


2007

## **Network and Database Security: Regulatory Compliance, Network, and Database Security - A Unified Process and Goal**

Errol A. Blake

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

---

### **Recommended Citation**

Blake, Errol A. (2007) "Network and Database Security: Regulatory Compliance, Network, and Database Security - A Unified Process and Goal," *Journal of Digital Forensics, Security and Law*. Vol. 2 : No. 4 , Article 5.

DOI: <https://doi.org/10.15394/jdfsl.2007.1033>

Available at: <https://commons.erau.edu/jdfsl/vol2/iss4/5>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).



# **Network and Database Security: Regulatory Compliance, Network, and Database Security - A Unified Process and Goal**

**Errol A. Blake**

4192 Medlock River Court  
Snellville, GA 30039  
(678) 367-7170  
ErrolBlake@gmail.com

## **ABSTRACT**

Database security has evolved; data security professionals have developed numerous techniques and approaches to assure data confidentiality, integrity, and availability. This paper will show that the Traditional Database Security, which has focused primarily on creating user accounts and managing user privileges to database objects are not enough to protect data confidentiality, integrity, and availability. This paper is a compilation of different journals, articles and classroom discussions will focus on unifying the process of securing data or information whether it is in use, in storage or being transmitted. Promoting a change in Database Curriculum Development trends may also play a role in helping secure databases. This paper will take the approach that if one make a conscientious effort to unifying the Database Security process, which includes Database Management System (DBMS) selection process, following regulatory compliances, analyzing and learning from the mistakes of others, Implementing Networking Security Technologies, and Securing the Database, may prevent database breach.

**Keywords:** Information Technology (IT), Information Security (InfoSec), Database Management System (DBMS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes- Oxley Act (SOX), California Security Breach Information Act (CSBIA), Gramm-Leach-Bliley Act (GLB), The Fair and Accurate Credit Transactions Act (FACT Act), The Enterprise Information Security Policy (EISP), System-Specific Policy (SSP), Electronic Communications Protection Act (ECPA), SQL Injection, PCI Data Security Standard (PCI DSS).

**Categories and Subject Descriptors:** H.2 [Database Management]: Security, integrity, and protection K.4 [Information Security]: Management of Information. K.4.4 [Computers and Society]: Ecommerce and Security. K.6.5 [Management of Information Systems]: Organization Security, Policy and Protection.

**General Terms:** Management, Performance, Security, Legal Aspects

## **1. INTRODUCTION**

Information Security is a constantly evolving field; threats are increasing daily and regulatory voices are tightening their compliance standards. It can be easily stated that top level executives are sent to the guillotine after a security breach; especially when it is sensitive information being compromised.

Most data custodians face Information Security risks on a daily basis; thus, it is up to Information Security professionals to research these risks, threats, exploits and vulnerabilities and take the necessary measures to secure private information from unauthorized access and mismanagement. Upper level management is placing more accountability in the hands of its Information Technology department to protect sensitive information. Thus, it is assumed that IT has the privilege to protect the company's Information Systems. It may be safe to say that some people are confused with the term Information Security (InfoSec). Many believe that the term is associated with securing data communication networks. The term is often used interchangeably with information assurance and computer security. Information Security and Assurance and Computer Security, share the common goals of protecting the confidentiality, integrity and availability (CIA) of information; however, there are some subtle differences between them. The difference is stated in the following quote: "these differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration" (wikipedia.com, 2007). Whitman (2004) states that "businesses have become more fluid; the concept of computer security has been replaced by the concept of information security". Sometimes an individual uses the term Information Technology Security interchangeably with Information Security. Many Information Security professionals may find this misconception offensive especially when InfoSec is used inappropriately. To avoid any confusion, one may have to define Information security, and Database Security. According to Whitman (2004) "Information Security (InfoSec) is the protection of information and its critical elements including the systems and hardware that use, store, and transmit that information". Wikipedia gave an excellent definition and analysis of database security. Wikipedia's definition and analysis is the following:

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authorized misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. Database Security is also a specialty within the broader discipline of computer security [now information security] (Wikipedia, 2007).

The sources have given a clear concise definition of InfoSec and Database Security. One will have to conclude that these two definitions are somewhat similar. They are similar because they arrive at the same conclusion; they are unified in gaining the same outcome. The definitions conclusions are to protect

information from unauthorized access and misuse while the information is in use, storage, and being transmitted. One cannot rely on the Traditional Database Security alone to protect data confidentiality, integrity, and availability. An effort must be made to unify the process of securing data or information whether it is in use, in storage or being transmitted. Unifying the Database Security process, which includes DBMS selection process, following regulatory compliances, analyzing and learning from the mistakes of others, Implementing Networking Security Technologies, and Securing the Database, may prevent database breach.

