International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 2, Issue 1, January-March, 2023, Available online at: https://ijmirm.com

Evaluating the Effectiveness of Database Security Processes and Methodologies

Osama Abdullah Badaghaish[1], Mohammed Muidh Alrasheedi[2], Faisal Ali Almutairi[3], Ahmad Eid Aldhafeeri[4], Mohammed Mahyur Alanazi[5], Salim Barkah Almutairi[6]

[1,2,3,4,5,6]Network and Database Security, Trainer, Programming and Web Development Engineering at Hafr AlbatinTechnical College TVTC Saudi Arabia

ABSTRACT

The research is based on looking within the larger context of computers and databases and then taking a step forward in understanding effective security methods and protocols. Database security is one of the important components that all databases today should have when looking at threats that could either be internal to that database or external. Security is often one of those things that is given paramount attention but the role of the people cannot be underestimated. There are also a number of such security methods and the ways in which they could be implemented on time. When database security processes are being designed and implemented, three important aspects have to be considered which pertains to information security of the larger database, confidentiality and integrity Therefore, the goal here is to ensure that there are the right measures put in place that are then needed to protect the very confidential data and information sets housed within that firm's database. In addition to that, the focus here also is on ensuring that other elements and sub features of the larger database structure are also covered and protected and these include both the actual hardware and the software that is used to run the given database. The goal of this paper was therefore to pick and select some of these important yet practical database security strategies that could be implemented in a small sized organizational environment. These included the use of access controls, having right encryption of the data sets, database auditing processes, as well as segregation of duties and management tasks within the database environment.

Keywords: Data security, network, risks, processes, control, environment, structure, information, security methods, protocols, methodologies, Data integrity, Accessibility, physical limit, hardware, confidentiality, authorize, accuracy, vulnerabilities, security policies

Objective:

The objective of this comprehensive project is to look within the larger context of computers and databases and then taking a step forward in understanding effective security methods and protocols.

There was a time when firewalls were considered one of the central modes of security protection.

But with the rise of both internal and external threats, other security methods have evolved such as user login/authentication, as well as database and server based security.

The scope or the main aim of this research subject would be to look and evaluate some of the more widely used database security processes and methodologies out there and see which ones of these could be more effective and workable.

Project Plan:

The project plan here would be to understand that there are a number of deliverables and steps as part of the larger research that have to be completed.

There is therefore, the need to know how that time would be divided within the accomplishment of these different projects. The balance of time and the research materials would come to determine how effective the project research progress would be. The table here shows the different sections of the research, the anticipated time for them and the level of effort that needed to put on in their successful and on time completion:

Type of Deliverable	Anticipated Time	Anticipated Effort
Working on the Literature Coverage	This is a very important step and around 3 weeks are to be anticipated here. It consists of gathering information pertaining to database security methods from credible online sources, recent book based publications on the topic as well from accessing articles pertaining to the subject.	A lot of effort would be spent on this part of the project which consist of not only gather ample research materials but more importantly those that are considered to be directly applicable to the subject matter and those that are also recently published rather than outdated
Working on the Project Report	This is the most important deliverable of the entire research report. Hence, It is anticipated that 50% of the time would be geared or given to the completion of the project report. This could translate to around a month spent on this part	This is also one of those deliverables that would consume a lot of effort and time. After all of the necessary research materials have been gathered and accumulation of the , most relevant and the most up to date materials is done. Then the actual process of the report drafting will be initiated.
Project Conclusion and Project Presentation	1 Week	It is anticipated that some effort would also be spent here. The creation of particular of a presentation that would capture the most important and interesting aspects of the research. Once that is done, then the project conclusion will also be worked on
Project Retrospective	2-3 Days or slightly more	The goal here would be to go over the entire project and see the major lessons learned and how the knowledge of IT has been very helpful. So some effort would be needed pertaining to analyzing the own knowledge and how it helped to fulfill some of the deficiencies that might otherwise have existed
Final Edits	1 Week	A week would be devoted in making all of the final edits to the research before it is presented and submitted

Literary Coverage:
It is often seen that the quality of our own research is often based on the quality but also the diversity of the resources that we have utilized. In that regards, the two goals that need to be accomplished out of the literature coverage is that of ensuring that have a good mix of sources (credible scholarly articles, updated books, online credible sources and so forth) pertaining to database security methods. Thereafter, it is assured that there might not be the overly focus or emphasize one type of resource versus the other. The goal here would be to have some balance in the variety and the extent of the different sources used pertaining to database security.

Likely Outcome:
The likely outcome here would be to present those results that come to coherently show the most applicable database security tools of today. Therefore, in order present findings which demonstrate on one hand that database security is a very important methodology to have but also to show that there are different ways of implementing such security. Therefore, the hope here is to come up with analyzing different types of database security processes and methodologies that are used and how well they come to create effective security for a given database system.

LITERATURE REVIEW

So far and in regards to this topic of effective database security, there have been a number of quite interesting books. In selecting such books, one of the main areas of focus was to see what is the sort of relevancy of the information that is presented in them and how they could pertain to database security as well. Without any doubt, there is the need but at times also the challenge to know or figure out how a database environment whether simple or complex could be made secure. But there are also a number of such security methods and the ways in which they could be implemented on time. One of the authors that takes us in detail regarding database security and the ways in which some issues have to be addressed is

Hassan Afyouni and his book called "Database Security and Auditing: Protecting Data Integrity and Accessibility". In this book, the author notes that security is often one of those things that is given paramount attention but the role of the people cannot be underestimated. In other words, we often might associate security with good firewalls or login and authentication measures, but at the same time it is the people who have to create the "physical limits" (Afyouni, 2005, P. 26) in terms of how has access and who doesn't. The author also presents a good listing of the different networks, operating systems as well as the applications that could also benefit from different types of security methods as well. This would be one of the books that is frequently referred in the research.

