Data security course work

\n[toc title="Table of Contents"]\n

\n \t

1. Q 1- Current event \n \t
2. Data Security incident at Leicester City \n \t
3. References \n

\n[/toc]\n \n

Q 1- Current event

Locate a recent news item (less than one month old) that deals with an issue of Data Security. Summarize the data security incident and then state what principle(s) of data security was violated or ignored. Include a link to the news item. (http://blog. alertsec. com/2011/03/new-data-breach-incident-at-leicester-city-council/)

Data Security: Data security is very important as it ensures that data of a given company or institution is protected against the deliberate or accidental access of data by unauthorized people. Breaching of data security can bring a company or an institution down to its knees. Care should therefore be taken to ensure that data security is taken into consideration and that nothing goes wrong with an institution's data.

Data Security incident at Leicester City

The city council at Leicester City recently experienced an incident of data security whereby a USB memory stick containing data of about 4, 000 people was lost. The USB memory stick had medical details and home security codes for over 4, 000 city residents. The USB stick got lost in early March this year. The information has been confirmed as published in a local newspaper.

The affected citizens were signed up to Leicester Care which provides support to vulnerable city residents. It is however ironical that Leicester city council had experienced a loss of another unencrypted USB memory stick which had information of over 80 children which prompted them to sign up an undertaking with ICO. The council has embarked on an operation of resetting all codes and reported the same to the ICO (Information Commissioner’s Office). This incident has also been reported to the police and investigations into the matter are underway. The affected people are very worried and blame the Leicester City for such an ‘ irresponsible’ occurrence.

Q 2- From your current event (“ recent topic”) of Q1 create a plan to prevent such a security incident from happening in the future. In other words, what steps should be taken, and what tools used to prevent the problem?

The above security incident exposed confidential information about city resident’s medical information and home unlock codes to unauthorized people. This problem can be solved by devising mechanisms which will ensure that even if the USB memory stick is lost, confidential information is not exposed to unauthorized people. A replica of the information in the USB memory stick should also be kept to ensure that the information is always available even if the USB memory stick is lost. The following steps can be taken to prevent the problem.

i. Using lock codes to protect the USB memory sticks. This will ensure that a person cannot be able to access information in a USB memory stick unless he/she has the unlock code for that particular kind of USB memory stick. (Marsha, 2002) This will help in protecting data from unauthorized access.

ii. Using data security software or data encryption software can ensure that all the data stored in the USB memory stick is safe. The encryption software will ensure that even if unauthorized person gets the lost/stolen USB memory stick, he /she cannot access the data. Some of the software used for protecting data against unauthorized access includes:

a) Encrypting File System (EFS) – They help to prevent unauthorized access to data and even if a USB memory stick is lost, one who gets it cannot access the data inside it as they are gibberish.(Shimanek, 2001) This ensures that unauthorized persons cannot get the contents of the lost USB memory stick.

b) My Document Redirect – This helps in redirecting users into the documents folder on the server. This helps in making backup copies of the data. The data can be later accessed incase a USB memory stick is lost containing some confidential data is lost.

c) Using Microsoft’s BitLocker To Go – This helps in encrypting data found in the USB memory stick. (Marsha, 2002)

d) Using Apricorn Aegis Padlock – this system helps to provide some form of hardware based encryption which requires a valid PIN in order to access the contents of a storage device like a USB memory stick. (Marsha, 2002). This will protect the contents of the USB memory stick as a person cannot access its contents before entering the valid PIN.

iii. All data in the company or organization should be backed up. This ensures that even if a USB memory stick is lost, data can still be retrieved from the backed up copies.

References

Anna Shimanek, (2001) Note, Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles, 26 Iowa J. Corp. L. 455, 462–463

Bainbridge, D. (2005) " Introduction to Computer Law - Fifth Edition", page 430. Pearson Education Limited.

Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan. (2002)The Right to Privacy and Person Data: The EU Prods the U. S. and Controversy Continues, 9 Tulsa J. Comp. & Int'l L. 391, 441

http://blog. alertsec. com/2011/03/new-data-breach-incident-at-leicester-city-council/