Databases and Security

Your Name Here

Instructor's Name Here

Introduction

Information Technology (IT) is prevalent in almost every aspect of life. It is utilized in businesses and by individuals for a variety of activities. It is possible for individuals to communicate with others, shop and pay bills on-line, and store valuable, personal information where it can be accessed quickly. This necessitates the need for computer systems to provide a level of security to reduce the opportunity for this digital information to be compromised. The term 'security' as applied to computer systems often refers to the network and the hardware on which the data is stored. Information Technology Security (IT Security) is the implementation of measures designed to protect computer systems and networks to protect and safeguard data to safeguard data against unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure to preserve the confidentiality, integrity, availability, and ability to perform the permitted critical functions (SANS Institute, n.d.). However, security also applies to other aspects of computing, specifically databases. A database (DB) provides a method to store information in an organized manner which enables the data to be accessed, managed, and updated easily and databases are often used to store sensitive information. Databases require a database management system (DBMS) to access the information stored within (Bean, n.d.).

As the use of IT and databases has increased, the number of cyber attacks has also increased. In 2005, a security breach compromised the data of approximately 92 million customers of AOL and the data of an additional 40 million individuals was compromised as the result of a security breach of Cardsystems Solutions Inc. In 2015 to date, data breaches have occurred at a wide variety of companies, including the data of 145 million E-bay customers, 2.4 million AOL users, 76 million P Morgan Chase customers, 56 million Home Depot customers, 11 million Premera patients, and 25.5 million individuals from the data of the US Office of Personnel Management in two separate incidents, among numerous others (Information is

Beautiful, 2015). These data breaches are occurring world-wide and the data obtained is often used to commit other crimes, such as identity theft.

The 2015 Cyberthreat Report reflects that 71 percent of the respondents were victims of successful cyberattack in 2014. Seven percent indicated that they had been victimized ten times or more during the previous twelve months. Fifty-two percent indicated the expectation of being victimized again in 2015. Sixty-two percent of the respondents indicated that the budgets for IT Security are increasing during 2015. The probability of becoming the victim of a cyberthreat or cyberattack necessitates asking the question of "What can be done to further ensure the integrity of data that is stored within database systems in the case of a security breach?"