Another great book on database security is by author Ron Ben Natan and titled "Implementing Database Security and Auditing". In this book, the author also makes note of the notion that on one hand, there is the challenge to have a higher level of data assurance as a result of different security protocols. But then there is also the additional challenge of knowing what are the right auditing processes that could also be implemented. The author then notes that when different security methods are being put into place, there should be more emphasis on an "enterprise security" basis per which it would be easier to have a holistic type of security on the different components of the larger IT infrastructure of the organization (Natan, 2005, P. 35-36). Therefore, this would also be a book that must have used for the research.

The third book that would be analyzed and looked into is by authors Alfred Basta and Melissa Zgola and called "Database Security". In this book, the author also go in detail in terms of understanding how database security should be implemented around the larger database environment but also to look at ways in which security risks or security breaches could be reduced. The authors also consider the security testing and security auditing as two important means in which security performance could be enhanced in the database environment.

The fourth book that is looked into so far regarding database security implementation is by authors Michael Gertz and Sushil Jajodia called "Handbook of Database Security: Applications and Tools". This book also does a rather good and in depth job in to considering different techniques that could optimize security performance in the databases. The authors mention techniques like that of proper "authorization", or data "portioning" (Gertz and Jajodia, 2007, P. 196-197) as two of the key means in which database security could be implemented. Another source that have looked into and will be using is a scholarly article by author Meg Coffin Murray titled "Database Security: What Students Need to Know" (Journal of Information Technology Education, 2010). In this article, the author presents the notion that one of the most pertinent means of implementing database security is by having the right authorization and authorized users to deal and work on the data. In addition, the author also presents rather extensive information on a whole host of other database security techniques such as "grant", "access control", "row level security" and a number of others. So this would be a very valuable and in depth resource to use for the research.

Another great article that has been found on the topic of database security is titled "Making Database Security an IT Security Priority" by the SANS Institute (https://www.sans.org/reading-room/whitepapers/analyst/making-database-security-security-priority-34835). There are a number of great points addressed in this article pertaining to DB security such as having a comprehensive and holistic strategy towards a good database security but also ensuring that different controls have been put or implemented at the different levels for good database security. Another great book that have looked into pertaining to database security measures is by authors Parker Charles and Deborah Morley and titled "Understanding Computers: Today and Tomorrow, Comprehensive". There are a number of great points that the authors in this book also mention pertaining to database security such as that of knowing who has control of what resources or type of access. But in addition to that, the authors here again stress on the notion that database security at different levels isn't something that should belong to one person but to the entire organization.

Furthermore, another great book looked into pertaining to database security is by author Mullins Craig S and titled "Database Administration: The Complete Guide to DBA Practices and Procedures". The great aspect of this book is that the author has noted a sequence of actions that the database person or the DB manager has to implement to ensure a higher level of security. These actions include ensuring that specific user defined tables could be created so only those users have access to their information. In addition, the author also noted that focus should be given on the right "grant" and "revoke" permissions to different users. So this again would be a good resource for the research project.

Finally, two other great books that are looked at pertaining to by research topic are "Developing and Evaluating Security-Aware Software Systems" by author Khaled Khan and "Protecting Oracle Database 12c" by Paul Wright. The main message that both of these authors presents is that security could be breached for a number of reasons and that's why having a multi layered security approach is very beneficial. Furthermore, the authors also make the case that there should always be a focus on performance in terms of where security might be weak and what could then be done in terms of taking the right steps to improve it. So these are the sources that are considered so far for the research.

Research Findings: Effective, Dependable and Reliable Database Security Strategies:

I-Important concepts within database security:

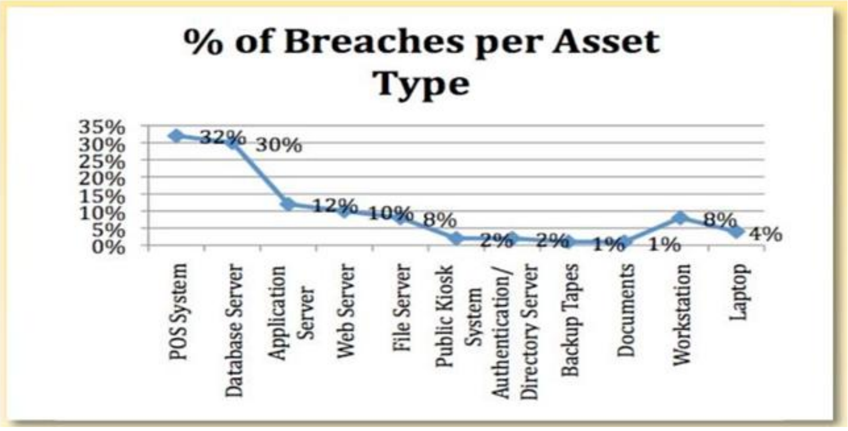
In terms of trying to narrow down the scope of the larger topic of database security, one of the important areas of focus could be on trying to understand, assess and then analyze some salient and reliable database security measures. Database security by its very self is a topic that concerns both small and larger corporations in the public and private sector who have employed some type of an in-house database platform. In that context, these organizations and corporate individuals also have to make the very important determination that leaving their database unsecure could pose a number of short and long term dangers and hence, it is more important that effective but also workable database security processes could be implemented on a timely fashion.

