QUIZIZZ Worksheets

BSIT 3-1N - AIS 2nd Quiz - 4-29-2024

Total questions: 30

Worksheet time: 15mins

Instructor name: Mr. Montaigne Molejon

Name

Class

Date

1. Which community of interest would be most concerned with the ease of use and user interface of a new software application?

a) Organizational Management and Professionals
b) Legal Department
c) Information Technology Management and Professionals
d) Information Security Management and Professionals

2. Which community of interest within an organization is primarily tasked with the responsibility of focusing on safeguarding the organization's information systems and digital data?

a) Organizational Management and Professionals
b) Information Technology Management and Professionals
c) Legal Department
d) Information Security Management and Professionals

3. When an organization deliberate whether to continue with in-house software development and opting for outsourcing, which community of interest is charged with the task of thoroughly analyzing and assessing the financial implications associated with each option?

a) Organizational Management and Professionals
b) Legal Department
c) Information Technology Management and Professionals
d) Information Security Management and Professionals

4. When a data breach occurs that compromises sensitive customer information, which specific community of interest within the organization holds the primary responsibility for initiating the response and effectively managing the aftermath of the breach?

a) Information Security Management and Professionals
b) Information Technology Management and Professionals
c) Legal Department
d) Organizational Management and Professionals

5. An organization is implementing a new enterprise resource planning (ERP) system. Which community of interest is likely to focus on how the ERP system supports production management and resource allocation?

a) Information Technology Management and Professionals
b) Legal Department
c) Information Security Management and Professionals
d) Organizational Management and Professionals

6. Which of the following best supports the "Security as Science" perspective?

a) The influence of end-user behavior on the overall security of an information system
b) The importance of understanding organizational behavior and change management for effective security
c) The role of technology developed by computer scientists and engineers in achieving rigorous security performance
d) The need for security administrators to have flexibility in implementing security mechanisms

7. Which of the following statements best reflects the integration of the "Security as Art" and "Security as Science" perspectives?

a) Security should be primarily focused on the behavior and interactions of individuals within the organization
b) Security implementation should be a purely technical exercise, focused on the latest security technologies
c) Security is a balance between the creative application of security mechanisms and the use of scientifically-developed technologies
d) Security administrators should strictly follow industry standards and best practices

8. Your organization is considering implementing a new security system that will significantly impact the daily workflow of employees. Which of the following approaches would be most effective in addressing the concerns of both the "Security as Art" and "Security as Social Science" perspectives?

a) Relying solely on the expertise and creativity of the security administrators to design and implement the security measures
b) Conducting a thorough technical analysis of the security system and its compliance with industry standards
c) Engaging with end-users to understand their needs and preferences, and then tailoring the security system accordingly, while also considering the latest security technologies.
d) Focusing on the development of a comprehensive security policy that outlines the organization's security requirements and expectations for all employees.

9. Which aspect of security management is emphasized when security is viewed as a social science?

a) Deployment of untested technologies
b) Enhancing user performance and security through appropriate policies and training
c) Focusing exclusively on external threats
d) Isolating the security team from the rest of the organization

10. What is the most common type of intellectual property breach?

a) Copyright infringement
b) Software piracy
c) Patent infringement
d) Trade secret theft

11. A developer finds that sections of their proprietary code have been used in another company's software without permission. What type of intellectual property compromise does this represent?

a) Trademark infringement
b) Violation of trade secrets
c) Copyright infringement
d) Patent infringement

12. What is the function of a license agreement during software installation?

a) To install additional software components without user consent
b) To track the number of installations
c) To legally bind the user to terms that permit use of the software
d) To ensure the software installs correctly

13. Which of the following statements about intellectual property is TRUE?

a) Intellectual property includes trade secrets, copyrights, trademarks, and patents
b) Intellectual property is limited to the ownership of tangible representations of ideas
c) Intellectual property always involves royalty payments or permission from the owner
d) Intellectual property always involves royalty payments or permission from the owner

14. What is the primary purpose of a backdoor in cybersecurity?

a) To provide the attacker with remote access to a compromised system
b) To display advertisements.
c) To warn users about potential system infections.
d) To replicate malicious code

15. Which of the following is NOT a type of malicious code?

a) Mail Bombing
b) Trojan Horse
c) Virus
d) Worm

16. What characteristic distinguishes a worm from a virus?

a) A worm can replicate itself without needing to attach to another program
b) A worm can replicate itself without needing to attach to another program
c) A worm requires human interaction to spread
d) A worm is less harmful than a virus

