Database Management & Security 360

A WHITE PAPER PRESENTED BY:

KG Hawes
Partners in Technology

2020

CONNECT: 400 International Way, Suite 300 | Springfield, OR 97477
(866) 687-9006 | www.kghawes.com

KG Hawes
Partners in Technology

ABSTRACT

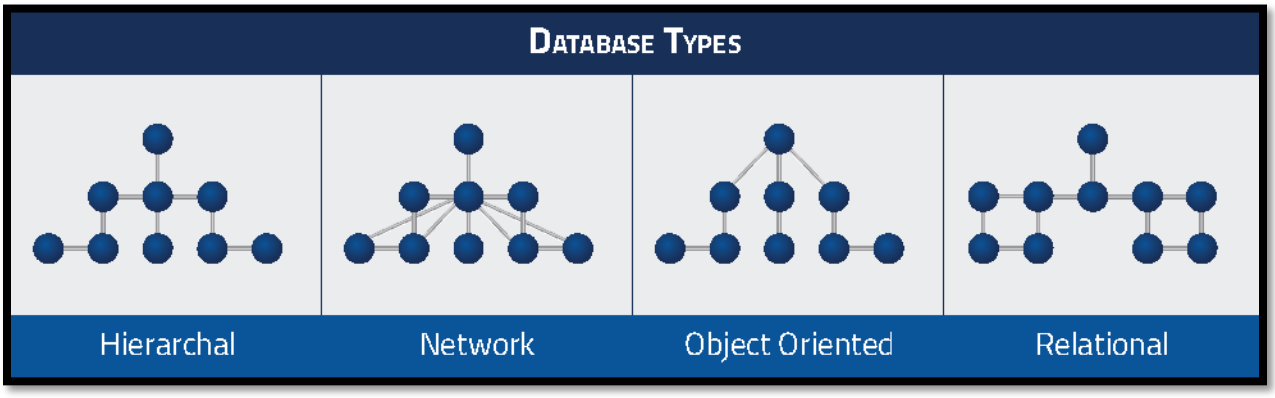
Database integrity plays a critical role in the success of today's businesses. Over one million companies worldwide depend on the accurate recording, updating, and tracking of data every minute of every day. While the concept of a database may seem simple, the systems themselves are quite complex, often necessitating the implementation of an independent management system. This paper will offer an overview of database functionality citing the imperative role of Database Management Systems (DBMS) and the attention these systems require. With the aim of aiding in infrastructure assessments for business owners or decision makers, this White Paper will conclude with a description of the burden database management can impose on IT departments and the benefits of utilizing database management services.

Contents

Database Fundamentals

Overview

To put it simply, a database is a library of stored information. The organization of the information within a database, referred to as it's "schema," can vary greatly. Four of the most common database schemas are *Hierarchical, Network, Object Oriented*, and *Relational*. These methods describe not only the arrangement of the data being stored but also the relationship between each different classification. This affects the performance of the database, or more plainly, the speed in which the information can be retrieved. Hierarchical databases arrange information in a tree structure, where the relationship between records is predefined. Network databases are similar to hierarchal databases in structure; however, the relationship between records is more web-like, supporting more relationships between records. Object-oriented databases utilize programming language to organize information around a class system. The most common database structure is arranged relationally, in columns and rows, for quick access, simplified comparison, or bulk updating.



In addition to information storage, a database performs the basic functions of retrieving, updating, and deleting its content. While conceptually simple, performing these operations can present a number of organizational issues if any of them are attempted simultaneously on overlapping data. This creates the necessity for a management system.

Database management systems (DBMS) are specialized software used to regulate any conflicting commands. DBMS are especially important when information needs to be accessed by multiple users or applications. These systems consist of two primary functions:

1) Database security (including compliance), *and*
2) Data organization and access.