## 2. LITERATURE REVIEW

### 2.1 Database Management System Selection. A Curriculum Development Trend

The three major DBMSs are Oracle, SQL Sever and DB2. DBMS selection is subjective. DBMS selection is simple; it depends on what you or your organization's needs are. DBMS solutions have advantages and disadvantages; it may be wise to compare these advantages and disadvantages with other solutions. However, Price (2007) states that there are *Pre-DBMS activities* one should consider. In a recent class room discussion or forum posting dated Monday, 19 February 2007, 10:07 AM, Price (2007) activities include:

- Does the proposed DBMS align with corporate strategic goals?  
Warren McFarlan's Strategic Grid and Henderson and Venkatraman's Strategic Alignment Model have been used extensively to support executive decision making processes.
- Has a business case been established for the proposed DBMS system?  
If so, who is the champion\sponsor and business analyst?
- How much will the DBMS selection process cost to the firm?
- Has a minimum or maximum range been established for (1) time to implement the DBMS and (2) procurement of a DBMS?
- What methodology will be used to manage the selection and implementation of the DBMS? Has a Project Manager been selected?
- Are the processes\activities to be supported by the new DBMS well-defined? Could these processes\activities be outsourced?
- Will the DBMS be a stand-alone, departmental, divisional or an enterprise solution?
- Does the firm maintain Lesson Learned documentation from previous software project implementation?
- When\who performed the last strategic review of the firm's IS infrastructure? Is the strategic review documentation available? Can the current infrastructure support the new DBMS?
- When was the last time that the firm's HR department performed a capability analysis of the firm's IS personnel?

Price, (2007) further states that “the answer to these pre-DBMS selection activities will provide valuable insight as to whether or not to use the resources of a consulting firm. Failure to understand the importance of such questions should serve as a red flag that management is not equipped to manage the design\implementation\maintenance of a DBMS system”. This is a subjective approach, but it makes sense. One will have to agree that pre-DBMS selection activities are needed when deciding on a DBMS.

After one has conducted their analysis or answered the questions to their pre-DBMS selection activities, one should then identify a model used to store, manage, and query databases. Ogbuji (2001) states “probably the most fundamental choice to make in the DBMS hierarchy is the model used to store, manage, and query databases. Besides affecting what software you need to acquire, this affects the very way you will think about the data, and can be a surprisingly hard choice to undo later on”. One will have to agree that the selection process depends on the model one uses, whether it is Hierarchical Model, Network Model, Relational Model, Object/Relational Model, Object-Oriented Model, Semi structured Model, Associative Model, Entity-Attribute-Value (EAV) data model, or Context Model.

Database Application, Design and Implementation courses have taught that there is a difference between the Database Model selected and DBMS that support that particular model. For an example Oracle supports Object-Relational Databases and Relational Database. However, most databases in the market are simply Relational. Therefore, it is important to keep in mind that DBMS selection depends on the Database model chosen, because not all DBMS support all Database Models. For the sake of this paper and argument, this paper will make reference to only Relational Databases in DBMS selection.

In today’s business environment relational database are the most popular. Relational databases are, of course, the current king of the hill in database technologies. This doesn't mean that more data is kept in relational databases than any other model. A brief reason why relational databases are popular is stated in the following quote. “Relational databases are wonderful for discouraging redundant data and for the speed of complex queries; they also have a huge number of tools and APIs to support them. They are best used in situations where a lot of records are being combined and cross-referenced to synthesize result” (Ogbuji, 2001). Ogbuji, states further that an example of where a lot of records are being combined and cross-referenced to synthesize result, “might be the production data of a manufacturing firm, where information about inventory, part specifications, personnel availability, costs, sales and supplies need to be thoroughly analyzed in order to make production decisions” (Ogbuji, 2001).

