COMPUTER SCIENCE, DATABASE SECURITY

Student’s name:

Institution affiliation

Date

**Computer Science, Database Security**

**Introduction**

A database entails a piece of organized information within an organization. Every organization has numerous types of data, which may entail financial details, customer information, plans for the future, or performance history (Blake, 2017). Therefore, a database is a basic requirement for an organization. However, its availability is not enough; the database should be secure and should be shielded from hackers and unauthorized persons. Theft of information can cost an organization millions of dollars. For instance, if a rival firm retrieves prospects, it may adjust its future and stay ahead of you and the rival company will have an unfair advantage. Protection of the database is key. A decision to incorporate a database of another company requires thorough scrutiny.

**Key assessment protocols (assessment of ABC database)**

The key assessment protocols that are essential to determine whether the database is secure will **b**e as follow; The first scrutiny will be based on the ability of the database system to be carefully accessed by a set of commands and programs. Only authorized individuals will be able to access data. Further, the authorized individuals must have secure login credentials like fingerprints and passwords. In other words, the system should have encryption on a secure single server with just one person holding the encryption key ("Data protection-data security-privacy", 2018). In addition, the data system should also be accepted if it has a database that has a backup system, but the programs should have control over it. ABC database history should also be scrutinized. Previous cases of hacking and data mishandling are critical in accepting or rejecting the database of the company.

A secure database involves a variety of tools and security controls put in place to protect database confidentiality, integrity, and accessibility. Examples of secure database protocols are auditing, backups, application security, access control, and applying statistical methods. A secure database must organize and take care of data. The database management system entails the physical database server and network infrastructure used to access the database. Secure databases can face threats like human error, insider threats, exploitation of database vulnerability, and attacks o backups. Despite the threats, a secure database is very important.

**Merits of a secure data**b**ase**

The first secure database is important since it is used to store an immense amount of data like customer profiles and product information. It also makes it easier for different users to access data from any place with speed. A secure database ensures that the information stored is valid and protected from deletion even during transmission over the networks. It makes sure that users can only see what they are supposed to see, and this means the confidentiality of the data is secured.

Secondly, a secure database protects data from data tampering, data security risks, and data theft. When data is properly secured, it reduces theft cases like stealing credit cards, .driver's licenses information, and setting up fake credit accounts using someone else's details. Data breaches or hacks can be controlled. Threats affect database security ad also functioning of the company. It may also bring harm to the organization. Secure data helps protect computers from hackers. When hackers gain accessibility to a computer, they may steal private information. This can distract the organization and its customers. Hackers can also destroy hardware and introduce viruses. Data tampering is the act of purposely editing data through illegal channels. Data tampering can lead to exposure of data and deletion of essential files if not well-taken care of.

Thirdly, the secure database is cost-effective for the company thus reducing the risk of losing money; instead, it acts as an investment. It is made possible when the security database complies with the organization's terms and policies. It also guarantees server protection from any harm that might lead to data processing failure (Lehto, 2013). It implies data recovery and backup is fast and possible after a system crash. Data access is also faster and accurate. Data checking is faster and easier to search and make inquiries. Understanding data is easy since it has simple and well structured.

**Conclusion**

Data organization, protection, and integrity are essential for any organization. There should be keen scrutiny for any database before it is admitted or incorporated with another. Integrity and confidentiality of information are paramount for survival and better performance in any organization. Briefly, the ABC database should be accepted if it has a working backup system with one server, which is encrypted and can only be accessed using encrypted keys, and it should have a reputable history.

**References**

Blake, E. (2017). Network and Database Security: Regulatory Compliance, Network, and Database Security - A Unified Process and Goal. *Journal of Digital Forensics, Security and Law*. doi: 10.15394/jdfsl.2007.1033

Data protection-data security-privacy. (2018). *Computers & Security*, *3*(1), 57-58. doi: 10.1016/0167-4048(84)90031-2

Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. *International Journal of Cyber Warfare and Terrorism*, *3*(3), 1-18. doi: 10.4018/ijcwt.2013070101