b:empowered

kasneb

CICT PART III SECTION 6

SYSTEMS SECURITY

THURSDAY: 30 November 2017. **Time Allowed: 3 hours.**

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

QUESTION ONE

(a) Distinguish between "shoulder surfing" and "pretexting" in the context of systems security. (2 marks)

(b) Most business organisations are cutting communication costs by eliminating paper based communication and embracing on instant messaging.

Highlight four security goals in using instant messaging. (4 marks)

(c) Assess five guidelines that should apply to the content of a successful system security policy. (5 marks)

(d) XYZ Ltd. is a company dealing with the transfer and maintenance of public critical files. The company wishes to recruit an incident response team to be dealing with incidents using digital tools.

Analyse five paramount skills that the recruits should possess. (5 marks)

(e) ABC Ltd. is a growing institution which is in the process of embracing information technology (IT) governance.

Required:
Citing four reasons, justify why ABC Ltd. needs to establish a systems control and security policy. (4 marks)
(Total: 20 marks)

QUESTION TWO

(a) Information needs to be identified, labelled and handled in accordance with the assigned security classification.

Citing four reasons, justify the importance of information classification. (4 marks)

(b) Ms Aoko, a company employee was involved in a social engineering attack while telecommuting.

Required:
(i) Propose two precautions that Ms Aoko should take upon realisation of the attack. (2 marks)

(ii) Evaluate four common social engineering attacks that Ms Aoko could have fallen victim to. (4 marks)

(c) Identify three tips that could aid in hardening the security of an access point in an organisation. (3 marks)

(d) (i) Control Objectives for Information and Related Technologies (COBIT) and International Organisation for Standardisation (ISO) are the main stakeholders involved in ICT related risks.

Analyse four factors in an organisation that affect the development of a successful ICT risk management framework. (4 marks)

(ii) Summarise three aspects of risk management in relation to the protection of data and resources in an enterprise. (3 marks)
(Total: 20 marks)

QUESTION THREE

(a) Describe five events that could be audited through system security log. (5 marks)

(b) Differentiate between "data integrity" and "systems integrity" within a network security context. (4 marks)

(c) Input processing requires that controls be identified to verify that data is accepted into the system correctly and that the input errors are recognised and corrected. These errors could in turn greatly impact the completeness and accuracy of the data.

Required:
Analyse four error correction procedures that could be instituted to guarantee the correctness of data. (4 marks)

(d) Identify four hardware tactics of controlling computer viruses in an organisation. (4 marks)

(e) Assess three professional dilemmas that face ICT employees. (3 marks)

(Total: 20 marks)

QUESTION FOUR

(a) Discuss two important "rules of evidence" that are used in computer forensics. (4 marks)

(b) Outline two vulnerabilities and two attacks that are likely to occur at the operating system level. (4 marks)

(c) Enumerate four guidelines that would ensure a secure mobile platform. (4 marks)

(d) To trust any program, we rely on rigorous analysis and testing.

Explain four key characteristics that must be considered during analysis and testing process of a program. (4 marks)

(e) Describe two security goals that make the secure socket layer (SSL) to be preferred in e-commerce. (4 marks)

(Total: 20 marks)

QUESTION FIVE

(a) Explain the main protection areas and the associated security threats of the first layer of defence-in-depth. (2 marks)

(b) Using a simple sketch, show how you would place a router, IDS, firewall, and DMZ in a corporate network in order to secure the resources of an organisation. (5 marks)

(c) Highlight five security threats that affect cloud computing. (5 marks)

(d) A company intends to construct a data centre and you are required to install the fire detection and suppression facilities.

Required:
Describe four facilities that you need to install in the data centre. (4 marks)

(e) Citing corresponding types of viruses, examine four types of techniques that viruses use to escape detection. (4 marks)

(Total: 20 marks)

....