17. An act of intentional or unintentional accessing or damaging a computer system without permission or authorization, with the goal of stealing, modifying, or destroying sensitive data or disrupting normal system operations

a) Attacks
b) Exploit
c) Risk
d) Human Error

18. This refers to the likelihood of an undesirable event to occur, such as a security breach or data loss. Organizations must identify and assess these undesirable events in order to implement appropriate measures.

a) Attacks
b) Risk
c) Human Error
d) Exploit

19. Which of the following is a common type of electronic disruption to an organization's internet connection?

a) Intentional or accidental electrical disruptions
b) A contractor digging up a cable
c) None of the mentioned
d) A tree falling on a communication line

20. Why are employees considered a significant threat to an organization's information security?

a) They lack the technical skills to use information systems
b) They are the closest threat agents to organizational data
c) They often have malicious intentions
d) They are not aware of the existence of data

21. Which aspect ensures that a policy is applied fairly across an organization?

a) Comprehensive writing
b) Uniform enforcement
c) Employee feedback
d) Legal approval

22. What is required for an organization to demonstrate compliance with an enforceable policy?

a) Policies must be available in English only
b) Enforcement must vary based on the employee’s role
c) Employees must be aware of the policy only
d) Employees must sign a document indicating understanding and agreement to the policy

23. What is the primary purpose of **due diligence** in an organizational context?

a) To ensure uniform enforcement of policies
b) To protect the organization from legal liability
c) To establish policies and procedures
d) To make a valid effort to protect others

24. Your organization has recently been sued for an employee's unethical actions that caused harm to a client. What is the MOST likely reason the organization is being held liable?

a) The organization did not ensure employees understood the policies
b) The organization did not uniformly enforce its policies
c) The organization failed to establish clear policies
d) The organization did not properly disseminate its policies

25. How does the concept of due care differ from the concept of due diligence in an organizational context?

a) Due care is a legal obligation, while due diligence is a voluntary effort
b) Due care is a short-term action, while due diligence is a long-term process
c) Due care focuses on protecting the organization, while due diligence focuses on protecting others
d) Due care focuses on establishing policies, while due diligence focuses on enforcing them

26. A government agency is sued for not following proper administrative procedures. Which type of law does this scenario involve?

a) Civil law
b) Private law
c) Criminal law
d) Public law

27. A citizen challenges a new law claiming it infringes on their constitutional rights. Under which category of law would this case be classified?

a) Criminal law
b) Private law
c) Public law
d) Civil law

28. Which commandment from the 10 commandments of computer ethics directly addresses the issue of software piracy?

a) Thou shalt not use a computer to bear false witness
b) Thou shalt not copy or use proprietary software for which you have not paid
c) Thou shalt not interfere with other people's computer work
d) Thou shalt not steal

29. An employee accesses a coworker's personal files without permission. Which commandment does this violate?

a) Thou shalt not snoop around in other people's computer files
b) Thou shalt not interfere with other people's computer work
c) Thou shalt not use a computer to steal
d) Thou shalt not use a computer to harm other people

30. What is the ethical principle behind the commandment, "Thou shalt not use a computer to bear false witness"?

a) Promoting the accurate and honest sharing of information
b) Allowing unlimited access to information
c) Ensuring all software is free
d) Preventing physical damage to computers

Answer Keys

1. c) Information Technology Management and Professionals
2. d) Information Security Management and Professionals
3. a) Organizational Management and Professionals
4. a) Information Security Management and Professionals
5. d) Organizational Management and Professionals
6. c) The role of technology developed by computer scientists and engineers in achieving rigorous security performance
7. c) Security is a balance between the creative application of security mechanisms and the use of scientifically-developed technologies
8. c) Engaging with end-users to understand their needs and preferences, and then tailoring the security system accordingly, while also considering the latest security technologies.
9. b) Enhancing user performance and security through appropriate policies and training
10. b) Software piracy
11. c) Copyright infringement
12. c) To legally bind the user to terms that permit use of the software
13. a) Intellectual property includes trade secrets, copyrights, trademarks, and patents
14. a) To provide the attacker with remote access to a compromised system
15. a) Mail Bombing
16. a) A worm can replicate itself without needing to attach to another program
17. a) Attacks
18. b) Risk
19. a) Intentional or accidental electrical disruptions
20. b) They are the closest threat agents to organizational data
21. b) Uniform enforcement
22. d) Employees must sign a document indicating
23. d) To make a valid effort to protect others
24. b) The organization did not uniformly enforce its policies

understanding and agreement to the policy

25. c) Due care focuses on protecting the organization, while due diligence focuses on protecting others

26. d) Public law

27. c) Public law

28. b) Thou shalt not copy or use proprietary software for which you have not paid

29. a) Thou shalt not snoop around in other people's computer files

30. a) Promoting the accurate and honest sharing of information