kasneb

**CICT PART III SECTION 6**

**SYSTEMS SECURITY**

**THURSDAY: 29 November 2018.** **Time Allowed: 3 hours.**

**Answer ALL questions. Marks allocated to each question are shown at the end of the question.**

**QUESTION ONE**

(a) Discuss five requirements of an effective information systems security policy. (5 marks)

(b) While systems security has remained a critical operation, the continued application of technology in businesses has necessitated greater emphasis on the same.

Examine four business engagements in which security is vital. (4 marks)

(c) ABC Limited intends to set up a central server that will be remotely accessed by the staff and customers to transact their business. The company has approached you to advise on a strategy that would ensure secure transactions across its network.

**Required:**
Assess four critical areas that you need to consider in order to secure the transactions. (4 marks)

(d) Discuss five steps that are required to determine the Business Impact Assessment (BIA) in an organisation. (5 marks)

(e) Differentiate between "fault-tolerant computer systems (FTCs)" and "high availability computing (HAC)". (2 marks)
**(Total: 20 marks)**

**QUESTION TWO**

(a) (i) Threats to information systems include ransomware.

With reference to the above statement, explain how ransomware attacks a system. (2 marks)

(ii) Propose six strategies for preventing ransomware attacks. (6 marks)

(b) Describe four types of firewall implementation techniques for data transmission protection. (4 marks)

(c) Summarise four forms of technical controls that might be instituted within a LAN network environment. (4 marks)

(d) Assess four technological trends that have heightened ethical concerns with regard to security. (4 marks)
**(Total: 20 marks)**

**QUESTION THREE**

(a) ABC Ltd. engages purely in an e-commerce mode of carrying out business transactions. The company has a central server at its headquarters located in Nairobi city. The server connects to a remote work station country wide via internet infrastructure.

**Required:**
Discuss three passive attacks that could be used to gather information on the above network infrastructure indicating the possible points of attack. (6 marks)

(b) Citing an example in each case, distinguish between "security policy" and "security mechanism". (4 marks)

(c) Hybrid encryption could be used to provide a better method of encryption.

Use an illustration to describe hybrid encryption model. (4 marks)

(d) A typical best practice network server protection mechanism used by organisations is a reverse proxy setup.

(i) Describe the role of a reverse proxy. (2 marks)

(ii) Outline the reverse proxy protection process. (4 marks)

**(Total: 20 marks)**

**QUESTION FOUR**

(a) Several circumstances exist when human error results into exposures to threats for information systems.

Examine four human errors that expose information systems to threats. (4 marks)

(b) Using a typical business illustration, describe dirty data in the context of data migration projects. (2 marks)

(c) Propose five ways of enhancing security of mobile devices. (5 marks)

(d) Software problem discovery leads to rapid effort to "patch" the system to repair or restore security. Patches may however, make the system less secure rather than more secure.

Argue four reasons to support the above statement. (4 marks)

(e) The most common use of digital certificate is to verify that a user sending a message is who he claims to be and to provide the receiver with the means to encode a reply.

Illustrate the structure of a digital certificate. (5 marks)

**(Total: 20 marks)**

**QUESTION FIVE**

(a) An organisation requires to resume operations after a system failure that has affected two of their core servers. Due to the size of data to be backed up, the organisation had adopted the incremental backup on one server and the differential backup on the second server.

**Required:**

Discuss the two types of backup and the approach that should be used for the restoration of the two servers. (6 marks)

(b) XYZ Bank has noticed a denial of service (DOS) attack that has affected access to their servers. Having consulted you, it was discovered that the communication session could not be established by the TCP/IP.

**Required:**

(i) Discuss the type of attack that is most likely to have occurred to cause the denial of service and how this session would be established in a normal communication. (3 marks)

(ii) Describe a countermeasure that could be used to mitigate this problem. (2 marks)

(c) An organisation has invited you to conduct ethical hacking in their institution. Describe the first step that you should undertake in this process and state its importance. (3 marks)

(d) Many countries are facing challenges in arresting and convicting ICT criminals.

Outline three ways in which computer forensics could be used to enforce law in a country. (3 marks)

(e) Organisations have various reasons for promoting a work environment in which employees are encouraged to act ethically when making business decisions.

Highlight three reasons why fostering good business ethics is important. (3 marks)

**(Total: 20 marks)**

.....