KASNEB

CICT PART III SECTION 6

SYSTEMS SECURITY

PILOT PAPER

September 2015. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Classified information is material that a government body could claim is sensitive information that requires protection. Documents and other information assets are typically marked with one of several levels of sensitivity.

Required:
Explain four general classifications of information sensitivity. (8 marks)

(b) Describe the following terms:

(i) Trojan horses. (2 marks)

(ii) Dirty data. (2 marks)

(iii) Civil strife. (2 marks)

(iv) Vandalism. (2 marks)

(c) Draw a diagram illustrating the triad security objectives. (4 marks)
(Total: 20 marks)

QUESTION TWO

(a) A college uses virtualisation technology to deploy information security courses. Some laboratory exercises involve studying the characteristics of computer viruses and worms.

Required:
Appraise the use of virtualised environment as opposed to using actual personal computers. (8 marks)

(b) Buffer overflow is an attack method where a program will overrun buffers memory boundary and overwrite adjacent memory location for an attacker.

Required:
Analyse four controls that can be put in place to avoid buffer overflow. (8 marks)

(c) Citing a suitable example, explain the term "network spoofing". (4 marks)
(Total: 20 marks)

QUESTION THREE

(a) Distinguish between the following terms:

(i) Differential and incremental backups. (2 marks)

(ii) Cloud backup and local backup. (2 marks)

(iii) Cold site and hot site. (2 marks)

(b) Highlight four ways a firewall can be used to enhance transmission security. (4 marks)

(c) E-commerce is a buying and selling activity conducted via internet and thus requires security to avoid fraud.

Explain five ways in which you could avoid fraud in e-commerce transactions. (10 marks)
(Total: 20 marks)

QUESTION FOUR

(a) Intellectual properties require great controls to protect the ownership of the property.

Explain the following terms in relation to intellectual property:

(i) Copyright. (2 marks)

(ii) Patent right. (2 marks)

(b) Computer forensics is a branch of digital forensics that deals with evidence found in computers and digital storage media.

Explain five ways an organisation can apply computer forensics in various cases. (10 marks)

(c) Explain three main stages used in risk analysis process. (6 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Explain the following security control methods:

(i) Private key cryptography. (3 marks)

(ii) Public key cryptography. (3 marks)

(b) Most business personnel have opted to use mobile devices to conduct their businesses online. However, mobile devices such as smart phones are also faced with security challenges.

Examine three mobile malwares that pose threats to smart phones. (6 marks)

(c) Systems security policy in an organisation is crucial and is regarded as the backbone of the ICT infrastructure and usage.

Required:
Explain the importance of security policy in an organisation. (6 marks)

(d) Describe a Greyhat hacker. (2 marks)

(Total: 20 marks)

.....