Cyber Security and Privacy, IIT Madras

**Week 1 Quiz**

1. A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source is:

a. Spear Phishing b. Man in the Middle Attack

c. Smurf Attack d. Social media phishing

1. A malicious attack where hackers encrypt an organization’s data and demand payment to restore access is known as:

a. Spyware b. Ransomware

c. Whaling d. Watering hole attack

1. Which of the following characteristics are most likely to be found in a phishing email?

a. Sense of urgency and immediate action requests.

b. Unusual or inappropriate requests

c. Incorrect sender name or email address.

d. All of the above.

1. From a managerial perspective, Information Security is generally understood as a:

a. Product b. Technology

d. Product, Technology and Process c. Process

1. The practice of keeping an organization's network infrastructure secure from unauthorized access is known as:

a. Data Security b. Network Security

c. Information Security d. Operations Security

1. Which of the following statements most accurately reflects the complex role of technology in cybersecurity?

a. Technology acts as both a source of threats and a tool for defense.

b. Technology is solely a source of threats and vulnerabilities.

c. Technology plays a triple role: source of threats, asset to protect, and defense weapon.

d. Technology solely serves as a defense weapon against cyberattacks.

1. \_\_\_\_\_\_\_ is a manipulation technique that exploits human weakness to gain private information, access, or valuables

a. Spyware c. Logic Bomb

c. Social Engineering d. Man in the Middle Attack

1. True or False: The word "Cyber" in "Cybernetics" originates from the French language.

a. True b. False

1. The impact of a cyber security incident on organizations can include:

a. Financial Loss b. Reputation Damage

c. Regulatory fine d. All the above

1. True or False: A Vendor guarantees that their IoT solutions are 100% safe from cyberattacks. This statement can be

a. True b. False

**Week 2 Quiz**

1.CIA triad refers to:

a. Confidentiality, Integrity and Availability

b. Confidentiality, Integrity and Authentication

c. Confidentiality, Integrity and Authorization

d. Cybersecurity, Investigation and Authentication.

2. What aspect emerges from the intersection of 3 components of Information Security?

a. Technology b. Policy

c. Human Security d. None of the

3. -------------, authentication and authorization are means to ensure CIA.

a. Investigation b. Identification

c. Classification d. Verification

4. Should all 27 cells of McCumber’s Cube be addressed with the same priority?

a. True b. False.

5. Which of the following is/ are the design principles of high availability systems

a. Eliminate single points of failure

b. Ensure reliable crossover

c. Identify failures in real time

d. All the above

6.In ensuring confidentiality, what is the crucial process that involves classifying information and and individuals, and mapping them based on the level of access?

a. Identification b. Authentication

c. Authorization d. Encryption

7. In addition to cryptography, a number of measures may be used for confidentiality, including:

a. Information classification b. Secure document storage

c. Application of general security policies d. All the above

8. When a control provides assurance that every activity undertaken can be attributed to a n named person or automated process, it is known as:

a. Integrity b. Accountability

c. Accessibility d. Authenticity

9. Identify the components of Information Security

a. Network Security b. Computer & Data Security

c. Management of Information Security d. All of the above

10. Which are the three types of power McCumber’s Cube identifies?

a. Technologies b. Policies and Practices

c. People d. All the above

**Week 3 Quiz**

1. The process of defining and specifying the long-term direction to be taken by an organization a and the allocation and acquisition of resources needed to pursue this effort is known as:

a. Governance b. Security Management

c. Strategic Planning d. Objectives

2. Which of the following statements best describes the relationship between GRC (Governance, . Risk, and Compliance) and cybersecurity ?

a. GRC focuses solely on cybersecurity management and overlooks other risk management . . .. initiatives.

b. Cybersecurity is the primary focus of GRC, with minimal consideration for other risks.

c. GRC integrates cybersecurity as one component within the broader framework of enterprise risk .. management (ERM).

d. GRC is a standalone framework independent of cybersecurity and risk management.

