RC0-C02^Q&As

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

QUESTION 1

Which of the following must be taken into consideration for e-discovery purposes when a legal case is first presented to a company?

A. Data ownership on all files

B. Data size on physical disks

C. Data retention policies on only file servers

D. Data recovery and storage

Correct Answer: D

QUESTION 2

An information security assessor for an organization finished an assessment that identified critical issues with the human resource new employee management software application. The assessor submitted the report to senior management but nothing has happened. Which of the following would be a logical next step?

A. Meet the two key VPs and request a signature on the original assessment.

B. Include specific case studies from other organizations in an updated report.

C. Schedule a meeting with key human resource application stakeholders.

D. Craft an RFP to begin finding a new human resource application.

Correct Answer: C

You have submitted the report to senior management. It could be that the senior management are not that bothered about the HR application or they are just too busy to respond.

This question is asking for the logical next step. The next step should be to inform people that are interested in the HR application about your findings. To ensure that the key human resource application stakeholders fully understand the

implications of your findings, you should arrange a face-to-face meeting to discuss your report.

QUESTION 3

The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO\\'s budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.

B. The company should transfer the risk.

C. The company should avoid the risk.

D. The company should accept the risk.

Correct Answer: B

To transfer the risk is to deflect it to a third party, by taking out insurance for example.

QUESTION 4

The internal audit department is investigating a possible breach of security. One of the auditors is sent to interview the following employees:

Employee A: Works in the accounts receivable office and is in charge of entering data into the finance system.

Employee B: Works in the accounts payable office and is in charge of approving purchase orders.

Employee C: Is the manager of the finance department, supervises Employee A and Employee B, and can perform the functions of both Employee A and Employee B.

Which of the following should the auditor suggest be done to avoid future security breaches?

A. All employees should have the same access level to be able to check on each others.

B. The manager should only be able to review the data and approve purchase orders.

C. Employee A and Employee B should rotate jobs at a set interval and cross-train.

D. The manager should be able to both enter and approve information.

Correct Answer: B

QUESTION 5

The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year\\'s growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.

B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.

C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.

D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Correct Answer: B

Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field.