After a Database Model is identified and selected one should select a DBMS

that supports that model. Before a DBMS is selected one must consider the features the DBMS has to offer. Information Security professionals who love their craft may say that the security-related features of a DBMS is one of the most important features one should first consider and research. Ogbuji, (2001) strengthens the point made that one should first consider security related features of a DBMS. “Probably the most important general features to consider in your DBMS hunt are security-related. Consider how thoroughly the DBMS requires authentication from users and keeps an audit trail of the accesses” (Ogbuji, 2001). Again this paper stresses that the selection process is subjective. Other features are dependent on what the user or company needs and can afford. Mbutia (2007) stated in a recent class room discussion or forum posting dated Friday, 16 February 2007, 08:24 AM; that “the features to consider include:

- Future of the supplier and are they used significantly by others.
- Cost – How much would it cost to buy, and how much would support, maintenance and upgrades cost.
- Query language - what query language is provided, and can more complicated mathematical functions be defined.
- Scalability - Are the number of rows or columns limited and so forth.
- Data types - what data types are provided .
- Interfaces and APIs – Do they provide for example JDBC or ODBC interfaces? Also consider the APIs provided and in what languages.
- System resources – how much of the system’s resources does it require such as size of installation, and disk space.
- Security.

Depending on the needs of the organization, DBMS selection is an important factor and starting point for the unification of Regulatory Compliance, Network and Database Security. Again this paper stresses that these features are not listed in order of importance, but they are subjective. This paper agrees with Mbutia (2007) listing of features; however, for the purpose of this paper security should be first.

### **3. APPROACH AND UNIQUENESS**

This paper’s approach and uniqueness stems from the fact that there are cases where well known company databases were breached due to some form of hacking. Unifying the process of Regulatory compliance, Network and Database Security may prevent the increase of database breach.

#### **3.1 Corporate data breach**

It is often said that experience is the greatest teacher and one should learn from the mistakes of others. Recent corporate data breaches should raise a red flag to IS professionals. Knowledge of these data breaches provides professionals with

the information about the techniques use to access the database; then enable us to find proper techniques to prevent such a case to happen again. The journal article *A Case Study on How to Manage the Theft of Information* written by Robert M Polstra III provides an excellent overview of corporate data breach. Thus, the information required for the overview of this section is provided by his article. The cases are as follows:

**Case I: Citigroup**

In May of 2005, Citigroup lost computer tapes that were being sent to the credit bureau via UPS that included Social Security numbers and payment history information for 3.9 million customers. After this event, this New York based company has decided that it will start sending its data to the credit bureau electronically using encryption.

**Case II: ChoicePoint**

ChoicePoint has made more than 50 acquisitions since 1997 to make it one of the largest collections of personal data in the United States. ChoicePoint sells data ‘to clients doing background checks on job and loan applicants and conducting criminal investigations’. On February 16, 2005, ChoicePoint went public to tell 145,000 people that identity thieves may have gained access to their personal information including their Social Security numbers and credit reports. ‘Authorities believe it was the work of a group of people who used IDs stolen from legitimate business people to set up phony businesses that contracted with ChoicePoint for ID checks, Bernknopf (ChoicePoint’s spoke person) said’.

**Case III: Egghead.com**

Egghead Software was a company that opened in 1984 to sell computer hardware and software that grew to have more than 205 stores worldwide. Then in 1998 the company moved its business to the internet as Egghead.com. In December of 2000, Egghead.com stated that ‘a hacker has breached its computer system and may have gained access to its customer database’. Jerry Kaplan, Egghead.com’s co-chairman, stated that there was ‘no evidence’ to support that the database with the credit card numbers for its customer was stolen but, he also could not give confirmation that they were not stolen. ‘Egghead's inability to determine how many of it’s customers credit cards had been compromised may mean that the company does not have a real-time auditing system in place, said Paul Robertson, senior developer for security service firm TruSecure Corp. ‘If you don't know how many credit-card numbers you lost, you are giving a quick, blanket, worst-case answer--and then finding out what happened afterwards,’ he said.’.

**Case IV: New Jersey Crime Ring**

Bank employees for Wachovia Corporation, Bank of America Corporation, Commerce Bancorp Inc., and PNC Bank stole information on 676,000 customer accounts that are all New Jersey residents. It is considered the largest banking security breach in history by the U.S. Department of the Treasury. ‘The suspects pulled up the account data while working inside their banks, then printed out screen captures of the information or wrote it out by hand, Lomia (a New Jersey Police Detective) said. The data was then provided to a company called DRL Associates Inc., which had been set up as a front for the operation. DRL advertised itself as a deadbeat-locator service and as a collection agency, but was not properly licensed for those activities by the state, police said’.