At the heart of all of this lies the fundamental notion of what database security is. Database security itself could be categorized as the “degree to which data is protected from tampering or unauthorized acts” (Afyouni, 2005, P. 3); hence, this effective definition comes to make the point that creating the necessary layers of database security should be one of the most important tasks of firms using them. What also cannot be denied is the very fact or notion that almost every other entity or organization uses database in some capacity or fashion and hence, the reliance on databases also cannot be denied.

This is the very reason as to why it should be considered that “database is a core component in today’s most commonly used system architecture” (Afyouni, 2005, P. 6). Such databases themselves could be from very small, linear and easy to manage ones to those that are bigger, more comprehensive and cover all of the departments of the larger enterprise. When database security processes are being designed and implemented, three important aspects have to be considered which pertains to information security of the larger database, confidentiality and integrity (Afyouni, 2005, P. 6).

In terms of the information security principle, the goal here is to ensure that there are the right measures put in place that are then needed to protect the very confidential data and information sets housed within that firm’s database. In addition to that, the focus here also is on ensuring that other elements and sub features of the larger database structure are also covered and protected and these include both the actual hardware and the software that is used to run the given database. The second principle here is that of confidentiality and the premise here is to ensure that only the authorized personnel of the firm have access to the database information but also ensuring that such very confidential information is also discussed to the authorized personnel of the firm. The third principle here is that of integrity which focuses on ensuring that the data being entered into the database is correct, accurate and of a consistent nature since the end output of that data would be dependent on the input that has been entered. This itself is often based on the important premise that “garbage in, garbage out” (Afyouni, 2005, P. 11) and therefore, those personnel who are working with entering different datasets into the data tables, records and fields have to double check on the correctness and the overall accuracy of the data being inputted.

Therefore, what has to be analyzed and considered here is that security vulnerabilities are a big issue not only to the databases that are utilized by corporations but also other types of IT assets. The following chart comes to show the percentage of security threats that have taken place on the different classifications of computer assets, both on the hardware and the software side (Making Database Security an IT Security Priority, SANS, P. 3).



From this chart, it could be seen that it is often the database servers that seem to have a high rate of breaches (around 32%). That itself then sends the message that it would be prudent to enact and implement different effective database security measures and policy action plans.

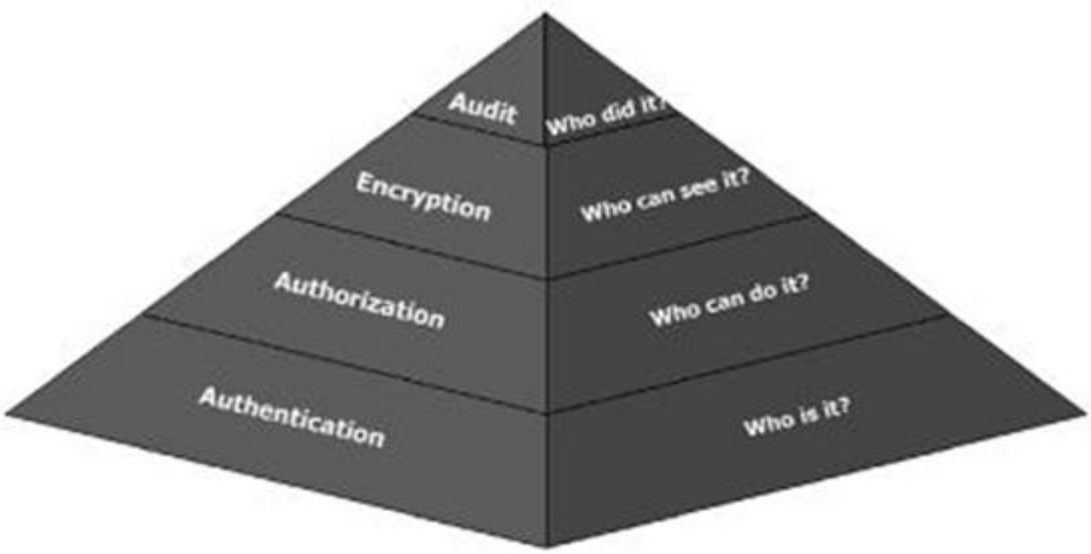
This is where the important consideration or viewpoint comes which is that it should be the top responsibility of the corporate management to understand the nature of database security and then being able to employ right security policies. As such, what should therefore be considered is that "database security must become a management priority" (Making Database Security an IT Security Priority, SANS, P. 5).

When management comes to realize the nature and implications of how things could go wrong without a solid database policy in place, then there would be more incentives for management to know what security methods, rules and action plans to employ. Some of these security strategies include the use of (Making Database Security an IT Security Priority, SANS, P. 5):

1. Various firewall structures
2. Intrusion Detection Systems (IDs)
3. Having effective controls on the operating system that houses the database
4. Having larger access controls around the database itself

Hence, the point to consider here is that database security should be given a top level priority by the firm and its different departments. Since a lot of the corporate data (which often is very confidential in nature) resides in such data, it then becomes important to assume that database security should be part of the company's overall "strategic plan" (Making Database Security an IT Security Priority, P. 6). The implication of this is that there are databases have often been targeted by outside threats and they are also considered to be "one of the top compromised assets" (Making Database Security an IT Security Priority, P. 6).