3. A written document provided by management that inform employees and others in the workplace . about proper behavior regarding the use of information and information assets are known as:

a. Guidelines b. Information Security Policy

c. De facto standard d. Practices

4. Which approach to cybersecurity management treats cybersecurity as a separate category distinct from other risks an organization may face, and focuses solely on cybersecurity, depending on the size and nature of the organization?

a. Standard Driven Approach

b. Organization Planning Approach

c. GRC Framework

d. Risk Management Framework

5. Benefits of implementing a GRC in an organization include:

a. Responsible operations

b. Data-driven decision-making

c. Improved cybersecurity

d. All the above

6. What is the purpose of the COBIT maturity model?

a. To assess an organization's maturity in IT governance processes

b. To rank organizations based on their financial performance

c. To determine the efficiency of network infrastructure

d. To evaluate employee satisfaction levels in the IT department

7. COSO's ERM framework emphasizes:

a. Operational efficiency b. Risk identification and assessment

c. Regulatory compliance d. Human resource management

8 . Which characteristic distinguishes the approaches of COBIT, COSO, and COSO-ERM from specific standards like ISO or NIST?

a. They prioritize cybersecurity over other risk management aspects.

b. They focus exclusively on small to medium-sized enterprises (SMEs).

c. They operate at the enterprise level rather than focusing on specific standards.

d. They are primarily developed by governmental regulatory bodies.

9. Why might some countries be hesitant to adopt the ISO 27001 model?

a. It is a mandatory standard with strict compliance requirements.

b. It is not recognized as a valid security framework by international organizations.

c. There are concerns about the model's overall effectiveness compared to existing approaches.

d. It prioritizes specific security vendors or technologies

10. Which of the following is not considered a principle or practice for securing IT systems?

a. Implement layered security to ensure there is no single point of vulnerability.

b. Do not implement unnecessary security mechanisms.

c. Maximize the system elements to be trusted.

d. Assume that external systems are insecure

**Week 4 Quiz**

1. A facility that provides only rudimentary services, with no computer hardware or peripherals is . known as:

a. Cold site b. Hot site

c. Warm site d. Service bureau

2. The amount of effort necessary to make the business function operational after the technology . element is recovered is known as:

a. Recovery Time Objective b. Work Recovery Time

c. Maximum Tolerable Downtime d. Recovery Point Objective

3. Contingency Planning includes:

a. Incident response plan b. Disaster recovery plan

c. Business continuity plan d. All the above

4. An investigation and assessment of the various adverse events that can affect the organization, conducted as a preliminary phase of the contingency planning process, which includes a determination of how critical a system or set of information is to the organization’s core processes and recovery priorities is known as:

a. Risk assessment b. Business impact analysis

c. Crisis management d. Incident damage assessment

5. The process that prepares an organization to reestablish or relocate critical business operations . during a disaster that affects operations at the primary site is known as:

a. Business continuity planning b. Disaster recovery planning

c. Strategic Planning d. Operational planning.

6. Which level of Organizational Planning typically addresses day-to-day activities and tasks?

a. Strategic Planning b. Tactical Planning

c. Operational Planning d. Top Management Planning

7. The job function of the Chief Information Security Officer includes:

a. Creating a strategic information security plan with a vision for the future of information security.

b. Understanding fundamental business activities performed by the company and suggesting appropriate information security solutions that uniquely protect these activities.

c. Improving the status of information security by developing action plans, schedules, budgets, status reports and top management communications

d. All the above

8. What is the unit of analysis in the contingency planning approach?

a. Business Assets b. Risk Assets

c. Business Processes d. Risk Factors

9. Which of the following is not a possible incident indicator?

a. Presence of unfamiliar files

b. Unusual consumption of computing resources

c. Unusual system crashes

d. Activities at unexpected times

10. What is the purpose of conducting an After Action Review (AAR) in incident response?

a. To review and improve the effectiveness of the DRP

b. To review and improve the effectiveness of the BCP

c. To review and improve the effectiveness of the IRP

d. To notify law enforcement agencies

**Week 5 Quiz**

1. The primary function of a cybersecurity policy within an organization is to:

a. Define a rigid set of penalties for security violations.

b. Eliminate the need for ongoing security awareness training programs.

c. Dictate specific technical security controls for implementation.

d. Establish a comprehensive reference point for organizational cybersecurity practices.