> It's expected that 57.6% of Government organizations, 73.5% of educational organizations and 74.5% of retail organizations are at direct risk of suffering a database breach. (1) 2019 Cyberthreat Defense Report

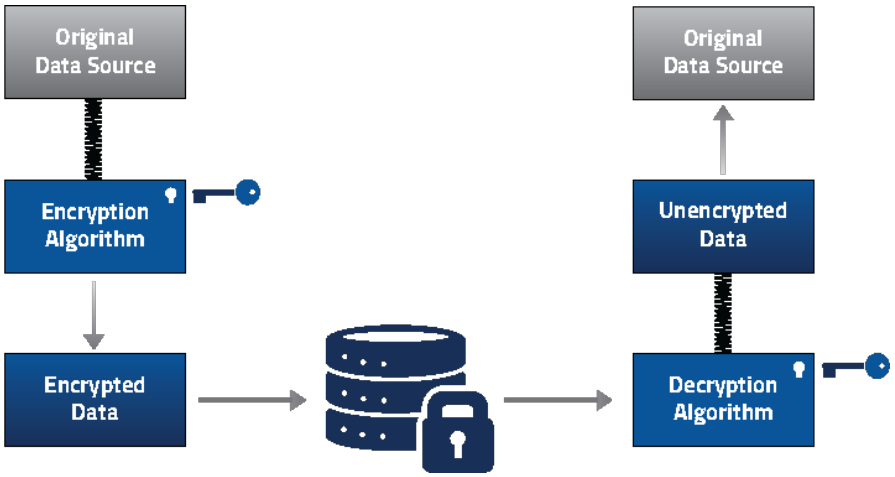
Database Security

Considering that a business' database holds all essential information, including financial data and intellectual property, there is nothing more important than maintaining its integrity and security. The two underlying approaches to database security are *encryption* and *access controls*.

Encryption

Encryption is the first step towards protecting your data. A basic encryption method utilizes an algorithm to encode the data within your database into a form that is otherwise indecipherable until it's decrypted with a special key. There are many strategies for encrypting data. The primary concern when employing a DBMS is to be certain that the encryption method is applied to both the DBMS and the operating system on which it exists. Weak operating system security can adversely affect the security of your database.

Encryption methods require the exchange of "keys" for users to be granted access to the data. Database security includes complex key management practices. The larger the database, number of applications being used, or authorized users, the more arduous key management practices need to be. If keys become lost or stolen, the security of the entire database could be compromised.



Some encryption may occur on an application level. In this case, an application independent from the database is needed to encrypt the data prior to it being stored. There are advantages to employing this method, the most important being that an outsider would need access to both the original application as well as the database in order to decrypt the data. However, if the data within a database is encrypted with varying methods, then it can become difficult to manage in terms of organization or searching. This present serious problems in key management, or organizing permissions and access, for the various applications that are performing the encryptions.

When Encryption is Required

In certain instances, encryption is a mandatory practice. Businesses whose databases house information pertaining to consumer financial data, personal consumer information, or any information related to government services or the military, are governed by federal compliance regulations. Businesses who fail to successfully secure this type of information risk serious legal and monetary damages for non-compliance.

Access Controls

Access controls refer to how users and applications access the database and what authentication practices are used. This is the first place to look for any loopholes in security such as incongruent administrative permissions or user credentials. Clearly defining user roles and access permissions is a simple yet effective way to enforce database security. Careful consideration should also be given to how the primary operating system and any applications interact with the database.

Simple steps should be taken to limit user access. This includes disabling old user accounts, removing accounts with public access, and limiting the number of users with administrative permissions. Attention to passwords, such as implementing a password strength policy or regularly auditing default passwords, can go a long way towards maintaining a secure database. Weak authentication practices are one of the most common reasons database security is compromised. If access controls are not managed properly they may undermine any encryption or key management efforts.

