CIPT$^{\text{Q\&As}}$

Certified Information Privacy Technologist (CIPT)

QUESTION 1

An organization is launching a new online subscription-based publication. As the service is not aimed at children, users are asked for their date of birth as part of the of the sign-up process. The privacy technologist suggests it may be more appropriate ask if an individual is over 18 rather than requiring they provide a date of birth. What kind of threat is the privacy technologist concerned about?

A. Identification.

B. Insecurity.

C. Interference.

D. Minimization.

Correct Answer: D

By suggesting that it may be more appropriate to ask if an individual is over 18 rather than requiring they provide a date of birth, the privacy technologist is concerned about minimizing the amount of personal data collected. This helps reduce privacy risks by limiting the amount of personal data that could potentially be exposed in a data breach.

QUESTION 2

A jurisdiction requiring an organization to place a link on the website that allows a consumer to opt-out of sharing is an example of what type of requirement?

A. Functional

B. Procedural

C. Operational

D. Technical

Correct Answer: D

QUESTION 3

Properly configured databases and well-written website codes are the best protection against what online threat?

A. Pharming.

B. SQL injection.

C. Malware execution.

D. System modification.

Correct Answer: B

Properly configured databases and well-written website code are essential protections against SQL injection attacks.

SQL injection occurs when an attacker exploits a security vulnerability arising from improper input validation in code for web applications that interact with databases. By injecting malicious SQL statements into an entry field for execution, an attacker can read, modify, or delete data that they are not normally able to access. Ensuring that database queries are securely written and that databases are configured to reject malicious inputs is critical to defending against this type of security threat.

QUESTION 4

To comply with the Sarbanes-Oxley Act (SOX), public companies in the United States are required to annually report on the effectiveness of the auditing controls of their financial reporting systems. These controls must be implemented to prevent unauthorized use, disclosure, modification, and damage or loss of financial data.

Why do these controls ensure both the privacy and security of data?

A. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.

B. Unauthorized use of data is an aspect of privacy; disclosure, modification, and damage or loss of data are aspects of security.

C. Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security.

D. Damage or loss of data are aspects of privacy; disclosure, unauthorized use, and modification of data are aspects of privacy.

Correct Answer: C

QUESTION 5

Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo\\'s Harm Dimensions?

A. Financial loss and blackmail.

B. Financial loss and solicitation.

C. Identity theft and embarrassment.

D. Identity theft and the leaking of information.

Correct Answer: C

Extracts from The boundaries of privacy harms: "Objective harms can also occur when such information is used to commit a crime, such as identity theft or murder."; "The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states--anxiety, for instance, or embarrassment--that accompany the belief that one is or will be watched or monitored. "