2 . Which type of policy is related to an organization's strategic purpose, mission, and vision?

a. Issue-specific information security policies (ISSP)

b. Systems-specific information security policies (SysSP)

c. Enterprise information security policy (EISP)

d. Technical implementation policy

3 . True or False: Standards are broad, abstract documents that provide detailed procedures for employees to comply with policies

1. True b. False

4. Which of the following reflects the hierarchical top-down order of information security policies?

a. Enterprise > Issue-Specific > Systems-Specific

b. Systems-Specific > Issue-Specific > Enterprise

c. Issue-Specific > Enterprise > Systems-Specific

d. All three policy types are independent and unconnected.

5. Which of the following components is typically included in the Enterprise Information Security . . Policy (EISP)?

a. Incident response procedures b. Statement of purpose

c. Software development guidelines d. Employee performance evaluations

6. True or False: Systems-specific security policies (SysSPs) can be separated into two general groups, managerial guidance SysSPs and technical specifications SysSPs

a. True b. False

7. \_\_\_\_\_\_\_\_\_\_\_ consists of details about user access and use permissions and privileges for an organizational asset or resource.

a. Access Control Lists b. Configuration rules

c. Authorized access and usage of equipment d. Authorization rules

8. True or False: Consequence-driven Cyber-informed Engineering (CCE) is a cyber defense concept that focuses on the lowest consequence events from an engineering perspective so that resourceconstrained organizations receive the greatest return on their security investments.

a. True b. False

9. \_\_\_\_\_\_\_\_\_ are nonmandatory recommendations the employee may use as a reference in complying with a policy.

a. Practices b. Procedures

c. Standards d. Guidelines

10. Creating "air gaps" to isolate critical systems is a cyber hygiene practice that focuses on:

a. Installing the latest security patches.

b. Strengthening user authentication.

c. Segmenting networks for improved security

d. Keeping complex passwords up-to-date.

**Week 6 Quiz**

1. A determination of the extent to which an organization’s information assets are exposed to risk is known as:

a. Risk identification b. Risk control

c. Risk assessment d. Risk Management

2. \_\_\_\_\_\_\_is the risk to information assets that remains even after current controls have been applied. . a. Risk appetite b. Residual risk

c. Inherent risk d. Contingency risk

3. Which of these is not a component of risk identification?

a. Plan & organize the process b. Classify, value, & prioritize assets

c. Specify asset vulnerabilities d. Determine loss frequency

4. The likelihood of an attack together with the attack frequency to determine the expected number of losses within a specified time range is known as:

a. Loss frequency b. Attack success probability

c. Loss magnitude d. Risk

5. \_\_\_\_\_\_\_is an information attack that involves searching through a target organization’s trash for sensitive information.

a. Shoulder surfing b. Network sniffing

c. Dumpster diving d. Watering hole attacks

6. Risk management in cyber security involves three key steps. These steps are:

a. Monitoring, auditing, and reporting.

b. Identifying risks, assessing risk, and controlling risks.

c. Training employees, patching vulnerabilities, and using firewalls.

d. Investigating incidents, recovering data, and learning lessons.

7. The "attack surface" in cyber security is a visualization tool that helps to understand:

a. The effectiveness of different security tools.

b. The relationship between various types of threats and the organization's assets.

c. The complexity of the organization's network infrastructure.

d. The cost of implementing different security controls.

8. During the Risk Identification phase, assets are classified into which of the following categories?

a. Financial assets, Intellectual property, and Human resources

b. Assets, Liabilities, and Equity

c. Tangible assets, Intangible assets, and Fixed assets

d. People, Procedures, Data and information, Software, Hardware, and Networking elements

