

**SCHOOL OF ENGENNERING SCIENCE AND TECHNOLOGY**

**CHINHOYI UNIVERSITY**

**OF**

**TECHNOLOGY**

**DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY AND ELECTRONICS**

**BACHELOR OF SCIENCE HOUNERS DEGREE IN INFORMATION TECHNOLOGY**

**PABAZHIRA BENEDICT MUFARO**

**NAME**

**C108800P**

**COURSE**

**DUE DATE**

**REG NUMBER**

**COMPUTER SECURITY 404**

**NUMBER 1**

**ASSIGNMENT**

**3 APRIL 2014**

**Ms MUHONDE**

**LECTURER**

**Question 1**

Explain how you would use the following to achieve information security within an organisation.

1. Data dictionary- it is the centralized repository of information about data such as meaning, relationships to other data, origin, usage, and format. The data dictionary is mostly read only. The views of the data dictionary serve as a reference for all database users. To achieve maximum security the organisation should access the data dictionary views with SQL statements. Some views are accessible to all Database users, and others are intended for database administrators only. The data dictionary is always available when the database is open. It resides in the SYSTEM table space, which is always online.

In order to achieve information security within an organisation the security administrator will also create additional public synonyms for schema objects that are used system wide as the database creates public synonyms for many data dictionary views so users can access them conveniently. Users will be denied naming their own schema objects because they might end up using the same names as those used for public synonyms.

Other Database products can reference existing views and create additional data dictionary tables or views of their own. The security administrator should make sure application developers who write programs that refer to the data dictionary should refer to the public synonyms rather than the underlying tables: the synonyms are less likely to change between software releases.

1. **Audit trails -**  (also called audit log) it is a security-relevant chronological record or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. In an organisation the audit trail will be run always in a privileged mode, so it can access and supervise all actions from all users; a normal user should not be allowed to stop/change it. Furthermore, for the same reason, trail file or database table with a trail should not be accessible to normal users. Another way of handling this issue is through the use of a role-based security model in the software. The software can operate with the closed-looped controls, or as a closed system.

**Question 2**

1. Two security threats associated with E-Commerce websites are:

**Threats from an actual attacker(s)** - the motivation is primarily psychological.  The intent is to garner personal information from people for the sheer purposes of exploitation (such obtaining Credit Card and Bank Account information; Phishing schemes, obtaining usernames and passwords, etc.).

**Technological failure** - anything related to the Internet can cause problems.  This can be anything from a network not configured properly to data packets being lost, especially in a wireless access environment.  Even poorly written programming code upon which the E-Commerce websites was developed can be very susceptible to threats.

1. Possible solutions for the threats above are as follows :

**Threats from an actual attacker(s)** - the business community should adopt more robust and secure platforms.  A prime example of this is the use of Linux as the operating system, Apache as the Web Server Software, and either PostGRESql or My SQL as the database (these are database languages created from the Structured Query Language, or SQL) they are more secure.

**Technological failure** – The network administrators should configure the network properly so that the network will be stable most of the times. There should a backup system in place in case the server hosting the E-Commerce website goes down the backup will continue with operations.

1. **In drafting the alternate backup and recovery process contract the security administrator should consider the following**

**Scope:** the scope of the contract should be clearly stated. For example data custodians are formally and explicitly made known of their responsibility of providing adequate backups to ensure the recovery of electronic information in the event of failure. These backup provisions will allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained. The security administrator should also make sure that in the contract includes company regulations pertaining to the long-term retention of information (e.g., financial records)

* The security administrator should consider the aspect that on data accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. Information located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives.
* The contract should include Backup documentation including identification of all critical data, documentation and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data centre disaster scenario, if applicable.
* The contract should have a clause where recovery procedures must be tested on a regular basis.

**Question 3**

**Efforts being made to curb cybercrime in Zimbabwe**

Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.Cybercrimerefers, mostly, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, identity theft, child pornography, and child grooming.

The Computer Fraud and Abuse Act passed in 2004 is one of the broadest statutes in Zimbabwe used to combat cyber-crime. It has been amended a number of times, most recently by the Deputy Chairman, Law Development Commission, the Identity theft enforcement and Restitution Act of 2008. Within it is the definition of a “protected computer” used throughout the Zimbabwe legal system to further define computer espionage, computer trespassing, and taking of government, financial, or commerce information, trespassing in a government computer, committing fraud with a protected computer, damaging a protected computer, trafficking in passwords, threatening to damage a protected computer, conspiracy to commit a cyber-crime, and the penalties for violation

The Zimbabwean government has introduced the Counter-Terror Social Network Analysis and Intent Recognition (ZCT-SNAIR) project which uses the Terrorist Action Description Language (TADL) to model and simulate terrorist networks and attacks. It also models links identified in communication patterns compiled from multimedia data, and terrorists’ activity patterns are compiled from databases of past terrorist threats. Unlike other proposed methods, ZCT-SNAIR constantly interacts with the user, who uses the system both to investigate and to refine hypotheses. Multimedia data, such as voice, text, and network session data, is compiled and processed. Through this compilation and processing, names, entities, relationships, and individual events are extracted from the multimedia data. This information is then used to perform a social network analysis on the criminal network, through which the user can detect and track threats in the network.

Behavioural countermeasures have been put into effect through the Sunday Mail as a tool in combating cyber-crime. Public awareness campaigns can educate the public on the various threats of cyber-crime and the many methods used to combat it. It is also here that businesses can also make us of IT policies to help educate and train workers on the importance and practices used to ensure electronic security such as strong password use, the importance of regular patching of security exploits, signs of phishing attacks and malicious code, among others.

International cybercrimes often challenge the effectiveness of the efforts made by the Zimbabwean government. Because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the Internet in order to take advantages of the less severe punishments or difficulties of being traced. Moreover, complexity in types and forms of cybercrime increases the difficulty to fight back. In this sense, fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law.

The efforts made to curb cybercrime in Zimbabwe are greatly evident and appreciated as the crimes are being continuously fought with revised polices.

**Question 4**

The Biba model addresses the issue of integrity in a computer system, i.e. whether information can become corrupted. If a high security object comes into contact with a low-level information, or be handled by a low-level program, the integrity level can be downgraded. For instance in an organisation like FBC Holdings, if one used a corrupted flash stick on company computers, the viruses on the flash drive might corrupt the documents on the computer, append them, truncate them, or even covertly communicate them to another parts of the system.

Integrity at FBC Holdings is achieved through the implementation of the Biba model in the following ways:

Role based access control- as the organisation is very big with hundreds of employees the company gives each and every employee a role. The roles given to the employees are the ones which will deny others access to the system while others are granted access. For example the security guard cannot access the bank teller’s information as their roles are different in the organisation.

Secrecy levels in the Biba model goes from high to low which maintains integrity within the organisation and information security as a whole. The clearance levels differ from employee to employee, a junior employee handles secret information yet he does not handle top secret information which senior employees do. For example the chief financial officer handles secret information from the auditors which can never be handled by the bank teller.

Using the Chinese wall in Biba model – the Bank can use the Biba model such that the system would be partitioned into different domains. The user can access all domains initially but as soon as the user chooses a domain he loses access to all other conflicting domains. An example is untrusted hard drives as soon as the computer reads an external hard drive the system permanently loses network write access on the Banks financial accounts to maintain information security