international

Correct Answer : D

30 : Which law addresses privacy and security concerns associated with the electronic transmission of PHI?
A : USA PATRIOT Act of 2001

B : American Recovery and Reinvestment Act
C : Health Information Technology for Economic and Clinical Health Act
D : National Information Infrastructure Protection Act of 1996

Correct Answer : C

31 : The penalties for offenses related to the National Information Infrastructure Protection Act of 1996 depend on whether the offense is judged to have been committed for several reasons. Which of the following is NOT one of those reasons?
A : For purposes of commercial advantage
B : For private financial gain
C : For political advantage
D : In furtherance of a criminal act

Correct Answer : C

32 : Which law requires mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of a federal computer system?
A : The Telecommunications Deregulation and Competition Act
B : National Information Infrastructure Protection Act
C : Computer Fraud and Abuse Act
D : The Computer Security Act

Correct Answer : D

33 : Which act is a collection of statutes that regulates the interception of wire, electronic, and oral communications?
A : The Electronic Communications Privacy Act of 1986
B : The Telecommunications Deregulation and Competition Act of 1996
C : National Information Infrastructure Protection Act of 1996
D : Federal Privacy Act of 1974

Correct Answer : A

34 : Which act requires organizations that retain health care information to use InfoSec mechanisms to protect this information, as well as policies and procedures to maintain them?
A : ECPA
B : Sarbanes-Oxley
C : HIPAA
D : Gramm-Leach-Bliley

Correct Answer : C

35 : Which law extends protection to intellectual property, which includes words published in electronic formats?
A : Freedom of Information Act
B : U.S. Copyright Law
C : Security and Freedom through Encryption Act
D : Sarbanes-Oxley Act

Correct Answer : B

36 : A more recently created area of law related to information security specifies a requirement for organizations to notify affected parties when they have experienced a specified type of information loss. This is commonly known as a _____ law.
A : notification
B : breach
C : spill
D : compromise

Correct Answer : B

37 : Which of the following is the result of a U.S. led international effort to reduce the impact of copyright, trademark, and privacy infringement, especially via the removal of technological copyright protection measures?
A : U.S. Copyright Law
B : PCI DSS
C : European Council Cybercrime Convention
D : DMCA

Correct Answer : D

38 : This collaborative support group began as a cooperative effort between the FBI's Cleveland field office and local technology professionals with a focus of protecting critical national infrastructure.
A : InfraGard
B : Homeland Security
C : CyberWatch
D : CyberGard

Correct Answer : A

39 : Another key U.S. federal agency is _____, which is responsible for coordinating, directing, and performing highly specialized activities to protect U.S. information systems and produce foreign intelligence information.
A : InfraGard
B : Homeland Security
C : the National Security Agency
D : the Federal Bureau of Investigation

Correct Answer : C

40 : Which of the following is compensation for a wrong committed by an individual or organization?
A : liability
B : restitution
C : due diligence
D : jurisdiction

Correct Answer : B

41 : Any court can impose its authority over an individual or organization if it can establish which of the following?
A : jurisprudence
B : jurisdiction

C : liability
D : sovereignty

Correct Answer : B

42 : Investigations involving the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis are known as _____.

A : digital forensics
B : criminal investigation
C : crime scene investigation
D : e-discovery

Correct Answer : A

43 : Also known as “items of potential evidentiary value,” any information that could potentially support the organization’s legal or policy-based case against a suspect is known as _____.

A : evidentiary material
B : digital forensics
C : evidence
D : e-discovery

Correct Answer : A

44 : The coherent application of methodical investigatory techniques to collect, preserve, and present evidence of crimes in a court or court-like setting is known as _____.

A : evidentiary material
B : forensics
C : crime scene investigation
D : data imaging

Correct Answer : B

45 : Permission to search for evidentiary material at a specified location and/or to seize items to return to the investigator’s lab for examination is known as a(n) _____.