9. Which formula accurately represents the calculation of risk in cyber security risk assessment?

a. Risk = Loss frequency + Loss magnitude

b. Risk = Loss frequency x Loss magnitude + Measurement Uncertainty

c. Risk = (% Risk Mitigated by Controls) / (Loss Frequency x Loss Magnitude)

d. Risk = Loss frequency - Loss magnitude + Measurement Uncertainty

10. You are a security analyst for a company that manages an online store with a customer database. Industry reports indicate a 10 percent chance of an attack this year, based on an estimate of one attack every 10 years. A successful attack could result in the theft of customer data. There is a 20% chance of the threat being able to materialize and achieve its objectives even in place of robust secure protection mechanisms. The customer database is most valued being an e-commerce company at 90 in a 1-100 scale. The IT department informed that 60% of the assets will be exposed after a successful attack. The estimation of measurements is 80% accurate. Calculate the risk associated to the asset with a potential SQL injection attack.

a. 3.756 b. 4.196

c. 3.276 d. 1.296

**Week 7 Quiz**

1. \_\_\_\_\_\_\_\_ is a comprehensive system comprising software, encryption techniques, protocols, legal arrangements, and third-party services that facilitate secure communication among users by utilizing digital certificates.

a. Registration authority b. Public key infrastructure

c. Digital signature d. Certificate authority

2. Which ring does the kernel, the core of the operating system, typically operate?

a. Ring 2 b. Ring 1

c. Ring 0 d. Ring 3

3. Which of the following statements is not true?

a. Hash functions are one-way.

b. It is possible to attach a message authentication code (MAC) to allow only specific recipients to access the message digest.

c. Hashing functions require the use of keys.

d. Hash functions are used in password verification systems to confirm the identity of the user

4. Which of the following is not related to defense against rainbow cracking?

a. Password hash salting b. key stretching

c. Key strengthening d. Private key encryption

5. Which of the following statements is/are correct?

a. TCP is a connection-oriented protocol, while UDP is connectionless.

b. TCP is comparatively faster than UDP.

c. TCP provides reliable data delivery, while UDP does not.

d. Both a and c.

6. Which of the following statements about Virtual Private Networks (VPN) are true?

a. A VPN is an encrypted connection over the Internet from a device to a network.

b. A VPN keeps the contents of the network messages hidden from observers who may . have access to public traffic.

c. A VPN protects its users by masking their IP address.

d. All the above.

7. Endpoint Detection and Response (EDR) solutions are primarily focused on:

a. Securing network perimeters and firewalls.

b. Protecting individual user devices from threats.

c. Monitoring and analyzing network traffic for malicious activity.

d. Providing vulnerability assessments for servers and applications.

8.Cryptojacking is a cyber attack that leverages a victim's computer resources for the attacker's financial gain. Which of the following best describes the attacker's activity in a cryptojacking attack?

a. Encrypting the victim's data and demanding a ransom payment.

b. Gaining unauthorized access to the victim's personal information for resale.

c. Silently using the victim's processing power to solve complex mathematical problems for . financial reward.

d. Disrupting the normal operation of the victim's system to cause inconvenience.

9. What kind of infrastructure Advanced Persistent Threat (APT) groups are typically known for targeting?

a. Personal computers of home users.

b. Critical infrastructure essential for national security (e.g., power grids, communication networks).

c. Public Wi-Fi networks at cafes or airports.

d. Outdated operating systems on personal devices of insignificant value

10. Which of the following is NOT one of the stages in the Intrusion Kill Chain framework? . . . a. Reconnaissance b. Exploitation

c. Cleanup d. Command and Control

**Week 8 Quiz**

1. The Cost-Benefit Analysis (CBA) formula for risk management decisions is given by:

a. CBA = ALE(prior) - ALE(post) – ACS

b. CBA = ALE(prior) - ALE(post) + ACS

c. CBA = ALE(prior) + ALE(post) – ACS

d. CBA = ALE(prior) + ALE(post) + ACS

2. In a cost-benefit analysis, \_\_\_\_\_\_\_\_\_ is the expected percentage of loss that would occur from a particular attack

a. Single Loss Expectancy b. Exposure Factor

c. Annualized Loss Expectancy d. None of the above

3. A \_\_\_\_\_\_ is a network security device that monitors traffic to or from a network and decides whether to allow or block specific traffic based on a defined set of security rules.