Hashed Password

Hashing passwords is the act of encrypting passwords that are stored on your database using a complex algorithm. Hashed passwords are only encrypted within the database and cannot be decrypted. This means when a user enters their password, the application in which the password applies “hashes” it and then compares it to the password stored in the system. Password hashing is intended to provide additional security for all the passwords housed within your database.

Database Failure

Most DBMS have incorporated utilities for backing up or recovering data in the event of a system failure. These utilities typically follow a two-tiered approach to protecting the integrity of the database by first, maintaining some kind of additional memory or duplicate storage facility for the "physical" data (such as the files within the database), and then by maintaining a secondary version of the "logical" data (i.e. the structure of the database itself), including functions and procedures. In the event of a failure, these secondary storage facilities can be accessed to reproduce any information that may have been lost, thus stabilizing the system.

Types of System Failures

A System Crash

System crashes occur when there is an issue with the hardware, software, or network that disrupts the DBMS reading and writing processes (i.e. the processes in which it transfers or records information).

A System Error

A system error occurs when there is an interruption in the reading or writing process that interferes with its completion of the task.

Local Errors

Local errors are similar to system errors but they result in a cancellation of the intended process.

Concurrency Control Enforcement

This occurs when there is an error in the system management. When tasks are not prioritized properly, and too many requests of the same nature are being made, then a deadlock is created. Requests are then either frozen or aborted.

Physical Errors

These can occur from a variety of issues relating to the physical environment of the system including power failure or wiring problems.

Catastrophic Situations

These are major threats to the system integrity as a whole due to serious conditions such as an environmental catastrophe such as a flood, or a security breach due to a large-scale infiltration.

System Log

DBMS typically utilize a system or “transaction” log technique which records the actions of the system in a preset number of intervals. This log not only keeps a record of “events” but also includes checkpoints for operations in case of a disruption. When the system hits a checkpoint, the logs are stored so that they can be accessed in back up or recovery efforts.

The lead into any number of these issues is often performance problems; when retrieval or storage operations become sluggish, it is a good indicator of a larger issue. The degree of difficulty in remedying performance issues can range greatly, from complicated flaws in the original coding, to a simple management system maintenance requirement. To avoid small issues with performance from becoming a serious failure, your database should get regular attention and tuning. Consistent maintenance schedules can help prevent potential calamity and optimize the use of your system.

Outside Threats

System failures are not the only threat to a business' database security. Cyber threats mean serious consequences for a business in terms of non-compliance and the resultant imposition of monetary damages in recovery costs and operational downtime. The two most common tactics employed by cybercriminals, in an effort to sabotage or steal information from your database, are SQL injections and DDoS attacks.

SQL Injections

This kind of attack injects malicious code into the language used for managing the data within your database. Criminals can use SQL injections to give themselves special user permissions, gaining access over the operating system administration controls, application privileges, and the ability to view or alter any data for the purposes of identity theft or fraud. This kind of attack is the biggest external threat to database security.

> A recent study showed that SQL injections represented nearly two-thirds of all web-application attacks. (2)

DDoS Attacks

In a Distributed Denial of Service attack (DDoS), the user's access is disrupted or temporarily disabled. This is typically achieved by overloading the system with requests causing a deadlock scenario similar to what happens in the event of a configuration problem. DDoS can be introduced to a system through various forms of malware. A DDoS attack is a common strategy for criminals engaged in a ransomware scam. In these attacks, access to the information on your database is locked down until you agree to pay the ransom for its release though the restoration of your system is never guaranteed.

