MTQuiz2: Test3

Due Sep 29 at 7:30am   **Points** 37   **Questions** 28   **Time Limit** 45 Minutes

Instructions

Answer the quiz according to what is needed, this quiz is composed of multiple choice with multiple answers, fill in the blanks and Essay question. Take note that the quiz is time limited so make the most of your time, you cannot return to the previous questions, therefore make sure of your answers. If you cannot submit the quiz on time, the system will automatically submit your scores. Good luck!!!

Attempt History

	Attempt	**Time**	**Score**
LATEST	**Attempt 1**	14 minutes	31 out of 37

⚠ Correct answers are hidden.

Score for this quiz: **31** out of 37
Submitted Sep 28 at 6:08pm
This attempt took 14 minutes.

Question 1	**2 / 2 pts**

What are the two pre-historic computers used by military in Information Assurance?

- ☐ Analytical Engine
- ☐ UNIVAC
- ☑ ENIAC
- ☐ EDSAC
- ☑ Bombe

Question 2	**2 / 2 pts**

What are the two reasons why Business planning always involves a tradeoff between cost and benefits.

- ☐ Legislative and regulatory mandates
- ☑ Costs come in various forms.
- ☐ Potential for loss
- ☑ Business is inherently profit-driven.
- ☐ Business reputation

Incorrect

Question 3	**0 / 2 pts**

What are the benefits of Information assurance for commercial enterprises. Choose all that apply.

☑ Providing for recovery in case of disaster

☑ Legislative and regulatory mandates

☐ Potential for loss

☐ Competitive advantage

☑ Enabling safe operation of business services

☑ Assisting the organization in meeting regulatory requirements

---

Question 4   1 / 1 pts

What type of Security safeguards generally identified as access control, identification and authentication, encryption, intrusion detection.

⦿ technical

◯ non-technical

◯ physical

◯ logical

Question 5   2 / 2 pts

What are the Functional Components of Information assurance?

Choose all that apply.

☑ protection

☐ cyber space protection

☑ capability restoration

☐ impacts and losses to their opponents

☑ response

☐ infrastructure systems

☑ detection

Question 6   1 / 1 pts

An asset like devices, computers, people that have value so are worth protecting?

◯ logical assets

◯ technical assets

   ○ non technical assets

   ◉ physical assets

   ○ systems assets

Question 7   1 / 1 pts

A _____ is a category of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

answer in lowercase only.

> threat

Question 8   1 / 1 pts

What federal law established in 1974, that pertains to the release of and access to educational records?

answer in lowercase only.

> family educational rights and privacy act

Question 9   1 / 1 pts

What specific HIPAA Admin Security Safeguards that focuses on authorization and supervision, clearance termination procedures.

answer in lowercase only.

> workforce security

Question 10   1 / 1 pts

A model of operation for computers handling classified information all users cleared, but must be need-to-know compartments (mandatory access control). System must handle requests across classifications.

   ○ multi-level

   ○ dedicated

   ○ system-high

○ compartmented

Question 11   1 / 1 pts

This act expressly prohibits the government from propagandizing the American public with information and psychological operations directed at foreign audiences.

answer in lower case only

| smith-mundt act |

Incorrect

Question 12   0 / 1 pts

A _____ is a weakness or fault in a system that exposes information to attack.

answer in lowercase only

| dangling threat |

Question 13   1 / 1 pts

A _____ is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).

answer in lowercase only

| dangling threat |

Question 14   1 / 1 pts

A follow-on to Health Insurance Portability and Accountability Act that provides additional protection relating to financial reporting and disclosure.

⦿ Patient's Omnibus Transaction on Mandatory Information Security

○ Security Rule

○ physical security

○ Privacy Rule

○ technical security

Question 15

1 / 1 pts

An the term _____ is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

○ compromise

○ exposure

○ object

◉ indicator

Question 16

1 / 1 pts

_____ is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.

answer in lowercase only.

risk

Question 17

1 / 1 pts

_____ is a process for an organization to identify and address the potential threat in their environment.

answer in lowercase only

risk management

Question 18

4 / 4 pts

What composes OODA? write your answer in lowercase

observe

orient

decide

act

Answer 1:

observe

Answer 2:

   orient

Answer 3:

   decide

Answer 4:

   act

Question 19   1 / 1 pts

It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.

answer in lowercase only.

> cyber espionage

Question 20   1 / 1 pts

Military activities that use computers and satellites for coordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

- ◉ Equipment disruption

- ○ Gathering data

- ○ Distributed Denial-of-Service Attacks

- ○ Propaganda

- ○ Web vandalism

Question 21   1 / 1 pts

Rearrange the letters to fill in the blank.

N M A L A S E I O

Behavior-based analysis involves using baseline information to detect _____ that could indicate an attack.

answer in lower case only.

> anomalies

Question 22   1 / 1 pts

Which protocol is used by the Cisco Cyberthreat Defense Solution to collect information about the traffic that is traversing the network?

○ HTTPS

○ NAT

○ Telnet

◉ NetFlow

Question 23   1 / 1 pts

Which stage of the kill chain used by attackers focuses on the identification and selection of targets?

○ exploitation

○ weaponization

◉ reconnaissance

○ delivery

Incorrect

Question 24   0 / 1 pts

During a cyberwarfare attack, which group is responsible for disabling the firewalls and IDS systems of the target?

○ offensive operations teams

◉ backdoor team

○ internal users

○ defense suppression team

Question 25   1 / 1 pts

Which security threat method would be used to target a specific demographic such as government workers for a particular country?

○ cloud computing

◉ search engine optimization (SEO) poisoning

○ cyberwar

○ money mules

Question 26   1 / 1 pts

True or False?
Cyberwarfare can be launched by a small group of highly skilled attackers.

○ True

◉ False

Question 27   1 / 1 pts

Refer to the exhibit. Rearrange the letters to fill in the blank.

E O P R I S N O A T

A recommended Enterprise Security Architecture consists of 5 layers; Security Drivers, Security Program Management, Security Governance, Security _____ and Security Technology Architecture.

answer in lowercase only.

operations

Partial

Question 28   1 / 3 pts

What are the three strategic end goals of cybersecurity? (Choose three.)

☑ preventing people from becoming hackers

☑ preventing strategic collapse

☐ deterring and disrupting hackers

☐ detecting anomalies in the organization

☐ stopping the creation of malware

☑ protecting information assets

Quiz Score: **31** out of 37

☑ protecting information assets