a. Intrusion Detection and Prevention System b. Router

c. Intrusion Detection System d. Firewall

4. What risk management approach aims to minimize the impact of losses resulting from an actual incident, disaster, or attack by implementing thorough contingency plans and preparations?

a. Mitigation risk control strategy b. Transference risk control strategy

c. Defense risk control strategy d. Termination risk control strategy

5. The product of the asset’s value and the exposure factor is known as:

a. Single Loss Expectancy b. Annualized Loss Expectancy (Prior)

c. Annualized Rate of Occurrence d. Annualized Loss Expectancy (Post)

6. Which of the following is not true?

a. Bit Stream ciphers encrypt data one bit at a time, while block ciphers encrypt data in fixed-. . . . size blocks.

b. Bit Stream Cipher is used for Data in Transit Encryption, whereas Block Cipher is used for . .. Data at Rest Encryption

c. Bit Stream Cipher can operate as a Block CIpher but Block Cipher cannot operate as a Bit .. .. Stream Cipher

b. Bit Stream ciphers are generally considered faster than block ciphers.

7. The False Acceptance Rate (FAR) in biometrics refers to:

a. The system mistakenly accepting an unauthorized user.

b. The system correctly rejecting an unauthorized user.

c. The time it takes for a system to identify a user.

d. The user's frustration with the authentication process.

8. The IAAA framework in the context of access control stands for?

a. Isolation, Authentication, Authorization, Availability

b. Identification, Authentication, Authorization, Accountability

c. Inspection, Authentication, Access, Authorization

d. Intrusion Detection, Analysis, Authorization, Administration

9. What is a significant challenge associated with symmetric key encryption?

a. Slower encryption and decryption compared to asymmetric methods.

b. Limited compatibility with modern encryption algorithms.

c. Higher computational cost for key generation.

d. Key management: securely distributing and safeguarding the shared key.

10. In risk management, which equation is used to calculate the expected loss per risk?

a. Single Loss Expectancy (SLE) = Asset Value × Exposure Factor (EF)

b. Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualized Rate of ….. Occurrence (ARO)

c. Asset Value = Single Loss Expectancy (SLE) × Exposure Factor (EF)

d. Annualized Rate of Occurrence (ARO) = Asset Value × Single Loss Expectancy (SLE)

**Week 9 Quiz**

1. Which of the following is not true about Blockchains?

a. Blockchain ensures confidentiality through encryption.

b. Blockchain ensures integrity through hashing.

c. Properties such as hiding, and collision resistance help blockchains make transactions . permanent.

d. Blockchains are implemented as queues.

1. What is the block size and key size of the Data Encryption Standard (DES)?

a. Block size: 64 bits, key size: 56 bits

b. Block size: 56 bits, key size: 64 bits

 c. Block size: 64 bits, key size: 64 bits

 d. Block size: 56 bits, key size: 56 bits

1. What is the purpose of the cryptography in the RSA algorithm?

a. To encrypt messages using a public key and decrypt them using a private key

b. To encrypt messages using a private key and decrypt them using a public key

c. To generate a random key for encrypting messages

d. To securely transmit keys over an insecure network

1. What is the term used to describe the concept where customers or partners can be held accountable for transactions, such as online purchases, which they cannot later dispute?

a. Unquestionability

b.  Nonreversal

c. Nonrepudiation

d. Indisputability

1. In the context of information security, what distinguishes Personally Identifiable Information (PII) from other data?

a. Its susceptibility to malware attacks.

b. Its encryption level for secure transmission.

c. Its uniqueness or proximity to a specific individual.

d. Its accessibility through public databases.

1. Who is considered the "Father of Modern Day Information Privacy"

a. Alan Westin

b. Alan Turing

c. Louis Brandeis

d. Samuel Warren

1. What is the core principle of informational privacy?

a. The right to remain anonymous at all times.

b. The complete elimination of all personal data collection.

c. The responsibility of companies to prioritize profits over user privacy.

 d. The ability of individuals to decide what personal information they share and with whom.