#### **Case V: LexisNexis**

LexisNexis is provider of legal and business data. In March of 2005, LexisNexis announced that the information on 32,000 people was stolen. These breaches occurred at one of the subsidiary companies, Seisint Inc. Seisint Inc. was the company who was the provider of data to the Multistate Anti-Terrorism Information Exchange (MATRIX) system. ‘LexisNexis, which acquired Seisint of Boca Raton, Florida, in September for \$775 million, expressed regret over the incident and said that it is notifying the individuals whose information may have been accessed and will provide them with credit-monitoring services’. In this incident, hackers stole username and passwords of legitimate users to access the confidential information. In a statement, ‘Kurt Sanford, president and CEO of LexisNexis Corporate and Federal Markets, said that the company will improve the user ID and password administration procedures that its customers use and will devote more resources to protecting user's privacy and reinforcing the importance of privacy’. This security breach is very similar to the incident that happened at ChoicePoint who is one of LexisNexis's competitors.

Polstra (2005) cases show a trend. The cases show that the information that was stolen, were stored in some form of database.

#### **Supplemental Case: TJX**

On March 29, 2007, Messmer (2007) wrote an article in Network World magazine. The article entitled *UPDATE--TJX data theft called largest ever: 45.7M credit card numbers Security breach detailed in financial filing*. Details of the article are as follows:

TJX yesterday (March 28, 2007) disclosed in financial reports that at least 45.6 million credit and debit card numbers were stolen in 2005 and another 130,000 last year by hackers who have yet to be caught. According to Gartner security expert Avivah Litan, the volume of stolen data gives TJX the dubious distinction of being the biggest known victim of hacker-based



card fraud in history. 'This is the biggest card heist we've heard of so far,' said Litan, an expert in e-commerce-related security.

Earlier this year TJX publicly stated it had contacted law enforcement in December 2006 when it 'earned of suspicious software' within its computer systems. According to the Securities and Exchange Commission filing, since last December TJX has been working with the Department of Justice, the Secret Service, and the U.S. Attorney in the Boston office in a criminal investigation to nab the intruders. TJX also is supplying information to the California attorney general's office, the Canadian Provincial Privacy Commissioners, and the U.K. Information Commissioner, as well as to the London metropolitan police.

The TJX data-theft case was a targeted attack by hackers, who broke in through unprotected wireless LANs, and made their way through the TJX network to the controllers to set up operations inside the TJX network to capture card data. 'They basically used a program to just capture the data.' TJX said it expects to incur \$5 million in costs in connection with the computer intrusion. So far, customers don't seem to be scared off by the news. Net sales for the 2007 fiscal year at TJX were \$17.4 billion, up 9% over fiscal 2006.

Demographic and credit card information are normally stored in a database and in most cases, there is some form of DBMS application managing the database. The New Jersey crime ring case was different. In this case the data leak was internal; where employees or nefarious thieves rather, were unscrupulous in handling the accounts of others. They engaged in flagitious activities for their personal gain. Polstra (2005) cases are prime examples of why management or Information Security professionals must make a conscientious effort to secure their database whether it was internal, social engineering or an external forced entry; to ensure the confidentiality, integrity and availability of data. The cases stated above are a handful of many cases that raised eyebrows of data breach. The TJX breach is the largest ever and it is a wake up call for the IS/IT industry to rethink corporate security.

#### **4. PROPOSAL**

Along with DBMS selection there are other factors that play a role in the unifying the process of securing a DBMS. This paper proposes that taking these factors into consideration and complying with the same factors may prevent the increase of database breach.

##### **4.1 Regulatory Issues and Compliance**

Regulatory compliance plays a role in the Database Security as well as the selection process. Some regulatory organizations have minimum security requirements for Databases. There are some DBMS that has more security

features than others. The DBMS selection process may be affected by the passing of the California Security Breach Information Act (CSBIA) (SB-1386). It is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. The Act stipulates that if there's a security breach of a database containing personal data, the responsible organization must notify each individual for whom it maintained information. A business reputation is at stake if their database is compromised. The Act, which went into effect July 1, 2003, was created to help stem the increasing incidence of identity theft. According to the *Federal Trade Commission – 2003 Consumer Fraud and ID Theft Report (2004)*, “The FTC received more than half a million consumer complaints (516,740) during calendar year 2003, up from 404,000 in 2002. These include 301,835 complaints about fraud and 214,905 identity theft reports! 42% of all complaints received by the FTC related to ID theft, up from 40% in 2002”. Bishop (2005) made an analysis in his article *Identity theft: The Next Corporate Liability Wave*. His analysis is the following:

