Fundamental Concepts of Data Security
ISEC2001

Business Continuity III

Question 1

Explain the difference between two BCP tests: Structured Walk-Through Test vs Simulation Test.

Question 2

It is advised that records of important events need to be maintained/documented. What should be done to the records afterwards?

Question 3

It is recommended that BCP maintenance is important for an organisation to respond well in a critical event. Give four (4) situations when an update of BCP is needed.

Question 4

What is a computer security incident? Give three (3) examples of computer security incidents that compromise Availability, Confidentiality, and Integrity.

Question 5

A director of an organisation has accidentally clicked on the attachment of a phishing email and hence the computer is now infected with the latest virus not yet recognized by the existing anti-virus programs. Soon after clicking the attachment, the director has suspected that email and its attachment. If a proper security incident response to this type of attack exists, discuss what would be an appropriate response procedure?

Question 6

One important stage in an incident response plan is Containment. Explain the purpose of this stage and give two (2) examples of the action taken in this stage.

Question 7

Handling security incidents is often recommended a coordinated response. Explain what it means by “coordinated”. Who are the persons involved in the response procedure?

Question 8

Once an incident has been contained/eradicated and the system has been successfully recovered, what is the next important step in security incident handling? What does it involve?