1. The FIPPs were first introduced in a report by:
2. The Federal Trade Commission (FTC)
3. The European Union
4. The US Secretary's Advisory Committee on Automated Personal Data Systems.
5. A private industry consortium
6. Which of the following aspects of data privacy is NOT explicitly addressed in the FIPP?
7. The right to be forgotten

b. The ability to access and correct personal data.

c. The requirement for secret personal data record-keeping systems.

d.The need for individual consent for data collection.

1. Which of the following statements BEST reflects the "reductionist" view?

a. Privacy is a fundamental right, independent of other rights.

b. Privacy is seen as a derivative right, stemming from other fundamental rights like property . or bodily security.

c. There is no such thing as privacy; it's an outdated concept

 d. Privacy is crucial for economic efficiency.

**Week 10 Quiz**

1. Privacy Paradox is:

a. The discrepancy between the expressed concern and the actual behavior of users when it comes to privacy in an online environment.

 b.The balance between privacy protection and data sharing in online environments.

c.The phenomenon where individuals prioritize convenience over privacy

d.The psychological phenomenon where individuals are unaware of the impact of their online behavior on their privacy

1. Which of the following is not an approach to pseudonymization?

a. Masking

 b.Tokenization

 c. Hashing

d.None of the above

1. Which of the statements about pseudonymization is not true?

a. Pseudonymization is a technique proposed by frameworks like Privacy by Design offering practical substitutes for using the raw data, especially when this data is sensitive.

b. Various pseudonymization techniques enable you to preserve format or understand the original intention for that data

c. Pseudonymization methods often maintain the capability to establish connections between data, which proves beneficial when linking datasets using personal identifiers or other sensitive columns.

d. None of the above

1. Externalization of restricted, but accurate information to a specific entity is known as:

a. Anonymity

b. Secrecy

 c. Confidentiality

d.Security

1. Differential privacy is:

a. A method of probabilistically limiting the amount of information an attacker can gain when data is released.

  b. A method for measuring and monitoring the loss of privacy experienced by an individual in a dataset that has been released.

  c. One of the most effective methods for providing individuals in a dataset with plausible deniability while still performing data analysis

1. All the above
2. Which regulatory framework evolved into the General Data Protection Regulation (GDPR) in 2018?
3. FTC privacy principles
4. APEC privacy framework
5. OECD Guidelines
6. EU Data Protection Direct
7. In the context of privacy, what does the acronym "FIPP" stand for?

a. Freedom of Information Processing Practices

b. Fair Information Practice Principles

 c. Federal Internet Privacy Protections

d.Financial Information Protection Protocols

1. Which of the following statements is true?
2. Quasi Identifiers are more valuable for targeted advertising than Identifiers
3. Identifiers are always anonymized, whereas Quasi-Identifiers are non-anonymized.
4. Identifiers are not considered personal data whereas Quasi Identifiers are.
5. Identifiers can uniquely identify an individual, while quasi-identifiers cannot on their own.
6. What are the two techniques used in k-anonymization?

a. Randomization and suppression

b. Generalization and encryption

  c. Suppression and generalization

d.Suppression and encryption

1. What does the optimal point on an R-U map represent?

a. Complete elimination of all data privacy risks,by fully anonymizing all data

b. Utilizing all PIIs data, extracting full value without privacy concerns

c. Maximizing data usefulness while maintaining acceptable privacy risks.

d. None of the above

**Week 11 Quiz**

1. When does the General Data Protection Regulation (GDPR) apply?

a. A company processes personal data and is based in the EU, regardless of where the actual data processing takes place

 b. Company is established outside the EU but processes personal data in relation to the offering of goods or services to individuals in the EU, or monitors the behaviour of individuals within the EUC

  c. Both A and B

d.None of the above

1. True or False: When personal data is transferred outside the EU, the protection offered by the GDPR need not travel with the data.

a. True b. False

1. The Information Technology (IT) Act in India was first enacted by the Indian Parliament in the year:

a. 2007 b. 2004

c. 2000 d. 2000

4. Privacy is a fundamental right in India

a.True b. False

5.Which of the following rights does the DPDP Act grant to data principals for the personal . .. data they have previously given consent?