“Each identity theft victim will on average spend \$1,495, excluding attorneys' fees, and 600 hours of their time to straighten out the mess, typically over the course of a couple of years. For out-of-pocket costs alone that is, say, \$2000 per victim. Multiplying that by 10,000 customer victims equals \$20 million. Adding as little as \$15 per hour for the victims' time and you get \$11,000 per case or \$110 million in total even before fines and punitive damages are considered. And that's on top of the potential impact on your company's future sales. The FTC estimates that over 24 million people in the United States have had their identity stolen. The \$11,000 damage figure per case developed above represents over \$26 billion of potential liability if fault can be ascribed to the data holder” (Bishop, 2005).

Bishop (2005) states further that “customer and employee databases are prime targets for identity thieves because a single vulnerability in a company's information security can yield access to personal data on thousands of persons”. One can see why the CSBIA and other laws were implemented.

Other regulatory compliance includes the “privacy legislation, such as the early Federal Act of 1974 and the more recent Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Children’s Online Privacy Protection Act (COPPA), require organizations to put in place adequate privacy preserving techniques for the management of data concerning individuals” (Bertino, 2005). Other federal laws impose a duty to safeguard consumer information in certain areas. For example, “under Title V of the Gramm-Leach-Bliley Act (GLB), financial institutions are required to take steps to protect their customers' data, and face the possibility of fines or jail

time for failure to comply” (Bishop, 2005). The Fair and Accurate Credit Transactions Act (FACT Act) was signed by President Bush on Dec. 4, 2003; it affects almost all companies in the U.S. Bishop (2005) states that

“Among its provisions, this law mandates that businesses must take reasonable measures to destroy information derived from consumer credit reports before discarding them, with effect from June 1, 2005. Shredding papers and wiping or destroying hard drives and backup media will be standard. From December 2006, merchants accepting credit cards must leave all but the last five digits off printed receipts”.

Since most customer data are stored in databases and customer and employee databases are prime targets for unscrupulous individuals, the government is putting in place regulations to help protect the consumer from illegal activities or information terrorism. However, professionals must also do their part to protect their network and databases from acts of terrorism. One must ensure that the DBMS has adequate security features that may help the organization meet the minimum regulatory compliance requirement.

## **4.2 SECURING THE DATABASE**

### **4.2.1 Policies**

It is imperative that Information Security managers or personnel, Database Administrators (DBA) as well as upper level management implement strict guide lines and procedures in protecting the corporate network as well as their database applications. The reason is that “IT security is focused primarily on protecting the perimeter, but with internal data leaks and security breaches topping the news security executives today are seeking measures to protect customer data and corporate intellectual property across the organization” (Dubie, 2006).

Bishop (2005) states that “in addition to the growing threat of class action lawsuits, new laws are coming into effect to hold organizations responsible for securing personal data. Companies should evaluate this risk and consider taking action to reduce their potential liability”.

Database security starts with policies. Policy is defined as “a plan or course of action as a government, political party, or business, intended to influence and determine decisions, actions and other matters” (Whitman, 2004). Policies are comprised of a set of rules that dictates acceptable and unacceptable behavior within an organization. One can take a closer look at a policy as an agreement, on what is acceptable behavior, made between the organization and individuals who work in the organization. It is a code of conduct for the performance of individual users.

Policies protect information, people, property and reputation. The Enterprise Information Security Policy (EISP) is an example of how a policy guides the

overall security program, including technology. A policy is a Management tool that is used to control the actions or behaviors of its members with regards to the misuse of the firm's information technology infrastructure. The EISP, also known as a program policy, is a general security policy that sets the strategic direction, scope and the tone for all of an organization's security efforts. The EISP guides the development, implementation, and management requirements of the information security program. The EISP must directly support the organization's vision and mission statements. In light of legal challenges it must also be defensible. Thus, the EISP must meet two criteria. The existing policy must be known by members throughout the organization, and violations of the existing policy must be handled in a standard and consistent way.

To further understand how policy manages access control in an organization, one could take a closer look at the System-Specific Policy (SSP). The SSP often functions as standards or procedures to be used when configuring or maintaining systems. "Normally a management guidance SSP is created by management to guide the implementation and configuration of technology as well as to address the behavior of people in the organization in ways that support the security of information", (Whitman, 2004). Policy forms a foundation of trust in the organization, and it is also an important source of support for organizational goals. It should prohibit activities that detract from achieving organizational goal.