As such, it should be made imperative to the top level management that the more effective security processes and controls that they implement, the easier it would be to protect the database assets but also to prevent any attack to take place. This comes to show that there should be full yet comprehensive support of the management to be able to gear more focus at database security management but also at knowing what types of database security tools could work better than others. The goal here is to have a rather comprehensive database security model, one which is able to implement data authentication, data authorization, data encryption and data audit as depicted in the following graph (Nata, 2005, P. 96):



The critical point to consider here is that database security should be on the top list of organizations heavily dependent or reliant on them especially smaller sized organizations that might have one centralized database environment. In such an environment, what should be considered is that databases are considered the main tool of work productivity since employees from all layers and levels of the management access them on a daily basis. But there are also a lot of facts and statistic out there to suggest the different types of threats and vulnerabilities around databases and that itself makes it rather critical that such organizations are able to have the right tools in place for DB security. For example, a report by the Privacy Rights Clearing House back in 2010 noted that in excess of 345 million customer records had been stolen or hacked into since 2005 from different databases ((Murray, 2010, P.2). This really comes to show the level of insecurity that could be found around such databases if they aren't properly configured or managed.

In addition to that, it isn't only the reputational costs that a small or a large organization suffers from in the face of data theft from their databases but also the immense financial costs. According to a report by the Ponemon Institute, the overall cost of data breach theft has now gone up to $202 for a given customer here in the United States, another fact to suggest the need to have very tight and strict but reliable database security strategies for centralized databased often used by small organizations (Murray, 2010, P.2).

One of the other very striking facts is the very notion that most of the data breaches themselves took place by using "hacking" and "malware" attacks and such attacks directed at the "database owner" (Murray, 2010, P. 2). Hence, the premise here is the ever growing need to have the best and most reliable database security management system in place especially for small firms that rely on centralized databases which could lead to very negative consequences in case of a data breach on them due to the central storage of all customer data.

II-Database security for cloud databases: An emerging DB trend

Among the different types of databases that have been used so far such as relational or object oriented databases, cloud databases are also becoming more and more popular especially among smaller firms due to their overall lower cost (Parker and Morley, 2014, P. 576). These days, almost every other firm uses the web for their work and productivity and that is where a database is also used to house all of that transactional information.

A very good example of this is the cloud database that is used by one of the largest online retailers Amazon.com where it is able to store information about its potential clients but also all product related information as well. But within smaller sized firms, the use of cloud databases is also cost effective and practical as they provide a lot more storage capacity but also make it easier to retrieve any data that might be housed there. Such cloud based services are often based by using the infrastructure of a third party like that of Google Cloud SQL or Windows Azure; however, the point is that they are a great way to store a lot of information and also having access to that data (Parker and Morley, 2014, P. 577). Again, the importance of having right, reliable yet adequate security measures comes to play in the use of such cloud databases in addition to having an effective "recovery plan in case of a disaster" (Parker and Morley, 2014, P. 577).

II-Most common security threats and risks to databases

The focus here is on small to medium sized databases in firms that might not have a huge budget dedicated to having the most advanced security features in place. It is often the larger sized firms that might have the capital budget in place to house the best security techniques, methodologies and practices.

Therefore, the most vulnerable databases are those of smaller firms such as small businesses or small corporations who do understand the different risks and dangers posed to their databases and hence might put in place an incremental approach of adding different layers of security management as their financial budgets permit them to do so. In that perspective, there are a number of vulnerabilities, threats and risks that these small sized databases might encounter and could be listed as (Afyouni, 2005, P. 19-30)

- Threats from different viruses, bugs or worms: These are often threats that come in the form of malicious code that could cause damage to the database software and bring the operations of the firm to a halt
- People related risks: These are those types of risks that are encountered when people in charge of maintaining and overseeing the database security of the firm leave the corporation for one reason or the other. In such an instance, it then becomes important to bring in a security expert in a short span of time
- Data and hardware risks: These are those types of database risks which could lead to the database hardware not operate as expected or one where some of the data might be tapered or be lost
- Confidence related risk: This is that type of a risk where the firm might be involved in data theft or data loss and has failed to take the right remedial steps in improving its database security capacities or giving safety assurances to its clients. In such instances, clients as such end up losing both the trust and the confidence that they otherwise had put in the firm and might take their business somewhere else

III-Important database security components that should be protected:

Companies using databases often put in place a whole range of security methods and protocols to ensure that if one security method or protocol might not work, there are a number of other layers of security in place. But at the same time, what also has to be considered is that there are a number of such components that are connected with database security and hence, such implemented security layers should also be able to protect and safeguard these different DB components. Some of the most prominent of these database security components that should be protected include the following (Afyouni, 2005, P. 26-30):

People: The focus here is to ensure that there are the right security mechanisms in place to protect and safeguard the different types of information belonging to the different personnel and people of the corporation. For example, a particular database might be reserved for a given person and therefore, it is important to check the credentials of a person purporting to be that person to ensure that the right access is being given to the right person.

Different types of applications: The other equally important component of database security is the different applications that might be residing on it. This is based on the notion that there often are multiple applications that might be housed on a particular database and hence having the right rules and methods of access is imperative to those applications

Network: This by its very self is one of the most critical components of the larger database enterprise architecture. This is because the more protected the network is, the easier it would be to detect and then block any vulnerabilities, threats or risks that might be incoming. At most times, firewalls are considered as the most practical but also cost effective measure to protect the database network and to detect any sort of vulnerabilities that might be found. At times, firms also employ different types of authentication measures on the given database network to ensure that authorized users will be given access to it

Operating system environment of the given database: There often are multiple users at the organization working with and having access to the given database. Therefore, such an operating system should ensure that it is able to give access to those personnel who are designed to use the given database. In having better level of security to the operating system on which the database operates, it should also have effective and stringent password mechanisms and intrusion detection systems as well. In that regards, the users of that database environment should be able to know that users of that database should be changing their passwords on a periodic basis for additional security measures.