a. Right to correct

b. Right to complete and update

c.Right to erasure

d.All the above

6. When was GDPR enforced?

 a. April 27, 2016 b. May 25, 2018

c.June 30, 2017 c. July 1, 2019

7.Which legal basis for processing personal data applies when someone's life is in . .. … danger, and the processing is necessary to save it?

a. Consent b. Vital interests

c. Contract c. Public interest

8. Within how many hours does GDPR require organizations to report cyber incidents?

a. 48 hours b. 72 hours

c. 96 hours d.120 hours

9. As per GDPR , when should an organization appoint a Data Protection Officer (DPO)?

a. Only when organizations are located within the EU.

b. Only when organizations handle sensitive personal data.

c. A DPO is not mandatory for any organization

d. When there is significant processing of personal data, sensitive data on a large scale

10.True or False: Indian Telegraph Act 1885 did not provide interceptive powers to the . .. government.

a. True b. False

**Week 12 Quiz**

1. Why is understanding the value that individuals assign to the protection of their personal data important for businesses?
2. To enable businesses to use personal data for maximum commercial gain
3. b.To help businesses develop privacy-enhancing initiatives that can provide a competitive advantage
4. To allow businesses to mandate strict data collection and usage policies without considering consumer preferences
5. To facilitate the creation of personal data trading markets where individuals can monetize their information
6. Which of the following is true?

a. Privacy valuation is consistent across all individuals and contexts

  b. Privacy valuation is influenced by external factors and remains stable over time

c.Privacy valuation can differ based on the specific context and circumstances

 d. Privacy valuation is solely determined by economic factors and market trends

1. What is the core idea behind the privacy calculus?

a. Individuals make irrational decisions about sharing personal information

b. Individuals engage in a cost-benefit analysis to decide whether to disclose personal data

 c. Individuals do not have any control over the disclosure of their personal information

d.Individuals are solely motivated by the potential benefits of data sharing

4.True or False: Willingness to accept tends to produce privacy valuations that are . .. .. … …. substantially lower than those produced by Willingness to pay.

 a. True b. False

5. Which design approach is best recommended to address privacy concerns with digital . contact tracing applications?

 a. Implement a centralized architecture where all contact tracing data is stored and . ….. processed by a single authority

b. Develop a decentralized, privacy-preserving architecture that minimizes the sharing . .. of personal data

c. Prioritize public health benefits over individual privacy protections in the design of . .. … contact tracing systems

 d. Require mandatory participation in contact tracing programs to maximize the . … ….. ………… effectiveness of the technology

6. What does Prospect Theory suggest about how people perceive gains and losses?

 a. People value all gains and losses equally.

b. Individuals are more likely to take risks for potential gains.

  c. Losses are typically felt more intensely than gains.

d. People only care about maximizing their financial gains

7. Which of the following is/are considered recommended practices to protect privacy in AI . systems?

a. Collect and handle data responsibly

b. Leverage on-device processing where appropriate

c. Appropriately safeguard data privacy inML models

d. All the above

8. AI systems must comply with privacy laws such as the GDPR, such that: (1) it requires . transparency about the collection, use, and storage of data. (2) it mandates that .. …. …….. consumers have appropriate controls to choose how their data is used.

  a. Only (1) is True b. Only (2) is True

c. (1) and (2) are True d. (1) and (2) are False

9**. ‘**Ajay’ enters into a contract with ‘Bijoy’ to provide a service ‘ABC’ to ‘Bijoy’. As part of the . contract, ‘Bijoy’ consents to processing of his personal data by ‘Ajay’. If ‘Bijoy’ withdraws . his consent to processing of his personal data, ‘Ajay’ may stop offering the service ‘ABC’ . to ‘Bijoy’. As per the Digital Personal Data Protection Bill, 2022, Bijoy is the \_\_\_\_\_\_\_\_\_\_\_.

a. Data Principal

  b. Data Processor

 c. Data Fiduciary

d. Data Protection Officer

10. What does Prospect Theory suggest about how people perceive gains and losses?

. a. People value all gains and losses equally.

  b. Individuals are more likely to take risks for potential gains.

  c. Losses are typically felt more intensely than gains.

  d. People only care about maximizing their financial gains