SSP's are technically specific, which means that it focuses on implementation of technical controls such as access control lists (ACL) and configuration rules. ACL's include the user access lists, matrices and the capability tables that govern the rights and privileges of users. More specifically, ACL's disclose who can use the system, what the system can provide, when the system will provide it, where the system will provide it and how authorized users can access the system. Lastly, configuration rules are specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

Management may also consider a formal access control policy (ACP). The ACP "determines how access rights are granted to entities and groups. The ACP must include provisions for periodically reviewing all access rights, granting access rights to employees, changing access rights when job roles change and revoking access rights as appropriate" (Whitman, 2004). Many security managers often fail to revoke access rights especially when an employee has been terminated or has left the company. These sorts of errors have cost companies millions of dollars. The ACP may be a part of the SSP. However, practice has shown that it is better to have specific policies separated even though they may be combined. The overall philosophy of the organization is also a key to managing access controls. Dr. Michael Whitman made it clear that "without an access control policy, systems administrators may implement

access controls in a way that is inconsistent with the organization's overall philosophy" (Whitman, 2004). Policies and organizational goals must go hand in hand. The organization and its IT security department must be heading in the same direction, on one accord.

Policies protect information, people, property and reputation, but only to a certain degree; even though they are in place they are often disregarded by employees who commit flagitious crimes for personal gain. The top level executives are then sent to the guillotine after a security breach, because the breach was engineered from the inside.

In business it is often easy to forget the word "trust". Often times contributing to the "bottom line" has overshadowed a main fundamental in managing a business effectively. Many organizations do not implement a micromanaging policy. They "trust" their employees to do the work. Trust and policies goes hand in hand. "Trust implies that one party is willing to depend on the other party for certain resources or action, even though negative consequences are possible" (Woon, 2006).

Unfortunately, upper level management may not trust employees due to the fact that other literature stated that employees are normally the main cause of security brecches. Dubie (2006) quoted Sean Franklyn, an IT security manager at a large financial services firm, said that "people are our weakest links. Most of our wounds are still self-inflicted. Configuration changes that aren't well thought out and leave us open and exposed in certain areas are still the hardest thing to lick". However, creating a security minded culture is a great start in securing database. Dubie (2006) states that "creating a security-minded culture is making it clear why certain security policies are in place. It's important to make sure security measures don't impede business processes".

#### **4.2.2 Current and Emerging Network Security Technologies**

This section will look at the current and emerging technologies that one may want to implement. Database security starts with implementing policies first and then focuses on securing the network where the system lays. Policies are the foundation for implementing security procedures. However, it is important to note that policies and security cultures cannot depend on people and processes alone. "There are technologies available today that helps automate policy enforcement, data collection and protection" (Dubie, 2006). After SSPs are implemented on the Database System, management may want to implement hardware that protects not only the DBMS but the entire network infrastructure. The network infrastructure ranges from physical security (securing the building where the databases are stored or operate) to the applications that run on or use that DBMS.

Technologies such as Network Access Control (NAC), and Outbound content monitors, are just a few from a long list of products that may help harden your network and database security. The concept of NAC is simple. Snyder (2006) states NAC simplicity as "authenticate every user connecting to the network,

then enforce an access-control policy based on who they are and other information, such as endpoint security checks and wired vs. wireless access method". Again the term policy arises. One of NAC's benefits is that it gives you the opportunity to set a policy for every user. It is important to note that NAC is fancy, complex and expensive, but it is just a component in the bigger picture of information security and network defense. One cannot put a price tag on keeping information safe. If one purchased a \$100,000.00 piece of equipment and it fails to do its job; then obviously it wasn't worth it. Careful analysis, research and testing need to be conducted to see if it is a right fit for the organization before heavily investing in it. Some vendors offer trial periods for their product.

Outbound-content monitoring is an excellent way to detect if sensitive information is leaving the network. Implementing Outbound-content monitoring or information leakage prevention to the corporate security architecture may help prevent the monumental ramifications a company may face if confidential information is leaked to the public, "due a disgruntled employee here, a careless one there" Schultz, (2007). Shultz, (2007) further states that:

Today's information leakage prevention monitoring systems can scan just about any type of DataStream, including Web traffic, e-mail, FTP, electronic faxes and instant messages. Some monitors also detect stored sensitive data squirreled away in Word documents, spreadsheets, PowerPoint - just about anywhere. In addition, they're much more linguistically sophisticated than earlier products. Shultz continued by saying Rather than just being able to search for simple keywords - like the name 'Trent' - or a particular Social Security number, they can do conceptual analysis. For an example outbound content monitors can understand when a mergers-and-acquisition memo needs to be flagged because it still contains sensitive information even though it has been paraphrased or rewritten. "Using language analytics, they're able to detect things that in the past would have slipped by".