Database management system: This is yet another important component of the larger database environment. Here, the focus is on having reliable authentication measures that would ensure that database access is granted after the person’s credentials are fully checked, verified and hence authenticated. A lot of this database management security policy could be based on knowing what the password policy is there for, but also ensuring that there is right protection of the larger database system itself.

Files within the data: One of the most important and strategic elements for the organization is the information and the files that are housed in the given database environment. In that context, what we come to see is that there is the need to have a number of file permissions to ensure that there is a heightened level of security that has been embedded into the system. But at the same time, what also has to be considered is that there should be multiple layers of security in place such as having the right monitoring of who is accessing the different files, when such files might have been accessed and so forth. However, it is also the actual data of the database system that should be protected at all times due to its proprietary value to the larger corporation. Therefore, there should be a number of additional security measures in place to protect that data files in the database. This could be achieved by having proper (1) data encryption (if such a possibility is made available to the database environment), (2) proper data access to those who are entitled in using that database as well as right (3) data validation mechanisms in place.

IV-Effective, Reliable and Dependable Security policies for small sized databases

The core focus of this research is to look at and evaluate some of the most effective, reliable and dependable security policies that could be implemented. In that perspective, the scope of this research is to consider small sized databases such as Oracle or Microsoft supported databases and then seeing most of the most reliable, dependable and effective security methods and policies that could be put in place. Hence, the following research would be directed at understanding and analyzing a variety of security policies for smaller sized databases that could provide a high level of data confidentiality, security and integrity.

I-Provision for having a required access control:

One of the most salient security policies for enhancing database data security is having some type of a "mandatory access control" (Jajodia and Gertz, 2007, P. 6). When such a required access control policy is created, it then ensures that there are uniform "regulations mandated by a central authority" (Jajodia and Gertz, 2007, P. 6). The main benefit of such a mandated policy is that it would then be applicable and enforceable on all tiers and layers of the corporate management such as the top, middle and the lower level management. The research indicates that among different types of mandatory access control policies in place, one of the more widely used one is the "multilevel security policy" (Jajodia and Gertz, 2007, P. 7).

This is a policy which comes to ensure that there are different types of "access classes" that are created within the larger database and after that, different types of "security levels" are then also put in place. Therefore, one might consider that some of the more confidential and highly secure data might have more restrictive access policies versus other tables, fields or records that might be storing more general datasets.

All of this is based on the very premise that data security itself for small firms that might not have a lot of other sophisticated means to protect their database could simply be to having a policy of "limiting access to data" (Murray, 2010, P. 3). This particular provision itself could be done by instituting a policy which is able to have the right (1) authentication of the users having access to that data, having the right (2) authorization and also having the right (3) access control after the first two steps have been fulfilled (Murray, 2010, P. 3).

When such policies are being created and instituted, it is important to consider that different types of "database security gaps" could be identified early on so that remedial steps could then be followed (Khaled, 2012, P. XX). This is a very important consideration because no matter how many security methodologies might have been instituted, there could still be that risk or the inherent policy of having a number of security loopholes or gaps in place that should be considered and evaluated. In going with this discussion that pertains to having right levels and types of access controls, there are a number of reasons as to why a small sized corporation using a database could benefit from it.

One of these is the very notion that such access controls are able to protect the database both from "external and internal attackers", because at times, the imminent danger to the database could come from an internal employee who might be upset about something. Furthermore, what can also be considered is that access controls also are a remedial tool in protecting the larger database system from different types of mistakes on part of the users (Making Database Security an IT Security Priority, SANS, P. 7). When an organization considers the use and full implementation of access controls, they also have to consider that such access controls should be placed on both the database "administrator" but also on all of its "end users" (Making Database Security an IT Security Priority, SANS, P. 8). This is a very important point to consider because it protects the database from all users who are directly interacting with it. What has to be considered from a technical point of view is that for databases that are often used by small or medium sized organizations, they are often based on SQL objects and with that allow the users to perform a number of functions.

Such functions related to their data include being able to read and select particular data, being able to add new data, update existing data, but also being able to delete old or redundant data. When such actions are performed, there could also be different users in that organization having different types of data privileges which is yet another thing to consider in securing the database environment. Such effective access control could take place when three important steps are followed which include having a (1) mandatory access control, (2) having proper discretionary access control and also having (3) role based access control (Murray, 2010, P.4).

All of these are mans of securing different records, tables and data elements of that particular database. When such different types of database rules are created, it is important to consider who in the management hierarchy should be given what type of a privilege. In other words, there should be a means to know who should be given what type of grant access to different parts of the centralized database. For example, once a user at the firm has been identified to be given a high privilege (such as a top level manager), the following is an example of how a technical rule could be created in allowing that access (Murray, 2010, P.4):

```
"GRANT privilege_name
ON object_name
To role_name;"
```

In defining such roles, it again is important to consider what data rights and access privileges have been given. However, there should be focus on full implementation of different types of access control since a threat to the database environment could come from any side and at any time. The very fact that the database system houses a lot of very confidential information about the company, it is the use of such access controls which ensure that the database administrators have access to only those data files and tools that are needed for their day to day job.

What we can consider here is that for smaller sized firms, there often aren't a lot of database administrators and so, it would be easier to manage the different access controls and how they have been created to implement the higher level of security. As mentioned earlier, such access controls aren't only created to prevent different types of attacks or incidents that might happen but also to protect the system from any sort of unintentional errors or mistakes that the database administrator might do.

