UNIVERSITY OF SWAZILAND

DEPARTMENT OF BUSINESS ADMINISTRATION

SUPPLEMENTARY EXAMINATION PAPER

JULY, 2014

TITLE OF PAPER : INTRODUCTION TO BUSINESS COMPUTING

COURSE CODE : BA 112 FULLTIME AND IDE

TIME ALLOWED : THREE (3) HOURS

INSTRUCTIONS:
1. THE NUMBER OF QUESTIONS IN THIS PAPER = SIX (6)
2. SECTION A IS COMPULSORY.
3. ANSWER ANY THREE (3) QUESTIONS IN SECTION B
4. THE MARKS TO BE AWARDED FOR EACH QUESTION ARE INDICATED ALONGSIDE THE QUESTION.

NOTE: MARKS WILL BE AWARDED FOR GOOD COMMUNICATION IN ENGLISH, AS WELL AS FOR ORDERLY AND NEAT PRESENTATION OF WORK. FURTHER MARKS WILL BE AWARDED FOR USE OF RELEVANT EXAMPLES.

SPECIAL REQUIREMENTS: NONE

THIS PAPER IS NOT TO BE OPENED UNTIL PERMISSION HAS BEEN GRANTED BY THE INVIGILATOR.

CASE

Databases are repositories of critical, often proprietary data. Protecting them with appropriate security is therefore vital. The computer that runs the DBMS should always be protected by a firewall. The firewall, a computing device located between a firm's internal network and external networks, prevents unauthorized access to the internal traffic whatsoever to reach the DBMS computer. If the database is processed over the internet, the firewall should provide limited access through packet filtering and other techniques.

For the best security, the DBMS computer should be protected by a firewall, and then all other security measures should be designed as if the firewall has been breached. In particular, all operating systems and DBMS patches should be installed as soon as they become available. In the spring of 2003, the Slammer worm infected the computers running on SQL Server. Months before, Microsoft had published a patch that prevented access by this worm. Only computers that did not have the patch were infected.

To prevent unauthorized access no one other than authorized operations personnel should be able to directly access the computer that runs the DBMS. Instead, all access should be via authorized application programs. The computer running the DBMS should be secured behind locked doors, and visits to that room should be recorded in a log.

All major DBMS products have extensive, built-in security features. These features allow for the definition of user accounts and user roles. Each user account belongs to a specific person. A role is a generic employee function, such as payroll clerk or field sales person. Each user account and user role is assigned specific actions for specific tables and for columns in those tables. For example, an account can be defined to allow access for a specific person say Themba Dlamini and a password ID defined to protect that account. Some DBMS products, such as Oracle, will disallow the definition of strong passwords.

Once an account is defined, it can be assigned specific permission, and it can also be assigned particular roles. When assigned a role, the user will inherit all permissions for that role. This means by which this is done varies from DBMs to DBMS.

The fund manager role is assigned specific permission for each of the tables in the volunteer database. If Themba Dlamini is assigned the fund manager role, then he can, for example, read and insert rows into contact the table. He may not however, update or delete any row in the contact table. It is also possible to further restrict actions to particular columns of each table.

Most DBMS products log failed attempts to sign on and produce other usage reports as well. The database administrator should periodically monitor such logs and reports for suspicion activity.

Finally it is important to have a plan of action for security emergencies. The steps to take vary from database to database. If the database contains little confidential data, this plan may just

have steps to report the security problem and to take corrective actions to prevent such problems in the future. However, if the database contains sensitive and confidential data, then the plan should include procedures for preventing further loss and for contacting the corporate legal staff and law enforcement agencies.

Questions

Summarize the steps that can be taken to protect the DBMS and its databases. 20 marks

Suppose that a database having valuable proprietary data has been breached. What steps will need to be taken 20 marks

SECTION B

Answer any three

Question 1

(a) Supposing you were the IT manager at the mall in Kenya when the terrorist attack took place. As an IT specialist what should you have done to make sure that when the terrorist's attacks took place you did not lose any of your work in the system? 10 marks

(b) A small business is interested in computerizing some of its recordkeeping functions with a laptop. What considerations are important in deciding the size of primary and secondary storage? What special features for secondary storage should be considered? 10 marks

Question 2

(a) What are the major factors to consider when selecting application software 10 marks
(b) Define fourth generation languages and list the seven categories of fourth generation tools 10 marks

Question 3

(a) Describe some of the problems of the traditional data processing environment 15 marks
(b) Define WAN 5 marks

Question 4

(a) Explain what a DBMS is and what it does 4 marks
(b) Define and describe the indexed sequential access methods and the random access method 6 marks
(c) What is the difference between an assembler, a compiler and an interpreter? 10marks

Question 5

Mr Dlamini has been employed by the university as the database administrator, what do you think are his duties 10 marks

What is data warehousing? 10 marks