Outbound-content monitoring hardware or software protection is helpful when there are attempts to compromise databases or the entire network.

Other technologies such as intrusion detection systems (IDS) are helpful in protecting or monitoring the entire network. IDS help determine (by conducting a trace to the source) whether an intrusion to unauthorized systems, or folders are internal or external. It is important to note that if the trace is leading to an external source, it is up to the Network Administrator to ensure that the IDS are properly configured so that the trace ends at the perimeter of the network. If your IDS trace through the corporate perimeter the organization is guilty of hacking. Once your device traces the path of communication outside the corporation perimeter the corporation has violated the Electronic

Communications Protection Act (ECPA); and or by definition Your organization is a hacker. One must remember that the ECPA prohibits unlawful access and certain disclosures of communication contents; meaning that IDS should not be tapping into a wire that it does not have access to. If the trace leads to the outside on should contact law enforcement so that they can conduct the trace on behalf of the company. One must remember that IDS software, when configured incorrectly will trace beyond the perimeter. The IDS software today is very intelligent; the software asks to define the address pool and all subordinate address pools that the company may own, so that it knows its boundaries. Therefore, if administrators want to trace outside the defined address pool, the software may ask if one has legal permission to do so. Therefore, it is very important to implement technologies that will help detect, monitor, tract and trace suspicious activities. Perimeter security is important because is protects the gateways to where the database systems lay. Perimeter security is just as important as system security.

#### **4.2.3 Other Suggestions and Technologies: Web Database Security Technologies**

One has to keep in mind that some organizations keep customer records or data, allow their customers access to that data via the web. The recent attacks on web based databases proves that the “Web is being used to provide users with direct access to established databases” (Bi, Vrbsky, and Jukic 1999). Securing these web databases is a paradigm in itself. However, this paper will speak briefly as to how to possibly implement technologies to secure web databases. Bi et al (1999) states that “Web database systems are typically built using commercial off-the-shelf components, such as Web servers and database management systems. Off-the-shelf components do address security, but unfortunately, a combination of these mechanisms does not necessarily provide the security and performance needed by an organization”. Web base databases are a concern; they are vulnerable, because any device connected to the web is at risk to an attack. These databases are deployed on web servers. Bi et al, 1999 states that:

A Web server represents the biggest potential security weakness in an organization. A Web server program with errors or a Web server that is misconfigured can allow unauthorized users to access confidential information that is stored in the server. Similarly, a faulty Web server can allow unauthorized users to execute commands on the server host machine and modify the server system, or even gain information about the host machine of an organization.

To prevent such a catastrophe, this paper suggests using the proxy server technology. One must remember that a proxy server is a server that “acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server

is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion” (Netproject, 2007). The proxy Database server intercepts all requests to the real Database server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. The real server then sends the information requested, back to the proxy server. With the proper configuration of firewall rules, routing tables and the proxy server; the proxy server technology may help secure the DBMS or Database. If the proxy server is compromised, the threat will not disrupt the network. One reason being; the proxy server is most likely located in a Demilitarized Zone (DMZ). A DMZ is a part of the network that is neither part of the internal network nor directly part of the Internet. It is a no-man's land between the Internet and the internal network. This zone is NOT in the internal network, but is NOT widely open on the Internet. A firewall or a router usually protects the DMZ with network traffic filtering capabilities (possibly stateful packet filtering). Therefore, if the proxy server is compromise, it does not pose a threat to the network because of where the proxy server is located; in the DMZ.

#### **4.2.4 DBMS programs and application security**

One must not overlook the simplest form DBMS security methods such as installing patches on the DBMS. Patches help prevent the exploits of vulnerabilities especially in a SQL server environment; vulnerabilities that include worms, Denial of service (DoS) attacks and Buffer overflow. Guimaraes (2006), states that “these vulnerabilities can be exploited by a remote hacker without ever having to authenticate to the server. The only thing that needed to be done to avoid losses was to download patches for the respective SQL Server bugs” and for other enterprise DBMS applications.