Therefore, proper, workable and effective database controls can ensure that it could "minimize the impact of errors and security incidents" (Making Database Security an IT Security Priority, SANS, P. 8). In addition to these points, one of the other associated recommendations for small sized databases is that they should be managed by some "centralized management" because such a methodology can ensure better and more efficient management. In addition to that, centralized management is a more rational option for small sized firms as they simply might not have a big budget to have different layers or levels of management to oversee the larger database enterprise nor the personnel needed for such an effort.

II-Use of Encryption within the database:

Another effective security strategy that a small to medium sized database can implement is the use of encryption. This is based on the reason that at times, encryption is considered to be one of the most reliable, dependable and a "strong security tool when implemented correctly" (Making Database Security an IT Security Priority, SANS, P. 9). When database encryption is implemented, the management again has to realize the fact that this is not a solution that could alleviate or solve all of the security issues or problems both internal and external but at least, is an important pillar for good database security management.

Such encryption of database security itself should be based on securing the data which is considered to be "in transit" as well as the data that is "at rest" (Making Database Security an IT Security Priority, SANS, P. 9) or one which resides inside the database system. By encrypting the data, it would then ensure that this set of data will be in a secure state when it travels through different types of interconnected networks. If such data leaving a database isn't properly encrypted, then a big fear could be that someone might be able to "sniff the network traffic" and then have access to the proprietary details of that network (Making Database Security an IT Security Priority, SANS, P. 9). A good example to illustrate this situation was when TJX became a victim of a big data breach back in 2006 when its customer credit card and related sensitive data was sniffed.

There are a number of effective encryption tools that these small to medium sized databases could employ such as that of (1) SSL tools, (2) SSH tools or the use of (3) IPsec tools (Making Database Security an IT Security Priority, SANS, P. 9). The same process should also be employed for the data that is at rest and therefore, that data which is residing within the firm's database environment. The premise here is that such stored database should be encrypted which could then enable to add that additional layer of security into it.

III-Use of auditing within the database:

In this focus on looking at and evaluating the different types of effective but also reliable database security strategies for small businesses, one of the other important tools that is used is that of auditing. In that regards and for small sized organizations, it becomes important to have that process of checks and balances in place to know how had access to what part of the database, what information might have been changed but also knowing what sort of access has been given to the different users of the database. The goal here to consider is that the central feature of using database auditing is to enable the small organization to "track database access and user activity" (Murray, 2010, P.14).

What also has to be considered here is that data audit isn't a direct means of preventing the onset of data breaches, but at least they are a measure to "identify if breaches have occurred" (Murray, 2010, P.14). For small sized organization, that could be an important tool to have so that if a breach can take place, they could understand how that breach happened, what were some of the underlying circumstances that might have enabled that breach and therefore, in the future, what sort of more proactive processes and steps could be taken to mitigate the occurrence of a similar breach from taking place (Murray, 2010, P. 10).

For smaller sized firms, they simply might not have the financial budget to be able to install very sophisticated security tools but also not having the financial resources to overcome a security breach that could potentially take place. Therefore, to minimize and reduce the risk of any type of security risk or threat to occur that could have long lasting financial repercussions, the use of "audit trails" is one of the most effective, dependable and reliable security toolkits for these smaller sized organizations (Making Database Security an IT Security Priority, SANS, P. 10).

In terms of the use and implementation of such audit trails, what should be considered is that they should be able to work with the actual business environment of the firm, but also being able to "track user activity". The tracking of this overall user activity shouldn't only be restricted to the different employees or the management of the small organization but also the person who has been given the role of the administrator.

That is very important to consider because at times, there could be the possibility that the administrator might end up abusing the system privileges that might have been assigned to him/her and hence, it is important to know that such audit trails have been created for the entire management of the organization. For these smaller sized organizations, there could be a number of pertinent activities that should be part of the audit trail process and some of these include the following (Making Database Security an IT Security Priority, SANS, P. 10-11):

- Being able to have a continuous policy of monitoring the administrative activity
- Being able to know when the users are logging on and logging off to the database system
- Being able to know what sort of system privileges the different users might have used
- Being able to know what sort of alterations or changes might have been made to the data and by which user such changes were done
- Being able to know when some of those data resources of the database might have been accessed