Decrypt, Inject, Deny: *3 of the Costliest Database Scams*

TJX Companies

TJX Companies, which includes thousands of retail stores such as TJ Maxx and Marshall's, suffered a major data breach as a result of weak encryption methods. The breach affected an estimated 100 million consumer's credit card information, resulting in a $9.5 million settlement, and a sizable reduction in the company's stock worth. After compounding all the cost associated with the breach, TJX Companies incurred an estimated $256 million in damages. (3)

Heartland Payment Systems

Heartland Payment Systems, a payment processing company, found themselves victims of one of the worse SQL injections to date. The breach went undetected for nine months exposing an estimated 134 million individuals' credit card information. In addition to being held responsible for any fraudulent payments made from the accounts of exposed consumers, Heartland was forced to halt operations for close to six months, costing them approximately $145 million dollars. (4)

Hollywood Presbyterian Medical Center

Hollywood Presbyterian Medical Center, a hospital in Los Angeles, was the target of a DDoS attack as a part of a ransomware scam. The DDoS attack effectively locked the hospital staff out of key records stored on its database for over a week. The hospital was forced to halt most services and divert patients to other nearby hospitals. Hollywood Presbyterian Medical center eventually paid the ransom of approximately $17K for the records release but estimates of the total cost of the shut-down and recovery is not yet available. It is said the hospital narrowly avoided compliance fines as the attack only limited access to patient information; however, no evidence was found that it had been stolen. (5)

Managing your System

Databases require regular updating and maintenance if a business hopes to nullify the risks of failure or intrusion. There are many costs associated with effectively managing your business system. In addition to the initial purchase price, some DBMS may require licensing, additional hardware, IT staff and/or training. There are many considerations to be made for effective management of your business' database system. One of the primary concerns is whether your IT department is prepared for the responsibility.

Is IT Prepared?

The following is a brief outline of the labor involved in database management and security. When considering the current or future state of your own business system, you need to be fully aware of the responsibility that your IT department will be undertaking to safeguard the business against compliance risks, operational collapse, or both. Recognizing the range of tasks can assist you in identifying the preparedness of your team and to make any necessary adjustments.

Installation: Installation processes may include hardware, software, drivers, and pre-installation configurations. Installation requirements can vary greatly by design and manufacturer.

Tuning: Tuning is one of the most difficult aspects of managing your business database system. Tuning is required on all levels of operation from files and applications to the operating system. Proper tuning is essential to the performance of the database. DBMS tuning requires configuration of the processor and memory.

Maintenance: Regular maintenance duties include defragmentation, backups, and updating. These tasks are essential to the core operating efficiency of the database. If maintenance is neglected, or postponed, it can cause serious interruptions in functionality.

Integration: IT staff must be capable of handling any integration issues with the database. The system is useless if it conflicts with any existing applications required for business operations.

Migration: Migration alters the design of the database itself and can be a risky endeavor for an inexperienced technician. This process is crucial during the implementation or upgrade of a current system and is used to remedy problems or create patches within an older system.

Monitoring: Database monitoring is a necessity for identifying performance issues and potential security breaches. For best results, IT departments should have a strategy for monitoring that includes an alert system.

Security: To ensure the strongest possible database security, a strategy needs to be in place. The strategy should include mapping of the database's use and exposures as a part of a larger assessment. Assessing your database and management system is a key part of developing infrastructure security and security protocols. Classification of the information stored on the database should be made by sensitivity level to create an organizational strategy around compliance demands. Security policies and protocols must be created and implemented and should include parameters for access controls, an alert system for violations, and constructive actions such as encrypting or segregating data.

Recovery and Repair: IT departments need to be well prepared in the instance a recovery is needed. Maintaining backups and transaction logs is mandatory but worthless if the department is not familiar with the various methods of restoring or repairing the system.

Database Management Services

As previously outlined, there are many steps that must be taken to manage and secure your business' database. In the event of a database failure, businesses may find themselves limited by the size and aptitude of their IT department. Because so much of a business' operations are reliant upon the functionality of their database, many are turning to third-party specialist to negate the risks. Hiring a third-party service can alleviate a lot of the IT burden for a business. There are numerous factors that need regular attention to ensure the best performance and security of your system. It is not only advantageous to have these needs met by experienced technicians, it is often more cost effective than hiring or dedicating existing staff to the cause.

