**8 Question 1**

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

**Structured Walkthrough test**

* In this test, the rep from each dept or functional area come tgt and go over the plan to ensure its accuracy.
* The group reviews the objective of the plan, discusses the scope and functions of the plan, reviews the organisation and reporting structure
* Evaluates the testing, maintenance and training requirements described
* This gives the people responsible for making sure disaster recovery happens effectively and efficiently a chance to review what has been decided upon and what is expected of them.
* The group walks through different scenarios from beginning to end to make sure nothing is left out.
* This also raises the awareness of team members about the recovery processes

**Simulation Test**

* Needs a lot more planning and people
* In this situation, all employees participate in operational and support functions or their representatives come together to practise executing the disaster recovery plan based on a specific scenario.
* This scenario is used to test the reaction of each operational and support representative.
* This is done to ensure specific steps were not left out and that certain threats are not overlooked.
* It raises the awareness of people involved
* The drill includes only those materials available in an actual disaster to portray a more realistic environment
* (The simulation test continues up to the point of actual relocation to an offsite facility and actual shipment of replacement equipment.)
* The drill includes only those materials that will be available in an actual disaster to portray a more realistic environment. The simulation test continues up to the point of actual relocation to an offsite facility and actual shipment of replacement equipment.

**Question 2**

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

**Reporting to management**

When recovery procedures are carried out, the outcome of those procedures should be reported to individuals who are responsible for this type of activity which is usually some level of management. If the procedures work properly, management should know of it. If problems are encountered, management should definitely be aware of them. Members of management are the ones who are responsible overall for fixing the recovery system and will be the ones who delegate this work and provide the necessary funding and resources.

**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.

**<choose four from the list>**

• The business continuity process is not integrated into the change management process.

• Changes occur to the infrastructure and environment.

• Reorganization of the company, layoffs, or mergers occur.

• Changes in hardware, software, and applications occur.

• After the plan is constructed, people feel their job is done.

• Personnel turn over.

• Large plans take a lot of work to maintain.

• Plans do not have a direct line to profitability.

**Question 4**

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

**Definition**

An unauthorised or unlawful action involving a security system

**Availability**

A ddos attack that could cause a server to hang thus affecting the availability of the system

**Confidentiality**

Hackers hacking into a system and stealing information.

Password cracking

**Integrity**

Employees accidentally deleting or amending information of company

Ransomware

DNS

DNS

A DNS Attack is any attack targeting the availability or stability of a network’s DNS service. Attacks that leverage DNS as its mechanism as part of its overall attack strategy, such as cache poisoning, are also considered DNS attacks.

A Domain Name System (DNS) attack is one in which a bad actor either tries to compromise a network’s DNS or takes advantage of its inherent attributes to conduct a broader attack. A well-orchestrated DNS attack can bring an organization to its knees.

**DoS, DDoS, and DNS amplification attacks**

Denial-of-service (DoS) attacks and distributed-denial-of-service (DDoS) attacks are two forms of the same thing. They’re what most people think of when they think of a DNS attack. In both cases, attackers flood internet servers with so many requests that they simply can’t answer them all, and the system crashes as a result.

**Question 5 (Needs more research on this type of question)**

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?

**Steps**

1. Disconnect the machine from the network to prevent spreading of the virus to other machines
2. Call IT support, note down information abt the computer after clicking the attachment, the it team may bring the machine to an isolated location and perform investigation
3. Remove the virus. Recover the data. Document the incident
4. Inform the anti-virus company to update the latest signatures. Or call in the police thereafter if it is attributed to criminal activity in the company.

**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.

**Definition**

Purpose: minimise any further damage caused by an incident by preventing it from spreading out and retainment of the machine at a stage for forensics or legal proceedings.

**Example**

* A server being attacked or infected by malware is taken off the network to prevent the spreading of the malware to other machines.
* When a machine is under attack, the firewall configurations are changed to block the traffic from the attacker's machine to the machine under attack.

**Question 7 (Analyse the way this question has been answered)**

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

Planning is prepared, incident response team is involved

**Definition**

* An incident response team should be available for anyone who discovers or suspects an incident involving the organisation has occurred.
* One or more team members depending on the magnitude of the incident and availability of personnel will then handle the incident. These incident handlers then analyse the incident data, determine the impact of the incident and act appropriately to limit the damage and restore normal services.
* The incident response team’s success depends on the participation and the cooperation of individuals throughout the organisations.

**Possible structure for an incident response team can include the following:**

1. Firstly, have a central incidence response team.

* This is a single incident response team that handles incidents throughout the organisation. (Definition)
* This model is effective for small organisations and organisations with minimum geographic diversity in terms of computing resources. (Effective for)

1. Distributed incident response team containing multiple incident response teams each responsible for a particular logical or physical segment of the organisation.

* This model is very suitable for large organisations and for organisations with major computing resources and distant locations.
* Eg. One team per division. One team per geographic region, one team per major facility.
* However, the teams should be part of a single coordinated entity so that the incident response process is consistent across the organisation and information is shared among teams.
* This is particularly important as multiple teams may see components of the same incident or may handle similar incidents.

1. Having a coordinating team

* This is an incident response team that provides advice to other teams without having authorities over those teams.
* For eg. a department wide team may assist individual agencies teams.

**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?

Post-incident review and activity which includes:

* Lessons learnt : What teams learn from the incidents so that they will not repeat any mistakes and know how to react when such an incident occurs again.
* Using collected incident data and evidence retention.