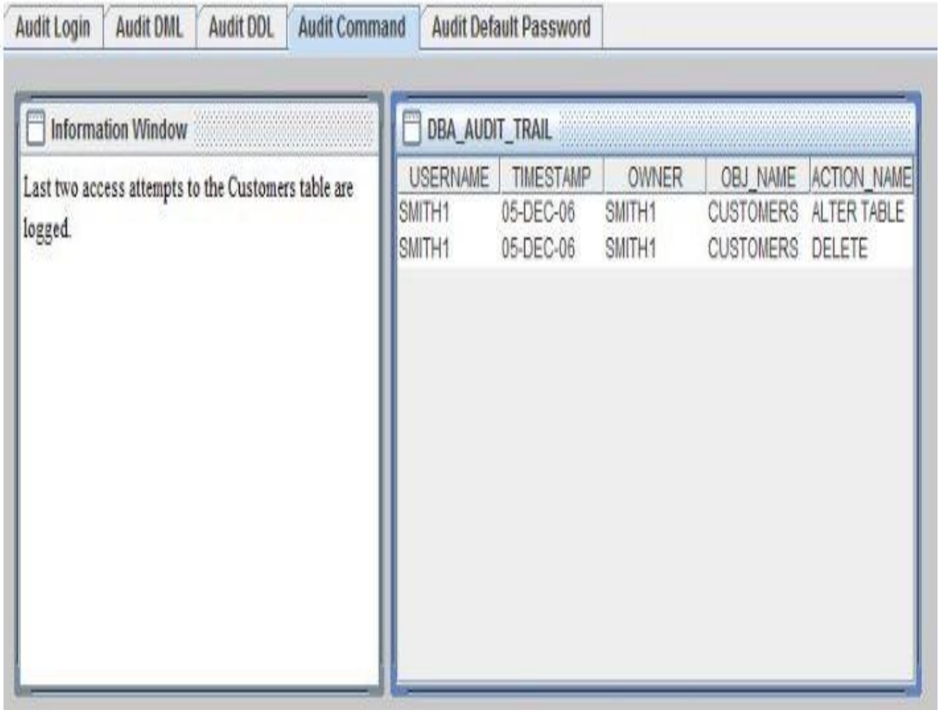
Among different types of audit trail tools that are found in the market, one of the more cost effective tools suited to the needs of smaller sized organizations is "Fine Grained Auditing" or also referred as FGA. This is an audit tool where a number of predefined conditions have to be programmed and then it would oversee and continuously monitor such activity and then being able to generate customized reports for the management as well. For these firms, it is very important on one hand to be able to know how the audit process is being monitored but what is also important to consider is how and where such audit information is being stored. There are just so many different types of database attacks that could take place and hence the more prepared that the firm is, the easier it would be to have the right detection and correction practices in place such as audit trails. For example, besides the use of data hacking as one way to target a database, "SQL injection attacks" is another threat on the right for database (Mullins, 2012) Therefore, it is important to have the right detection and prevention strategies at all times. SQL injection attacks is that type of an attack where some SQL statements are made which are then send to the database to "perform certain functions" (Natan, 2005, P. 150). Therefore, if and when that connection has been created between the database and the outside attacker, the "database becomes the target of the attack" (Natan, 2005, P. 150).

This is important because there should be some audit trail repository where all of that audited information has been created and stored and so would be accessible to the management whenever such a need might arise. The recommendation for smaller sized organizations is to use Oracle based database environments which are easy to operate, users can be trained in a short span of time and they also provide the ability to store the audit trail information. One such Oracle tool that provides the audit trail secondary storage facility is "Audit Vault" (Making Database Security an IT Security Priority, SANS, P. 11).

When database auditing processes and procedures are being implemented, what should be considered is "how much data to retain and how much to keep it" (Murray, 2010, P.14). This is an important issue to consider because for smaller sized organizations, they simply might not have a big enough budget to oversee a lot of the historical data nor store it. But at least, what effective and overseen data audit trails do is that they are able to have a "complete trace recording of user access and user actions" (Murray, 2010, P.14). Therefore, this is a way for the administrator to at least be able to find what went wrong based on actual data at hand. Some of the most important data audit items that are considered include some of the following (Murray, 2010, P.14):

1. Knowing how many login attempts by a user might have taken place
2. Knowing what type of data read operations might have taken place
3. Knowing how many unsuccessful attempts by a user accessing a given data table took place
4. Knowing what sort of data additions, inserts or modifications took place which violated different constraints that the data administrator might have imposed on that database

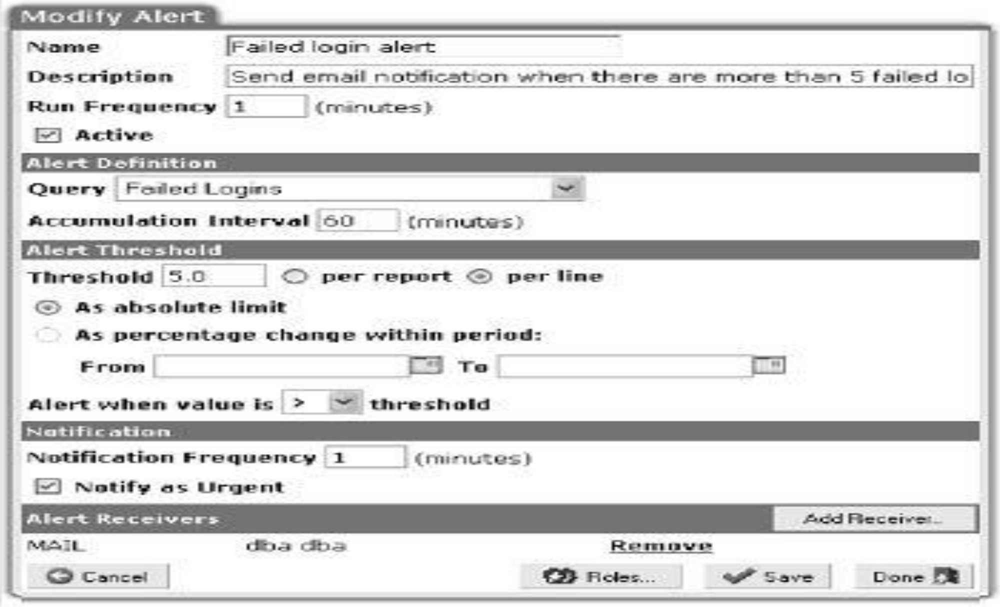
The following screen shot presents data that has been accessed from the data trail and the type of data (Murray, 2010, P.15):



Last two access attempts to the Customers table are logged.

