CIPT$^{Q\&As}$

Certified Information Privacy Technologist (CIPT)

Pass IAPP CIPT Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cipt.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

QUESTION 1

Which is NOT a suitable method for assuring the quality of data collected by a third-party company?

A. Verifying the accuracy of the data by contacting users.

B. Validating the company\\'s data collection procedures.

C. Introducing erroneous data to see if its detected.

D. Tracking changes to data through auditing.

Correct Answer: C

Introducing erroneous data to see if it\\'s detected is not a suitable method for assuring the quality of data collected by a third-party company1. This method could compromise the integrity and reliability of the data and cause confusion or harm to the users or the business1. The other options are suitable methods for assuring the quality of data collected by a third-party company1. Verifying the accuracy of the data by contacting users can help identify and correct any errors or inconsistencies in the data1. Validating the company\\'s data collection procedures can help ensure that they follow best practices and standards for collecting, storing, and processing personal information1. Tracking changes to data through auditing can help monitor and document any modifications or deletions made to the data1.

https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach

QUESTION 2

All of the following can be indications of a ransomware attack EXCEPT?

A. The inability to access certain files.

B. An increased amount of spam email in an individual\\'s inbox.

C. An increase in activity of the CPU of a computer for no apparent reason.

D. The detection of suspicious network communications between the ransomware and the attacker\\'s command and control servers.

Correct Answer: B

QUESTION 3

Between November 30th and December 2nd, 2013, cybercriminals successfully infected the credit card payment systems and bypassed security controls of a United States-based retailer with malware that exfiltrated 40 million credit card numbers. Six months prior, the retailer had malware detection software installed to prevent against such an attack.

Which of the following would best explain why the retailer\\'s consumer data was still exfiltrated?

A. The detection software alerted the retailer\\'s security operations center per protocol, but the information security personnel failed to act upon the alerts.

B. The U.S Department of Justice informed the retailer of the security breach on Dec. 12th, but the retailer took three days to confirm the breach and eradicate the malware.

C. The IT systems and security measures utilized by the retailer\\'s third-party vendors were in compliance with industry standards, but their credentials were stolen by black hat hackers who then entered the retailer\\'s system.

D. The retailer\\'s network that transferred personal data and customer payments was separate from the rest of the corporate network, but the malware code was disguised with the name of software that is supposed to protect this information.

Correct Answer: B

QUESTION 4

Which of the following can be used to bypass even the best physical and logical security mechanisms to gain access to a system?

A. Phishing emails.

B. Denial of service.

C. Brute-force attacks.

D. Social engineering.

Correct Answer: D

social engineering can be used to bypass even the best physical and logical security mechanisms to gain access to a system. Social engineering involves manipulating individuals into revealing sensitive information or performing actions that compromise security.

QUESTION 5

Which of the following methods does NOT contribute to keeping the data confidential?

A. Differential privacy.

B. Homomorphic encryption.

C. K-anonymity.

D. Referential integrity.

Correct Answer: D

referential integrity does not contribute to keeping the data confidential.