Benefits of Using a Service

Expert Experience: Hiring a service means you benefit from certified and experienced technicians who may be able to offer insights and efficiencies that can easily be overlooked by general IT staff. A service is likely to have seen the issues that your system may be facing now, offering an advantage in being able to quickly correct the issue the first time around.

Specialization: A service can offer a degree of specialization beyond just bare bones maintenance. Since they are only focused on the database, they can dedicate time and energy to improving functionality and processes. This kind of acute attention cannot be offered by an IT team with split responsibilities.

Uninterrupted Monitoring: Management services can offer 24/7 uninterrupted monitoring which can be near impossible for businesses to match with their own IT department. Twenty-four hour monitoring could mean a world of difference in the instance of a system failure, lessening downtime and other costs which occur as a result.

Overhead: Managing the complex needs of a business' database requires a number of tools and resources. It is the responsibility of a Management Service to obtain all of the current technology and innovations in the field in order to remain competitive. This eliminates the necessity for businesses to obtain/maintain these tools themselves. Likewise, it lowers other costs associated with managing your own systems, such as accrued man hours or consulting fees.

Conclusion

Business databases, while a completely indispensable tool for data management, pose a complex problem in the terms of cost, compliance, and security. With the growing threats of cyber-criminal activity and the cost incurred in the event information is lost or stolen, great care must be taken to ensure the integrity of crucial business information and confidential consumer data. Database Management System technology can ease some of the burden by automating key processes, yet they require attention of their own. DBMS facilitate nearly every aspect of daily operations, and therefore require an in-depth strategy for support to sustain their integrity.

Afterword

KG Hawes Technologies utilizes remote database administration solutions, around the clock, which allows your business to focus on its core competencies while maximizing cutting-edge technologies.

Our database administrators are highly trained and certified in all major database platforms. In addition to continual monitoring, our database administrators will also conduct periodic, comprehensive analysis to look for issues that could impact stability or performance. Our database services are both highly responsive and cost effective, In fact...

We offer our clients a flexible service plan that guarantees they only pay for the service time used.

DB MANAGEMENT SERVICES	PREVENTATIVE SERVICES	EMERGENCY SERVICES
▪ Application Tuning ▪ Database Tuning ▪ Memory Tuning ▪ Disk I/O Tuning ▪ Full Audit of Role-Based Security ▪ Process Tuning	▪ Database Alert Logs and Traces ▪ Storage Related & Schema Object Alerts ▪ Database Audit Alerts ▪ Resource Utilization ▪ Alerts from Maintenance Jobs ▪ Round the Clock Monitoring	▪ Performing Database Crash Recovery ▪ Repair Corrupted Databases ▪ Recover Lost Data ▪ Reestablish Connectivity ▪ Performance Improvements ▪ Assistance on Emergency Hardware ▪ Configuration

KG Hawes
Partners in Technology

developed by **KG Hawes**
400 International Way, Suite 300
Springfield, OR 97477
(866) 687-9006
www.kghawes.com
sales@kghawes.com

References

1) CyberEdge. (2019). 2019 Cyberthreat Defense Report. Retrieved August 21, 2020, from https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf
2) Dark Reading . (2019, June 13). SQL Injection Attacks Represent Two-Thirds of All Web App Attacks. Retrieved August 21, 2020, from https://www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-two-third-of-all-web-app-attacks/d/d-id/1334960
3) Cheng, A. (2013, December 19). Target admits 40 million cards are compromised; TJX's 2007 breach cost $256 million. Retrieved December 06, 2017, from http://blogs.marketwatch.com/behindthestorefront/2013/12/19/targets-card-breach-delivers-a-rude-christmas-surprise/
4) Armerding, T. (2017, October 11). The 16 biggest data breaches of the 21st century. Retrieved December 06, 2017, from https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html
5) Gallagher, S. (2016, February 17). Patients diverted to other hospitals after ransomware locks down key software. Retrieved December 06, 2017, from https://arstechnica.com/information-technology/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/