USERNAME	TIMESTAMP	OWNER	OBJ_NAME	ACTION_NAME
SMITH1	05-DEC-06	SMITH1	CUSTOMERS	ALTER TABLE
SMITH1	05-DEC-06	SMITH1	CUSTOMERS	DELETE

If and when there might be a lot of incorrect logins that are taking place to the organization's database that could suggest some suspicious activity. A user might stop logging to the database system after a couple of tries with the assumption that they might have forgotten their username or password combination. But if someone keeps trying to login to the system using different combinations, then that should send more like a red flag that this user might be accessing the database for which they might not be authorized to or the user simply doesn't have the privilege to access that database. That is where one of the security techniques that could be created is the use of an alert system that would send an email to the database administrator that someone has gone over the login limit and so that issue should be looked at. The following is an image showing an alert system that sends a message to the database administrator in case of excessive login attempts (Natan, 2005, P. 116).



Name: Failed login alert
Description: Send email notification when there are more than 5 failed lo
Run Frequency: 1 (minutes)
☑ Active
Query: Failed Logins
Accumulation Interval: 60 (minutes)
Threshold: 5.0 ○ per report ● per line
● As absolute limit
○ As percentage change within period:
From: To:
Alert when value is > threshold
Notification Frequency: 1 (minutes)
☑ Notify as Urgent
MAIL dba dba

IV-Being able to have separate working environments

Another important database security recommendation to be given to smaller sized organizations is simply to create some sort of a policy that could allow for the separation of different objectives. The goal here is to know that the administrator shouldn't be given all of the database duties but there should be some level of separation and segregation of such duties. For example, the administrator might be given some of the more critical tasks of the database such as overseeing the entire environment, but a number of other duties such as database testing, or further database development should be assigned to someone else (Making Database Security an IT Security Priority, SANS, P. 11). By doing that, it becomes easier to know that one person might not have full-fledged access to all of the vital resources but it also helps to ensure that specific person at the organization have their specific duties and access to only those specific privileges as well. As had been seen earlier, when security policies and processes have been instituted, the goal is to have both "GRANT" and "REVOKE SQL statements" and that makes it more manageable to know who to revoke access to and who to give access to (Mullins, 2012).

CONCLUSION

What has been seen here is that effective and on time database security management is not an easy process or task to accomplish, especially for smaller sized firms with a very limited financial budget. But on a brighter note and within the backdrop of different types of data threats and risks (such as data sniffing, hacking, internal user threat), there are some notable, reliable and highly practical security strategies that can be implemented.

The goal of this paper was therefore to pick and select some of these important yet practical database security strategies that could be implemented in a small sized organizational environment. These included the use of access controls, having right encryption of the data sets, database auditing processes, as well as segregation of duties and management tasks within the database environment. 100% security might not be a very tangible or attainable goal but at least what could be done is to reach a rather high level of database security through the integration of these specified and researched tools so that the organization's management can rest assured that they are comprehensively protected against different types of threats that might be inherent in the larger database environment. What was also seen was that when database security methods are enforced, key focus should also be given to "data integrity, security and privacy" (Parker and Morley, 2014, P. 558-559). All of these are means that also come to ensure that accurate and concise data is housed in the organization's DB environment but also imposing the right data validation methods as well.

If the organization isn't able to check on the reliability and the validity of the data being entered, then it would end up making wrong or incorrect assumption and results since the entered data itself was inconsistent. But for firms using databases, it is also important to ensure that one different security tools as such provide different types of security measures. For firms that might be engaged in receiving and sending a lot of confidential and highly proprietary data, the use of "stronger encryption tools being integrated into DBMS" (Parker and Morley, 2014, P. 561) is one of the most effective approaches that they can take.

At other times, such organizations also need to ensure that they have a backup copy of the main data being used in case data loss takes place as a result of a hacking attempt. All of this itself is based on the firm ensuring that it has put into place some type of a "disaster recovery procedure" ((Parker and Morley, 2014, P. 561) which could then provide the necessary level of data protection based on the integration and the use of multiple types of data security tools. This research also considered the ever growing use of cloud databases for small organizations as an effective alternative to existing object oriented or relational databases. Even within those database environments, there is still the big need to have an effective, reliable and dependable security strategies in place in addition to having a recovery backup plan as well.

WORKS CITED

[1]. Afyouni Hassan (2005). Database Security and Auditing: Protecting Data Integrity and Accessibility: New York, Cengage Learning Press.

[2]. Jajodia Sushil and Michael Gertz (2007). Handbook of Database Security: Applications and Tools; New York: Springer Science Publications.

[3]. Khaled M Khan (2012). Developing and Evaluating Security-Aware Software Systems; New York" IGI Press.

[4]. "Making Database Security an IT Security Priority" (2009). SANS Institute, accessed from https://www.sans.org/reading-room/whitepapers/analyst/making-database-security-security-priority-34835

[5]. Murray Meg Coffin (2010). Database Security: What Students Need to Know; Journal of Information Technology Education; accessed from http://www.jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf

[6]. Mullins Craig S (2012). Database Administration: The Complete Guide to DBA Practices and Procedures; New Jersey: Addison-Wesley Publications.

[7]. Natan Ron Ben (2005). Implementing Database Security and Auditing; New York: Digital Press.

[8]. Parker Charles and Deborah Morley (2014). Understanding Computers: Today and Tomorrow, Comprehensive; New York: Cengage Learning Press.

[9]. Wright Paul (2014). Protecting Oracle Database 12c. New York: Apress Publishing.

[10]. Zgola Melissa and Alfred Basta (2011). Database Security; New York: Cengage Learning Press.