Question 1

Read the case Study Below and use it to answer the questions that follow.

A Famous Data Security Breach & PCI Case Study: Four Years Later

Heartland Payment Systems (HPS) became famous in January 2009 for something it didn't want to be famous for: it was the victim of one of the largest data security breaches in U.S. history, with tens of millions of cardholder records possibly lost – the actual number has never been determined. The malware that surreptitiously stole and stored the account numbers was active for an estimated four months at a time when HPS was processing 100 million transactions per month.

Now, nearly four years later, HPS Chairman and CEO Robert O. Carr is speaking publicly about his company's experience and the lessons learned. It's a fascinating and dramatic story – one you didn't get at the time of the news reports on the breach, one that can only be told now. And it reinforces the adage that being compliant with the Payment Card Industry Data Security Standards (PCI DSS) don't mean you're secure.

I attended Carr's presentation on October 16 to the Technology Association of Georgia (TAG) in Atlanta. This report is based on Carr's remarks.

Facts about the Data Security Breach:

- The compromise came through a SQL injection attack on the company's website. Heartland immediately found out about it, and thought they had eradicated the malware.
- Roughly six months later, in mid-May 2008, the malware made the leap from the corporate network to the payment processing network, but HPS didn't know that at the time.
- Two weeks prior to the date the payment system was compromised, HPS was approved by their Qualified Security Assessor (QSA) as PCI compliant.

In late October 2008, HPS discovered they "might have a problem" based on information provided by one of the major card brands.

· Three forensics firms hired by HPS analyzed their IT security network; all three said the HPS system was free of malware. In January 2009, HPS staff members found the malware.

What happened Next: Disclosure

- The company's lawyers recommended a minimal level of disclosure about the breach, but Carr decided against that policy. HPS had a tradition of open communications with employees and customers, and Carr decided that he wanted to maintain that policy and share information as fully as possible. "We did a good job of damage control," he said during his October 16 speech.
- The company paid a heavy price. The stock price fell 78% in the weeks after disclosure, and 5,000 of the company's 250,000 merchants left. HPS was delisted by Visa and MasterCard. Four months later, VISA reinstated HPS.

The Full Cost:

The company suffered a $170 million loss. Although $20 million was covered by insurance, their net loss was $150 million.

Lessons Learned, all from Carr:

- "You can't just rely on firewalls."
- "Knowledge of security threats should not be viewed as a competitive advantage." When it comes to threats, companies should share information with peers and collaborate.
- HPS did not have an incident response plan in place at the time of the breach. It does now.
- The malware was able to move from HPS's corporate network to its payment processing system because of "human error."
- "You can't afford to have anyone in a position where they can make bad decisions that hurt you and help the bad guys," he said

Positive Developments from the Breach:

- HPS became very aggressive about data security as well as PCI compliance after the breach. It now pursues a policy of encrypting cardholder data from end to end – from the POS terminal to the end of the payment process.
- HPS worked with a Taiwanese firm to develop a more secure POS terminal for its merchants with encrypting hardware built-in. Now HPS believes its data security technology and processes are a competitive advantage.
- Carr helped initiate a new group within FS-ISAC to promote information sharing: the FSISAC Payment Processors Information Sharing Council.
- The leader of the hacking group, Albert Gonzalez, pleaded guilty and is serving a 20-year prison sentence. It was the longest sentence ever given for a cybercrime, according to SC Magazine. (HPS was not the only victim of Gonzalez — others included TJX,Hannaford and 7-Eleven.)
- Heartland's stock price and market capitalization have recovered the levels they had prior to the breach.

Required

i. From the example above, differentiate between *quantitative risk* and *qualitative risk assessment*. Illustrate your answer. (4 Marks)

ii. Assume you were asked to quantify the loss of data in financial terms (not the loss of stock price). Explain using an example how you would do this. (4 Marks)

iii. From your answers in i and ii above, justify why qualitative risk assessment is a more preferred method for risk assessment than quantitative risk assessment. (3 Marks)

iv. From the case above, demonstrate how the breach affected the Confidentiality, Integrity and availability of heartland payment systems. (9 Marks)

v. Security isn't simply a technology issue, it's a business issue. Discuss in reference to the case above (10 Marks)

Cracking

Section B

Question 2

You are the manager of a busy betting office which is located on a busy street. The office is open every day, from 8.30 am to 5pm every day. Six people are employed there, working morning, afternoon and weekend shifts. At the rear of the office are a staff toilet, a bathroom and a small kitchen where staff can make hot drinks and prepare food. There have been a lot of insecurity concerns in the country and this has prompted you to do a risk assessment to determine if the business and the facilities are safe.

Required

i. Explain how you will practically perform the Risk Assessment at the betting office (2 Marks)

ii. Explain at least **ten** likely threats and what can be harmed (5 Marks)

iii. Discuss **four** controls that are likely to be in place to minimize the impact of the threats focusing on their vulnerabilities and strengths (8 Marks)

iv. Give your opinion on the level of Security Assurance at the Betting Office and provide justified recommendations for improved security assurance (5 Marks)

Question 4

Omiti Enterprises sells a variety of knowledge and entertainment products mainly in CD-ROM to its customers in Nairobi. It is considering selling its music, academic and professional products over the internet. Currently, Omiti does not have an Internet presence and is not prepared to undertake all the learning required without strong support. In order to institute this ecommerce plan, the managers at Omiti understand the following services are needed

- Help in designing a website
- A service that would host its website
- A merchant account at a bank for deposits of credit card payments to its account
- A service that provides internet credit card authorization.

They are currently negotiating with a service provider who claims that it can manage all these functions. There would be a onetime set up fee, a monthly charge and a transaction fee.

i. What are the potential problems of relying on a service provider for managing all of a company's Internet transactions? (4 Marks)

ii. What are the benefits relying on a service provider for managing all of a company's internet transactions? (2 Marks)

iii. What are the potential problems of relying on an online service provider for your accounting needs? (4 Marks)

Computer fraud has been one of the areas that have been increasing among the various instances of fraud committed.

i. Explain **two** reasons why computer systems are particularly vulnerable to computer crimes. (4 Marks)

ii. Identify and explain **three** computer fraud techniques. (6 Marks)

Question 5

The following table gives part of some questions that an Auditor would like to use during an Audit of an Information Systems Department in an organization.

Test Area	Question
1. Password	2. Are passwords encrypted and not displayed on screen when entered?
3. Test plans	4. Are appropriate implementation, conversion and acceptance test plans developed for the organization distributed data processing and network hardware equipment?
4. File Handling Procedures	5. Have procedures been established to control the receipt and release of files, and secondary storage to and from other locations?
5. Contents and location of offline storage	6. Are offline library facilities located away from the computer room?
6. System value delivery	7. Are the systems (network and hardware) delivering value to customers, suppliers and the organizations in general including all other stakeholders?

i. For each question, clearly state what fact finding mechanism you could use and justify your reason. (5 Marks)

ii. For each question in (i), what evidence would you demand to see in order to verify the claims? (5 Marks)

iii. Assume that for each question asked on the Table above, the answer is "NO". Recommend appropriate control measures that can be put in place. (5 Marks)

iv. What **five** purposes will the information system audit policy serve in an organization? (5 Marks)