A : subpoena
B : forensic clue
C : search warrant
D : affidavit

Correct Answer : C

46 : Sworn testimony that certain facts are in the possession of the investigating officer and that they warrant the examination of specific items located at a specific place is known as a(n) _____.

A : subpoena
B : forensic finding
C : search warrant
D : affidavit

Correct Answer : D

47 : A process focused on the identification and location of potential evidence related to a specific legal action after it was collected through digital forensics is known as _____.

A : e-discovery
B : forensics
C : indexing
D : root cause analysis

Correct Answer : A

48 : Digital forensics can be used for two key purposes: _____ or _____.

A : e-discovery; to perform root cause analysis
B : to investigate allegations of digital malfeasance; to perform root cause analysis
C : to solicit testimony; to perform root cause analysis
D : to investigate allegations of digital malfeasance; to solicit testimony

Correct Answer : B

49 : In digital forensics, all investigations follow the same basic methodology once permission to search and seize is received, beginning with _____.

A : identifying relevant items of evidentiary value
B : acquiring (seizing) the evidence without alteration or damage
C : analyzing the data without risking modification or unauthorized access
D : investigating allegations of digital malfeasance

Correct Answer : A

50 : _____ devices often pose special challenges to investigators because they can be configured to use advanced encryption and they can be wiped by the user even when the user is not present.

A : Portable
B : Desktop computer
C : Expansion
D : Satellite transceiver

Correct Answer : A

51 : The most complex part of an investigation is usually _____.

A : analysis for potential EM
B : protecting potential EM
C : requesting potential EM
D : preventing the destruction of potential EM

Correct Answer : A

52 : When an incident violates civil or criminal law, it is the organization’s responsibility to notify the proper authorities; selecting the appropriate law enforcement agency depends on _____.

A : the type of crime committed
B : how many perpetrators were involved
C : the network provider the hacker used
D : what kind of computer the hacker used

Correct Answer : A

MATCHING

53 : ?

A : One of the first attempts to protect federal computer systems by establishing minimum acceptable security practices.	A : criminal law
B : Focuses on enhancing the security of the critical infrastructure in the United States.	B : public law
C : An approach that applies moral codes to actions drawn from realistic situations.	C : ethics
D : A collection of statutes that regulates the interception of wire, electronic, and oral communications.	D : Computer Security Act (CSA)
E : Regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments.	E : Electronic Communications Privacy Act (ECPA)
F : The study of what makes actions right or wrong, also known as moral theory.	F : Cybersecurity Act
G : Addresses violations harmful to society and is actively enforced and prosecuted by the state.	G : normative ethics
H : Defines socially acceptable behaviors.	H : applied ethics

Correct Answer :
A : D

B : F

C : H

D : E

E : B

F : G

G : A

H : C

FILL IN THE BLANK

54 : Ethics are based on _____, which are the relatively fixed moral attitudes or customs of a societal group.

Correct Answer : cultural mores

55 : The branch of philosophy that considers nature, criteria, sources, logic, and the validity of moral judgment is known as _____.

Correct Answer : ethics

56 : The act of attempting to prevent an unwanted action by threatening punishment or retaliation on the instigator if the act takes place is known as _____.

Correct Answer : deterrence

57 : _____ is a subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury.

Correct Answer : Tort law

58 : Information _____ occurs when pieces of nonprivate data are combined to create information that violates privacy.

Correct Answer : aggregation

59 : An organization increases its liability if it refuses to take the measures a prudent organization should; this is known as the standard of _____.

Correct Answer : due care

60 : Investigations involving the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis are known as _____.

Correct Answer : digital forensics

61 : _____ devices often pose special challenges to investigators because they can be configured to use advanced encryption and they can be wiped by the user even when the user is not present.

Correct Answer : Portable

62 : A process focused on the identification and location of potential evidence related to a specific legal action after it was collected through digital forensics is known as _____.

Correct Answer : ediscovery

63 : Sworn testimony that certain facts are in the possession of the investigating officer and that they warrant the examination of specific items located at a specific place is known as a(n) _____.

Correct Answer : affidavit