Certified in Risk and Information Systems Control™
An ISACA® Certification

The following correction applies to page 162 of the *CRISC® Review Questions, Answers & Explanations Manual 5th Edition*. The correction is boxed.

R3-66 Which of the following **BEST** protects the confidentiality of data being transmitted over a network?

A. Data are encapsulated in data packets with authentication headers.
B. A digital hash is appended to all messages sent over the network.
C. Network devices are hardened in compliance with corporate standards.
D. Fiber-optic cables are used instead of copper cables.

D is the correct answer.

Justification:
A. The authentication header protocol does not contribute to data confidentiality.
B. A digital hash appended to the messages will only ensure data integrity.
C. Network device hardening will only protect data at the end points and not during transmission.
D. While data can be extracted from fiber-optic cable via tapping, it is considered more reliable than copper cable. Detection of a breach is also readily identified with fiber-optic cables.

R3-67 During which phase of an incident response process should an attempt be made to limit the impact of an incident?

A. Mitigation
B. Recovery
C. Response
D. Detection

C is the correct answer.

Justification:
A. Mitigation involves remediation of the event. An attempt to limit the impact should be made earlier during response.
B. The recovery phase includes a full repair of the incident.
C. During the response phase, attempts can made to limit the impact of an incident because the occurrence is ongoing; depending upon the nature of the incident, the time following initial identification can present opportunities to intervene and limit severity.
D. Detection aims to identify an incident and determine its cause.

R3-68 Which of the following is the **MOST** important consideration when developing a record retention policy?

A. Delete, as quickly as practical, all data that are not required.
B. Retain data only as long as necessary for business or regulatory requirements.
C. Keep data to ensure future availability.
D. Archive old data without encryption as quickly as practical.

B is the correct answer.

Justification:
A. Deleting superfluous data is a process that may be called for by the policy. It is not a consideration when developing a records retention policy.
B. Good practice states that data should be kept only as long as required by business or regulation requirements.
C. It is better not to keep any data longer than necessary because the loss of old data may still pose a serious risk to the enterprise.
D. Old data should still be encrypted (and perhaps reencrypted with a stronger algorithm) if they are being retained by the enterprise.

ISACA®
Trust in, and value from, information systems