GUJARAT TECHNOLOGICAL UNIVERSITY
MBA. Sem-III Regular Examination January 2011

Subject code: 830403   **Subject Name: Technology and Business**
Date: 08 /01 /2011   **Time: 10.30 am – 01.00 pm**
                                                           Total Marks: 70

Instructions:
1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1 **(a)** What do you mean by "Efficiency" & "Effectiveness"? Explain Efficiency IT **07** matrices & Effectiveness IT matrices in detail.

(b) What is the meaning of "Business Intelligence (BI)"? Discuss why BI is **07** required in the business?

Q.2 **(a)** What are the most important factors that you would use in evaluating computer **07** hardware & computer software? Explain why? And Briefly explain different types of computer categories.

(b) Explain Pros & Cons of BI? Also explain the future characteristics of BI & **07** discuss what are the ways by which one can achieve those future characteristics.
OR
(b) What is the meaning of "Employee Monitoring"? Explain different technologies **07** by which one can monitor the employees. Discuss negative effects caused by employee monitoring.

Q.3 **(a)** Explain in brief different kinds of technologies / KMS that firm can use to **07** support its Knowledge Management infrastructure.

(b) What is the meaning of "SCM"? And explain five basic components of SCM. **07**
OR
Q.3 **(a)** What do you mean by "CRM"? Explain different types of CRM. And also **07** discuss successful CRM implementation strategy in the organization.

(b) Briefly define what is an "ERP"? Explain benefits & risks / cost associated with **07** an ERP system.

Q.4 **(a)** Short note : Content Management Systems (CMS) **07**
(b) Short note: Application, Operating System & Utility software **07**
OR
Q.4 **(a)** Short note: Technology used in BI **07**
(b) Short note: Benefits & Challenges associated with Outsourcing **07**

Q.5 **(a)** What do you mean by "ePolicies", list down major ePolicies available for **07** managing the information security & also explain any three ePolicies in detail.

(b) Identify & discuss the technologies which will have the greatest impact on **07** future business.
OR
Q.5 **(a)** What do you mean by Collaborative Partnership? What are the functions of a **07** typical collaborative business?

(b) Read the case carefully & give the answer of following questions: **07**
Thinking Like the Enemy
         David & Barry Kaufman, the founders of the Intense School, recently added several security courses, including the five-day "Professional Hacking Boot Camp" & "Social Engineering in Two Days".

Information technology departments must know how to protect organizational information. Therefore, organizations must teach their IT personal how to protect their systems, especially in light of the many new government regulations, such as the Health Insurance Portability & Accountability Act (HIPAA), that demand secure systems. The concept of sending IT professionals to a hacking school seems counterintuitive; it is somewhat similar to sending accountants to an Embezzling 101 course. The Intense School does not strive to breed the next generation of hackers, however, but to teach its students how to be "ethical" hackers: to use their skills to build better locks, and to understand the minds of those who would attempt to crack them.

The main philosophy of the security course at the Intense School is simply "To know the enemy". In fact, one of the teachers at the Intense School is none other than Kevin Mitnick, the famous hacker who was imprisoned from 1995 to 2000. Teaching security from the hacker's perspective, as Mitnick does, is more difficult than teaching hacking itself. A hacker just needs to know one way into a system, but security professional needs to know *all* of the system's vulnerabilities. The two courses analyze those vulnerabilities from different perspectives.

The hacking course, which costs $3,500, teaches ways to protect against typically associated with hackers: worming through computer systems through vulnerabilities that are susceptible to technical, or computer-based, attacks. Mitnick's $1,950 social engineering course, by contrast, teaches the more frightening art of worming through the vulnerabilities of the people using & maintaining systems-getting passwords & access through duplicity, not technology. People that take this class, or
read Mitnick's book, *The Art of Deception*, never again think of passwords or the trash bin the same way.

So how does the Intense School teach hacking? With sessions of dumpster diving (the unsavory practice of looking for passwords & other bits of information on discarded papers), with field trips case target systems, and with practice runs at the company's in-house "target range," a network of computers set up to thwart & educate students.

One feature of the Intense School that raises a few questions is that the school does not check on morals at the door: Anyone paying the tuition can attend the school. Given the potential danger that an unchecked graduate of a hacking school could represent, it is surprising that FBI does not collect the names of the graduates. But perhaps it
gets them any how-several governmental agencies have sent students to the school.

Questions:

1. How could an organization benefit from attending one of the courses offered at the Intense School?
2. If your employer sent you to take a course at the Intense School, which one would you choose & why?

****