Administrators should take the initiative to change the default passwords that are in place with the system before deploying the DBMS on the corporate network. Passwords are supposed to be strong. Usernames and passwords such as “system” and “system” or “sa” and “sa” or administrator and a blank password field are not strong password. MSDN Library (2007), states that:

Passwords can be the weakest link in a server security deployment. You should always take great care when you select a password. A strong password has the following characteristics:

- Is at least 8 characters long.
- Combines letters, numbers, and symbol characters within the password.
- Is not found in a dictionary.
- Is not the name of a command.
- Is not the name of a person.
- Is not the name of a user.



- Is not the name of a computer.
- Is changed regularly.
- Is significantly different from previous passwords.

Microsoft SQL Server passwords can contain up to 128 characters, including letters, symbols, and digits. Because logins, user names, roles, and passwords are frequently used in Transact-SQL statements, certain symbols must be enclosed by double quotation marks (") or square brackets ([ ]).

Sometimes we tend to over look the simplest things; the simple mistakes can cost the company millions.

One can harden the DBMS with Data encrypting tools. Tools that do data encryption are an excellent place to start when trying to secure one's database application; and Solix Technologies is an excellent place to start looking. Solix Technologies is a leading provider of enterprise data management solutions. They have proven success in helping organizations worldwide to meet compliance requirements, and achieve Information Lifecycle Management (ILM) goals and strategies; Solix initially focused on securing and archiving Oracle databases. "Solix Technologies provides best-of-breed solutions and has partnered with leading platform and application vendors like Oracle, SAP, Google, HP, EMC and Sun Microsystems to effectively cater to our customers unique environments and evolving needs" (Solix, 2006). Silverthorn (2007) gave a brief analysis of solix encryption software:

Solix has broadened the scope of its archiving software and has rechristened it as the Solix Enterprise Data Management Suite. The suite addresses both compliance and information lifecycle management (ILM) with four components: Secure Test and Development, Data Auditor, Enterprise Archiving, and Application Sunsetting and Migration. The compliance-related component, Data Auditor, monitors and reports on archived data that has been accessed, updated, or deleted. It's a policy-driven security tool that provides event notification and reporting of database activity, and can be searched during and audit or e-discovery inquiry".

Again the term policy arises. Policies are the foundation to secure anything. Sometime professionals focus on the external threats that affect databases and forget about the internal threats. Polstra's (2006) New Jersey Crime Ring analysis sheds light on internal thieves. Connor's (2006) article *Solix adds security features: Archiving software guards data via masking or encryption* quotes Brian Babineau, senior analyst for the Enterprise Strategy Group saying "Most people worry about the external threat of accessing that information, but with database information it is different, because developers and internal parties have access to that information. With this software, you can mask sensitive rows and columns in the database, so your developer resources do not

see them” (Connor, 2006). This software is not cheap. “Prices range from \$100,000 to \$400,000 for the components of Solix Enterprise Data Management Suite, which can be purchased separately. For the mid-market, the entry level can be as low as \$60,000” (Silverthorn, 2007). This paper suggests that careful analysis, research and testing need to be conducted to see if it is a right fit for the organization before heavily investing in it. Before deployment or placing the DBMS into production; one can place the DBMS into a testing environment, populate the database, and run a series of tests. One test to consider is SQL injection. The Administrator needs to secure the DBMS from SQL injection. E-government (2007) states that “SQL injection is the name for a general class of attacks that can allow nefarious users to retrieve data, alter server settings, or even take over your server if you are not careful. SQL injection is not a SQL Server problem (as many may think), but a problem with improperly written applications” on all DBMS. Guimaraes (2006) gives a brief description of SQL injection.

An SQL injection is an attack to the Database as a result of insecure code. You create a web page, for example, that will allow a user to input text into a textbox and that text will be used to build a query that will be executed against a database. A malicious user enters malformed data into the textbox which changes the nature of the query and allows the user to gain access to information that he/she doesn't have privilege to access, delete or alter data in the back-end database.

Guimaraes explains further that the attacker can shut down databases by using SQL injection. His explanation is stated below.

For example, consider a web page that has two input text fields, one to enter a user name and another to enter a password. The user enters a user name and password that matches a user name and password in the database. A dynamically created SQL statement is used to search the database for matching records. The user is then authenticated and allowed access to the system. Users who enter an invalid user name and password should not be authenticated. However, a hacker can enter malformed text into the user name textbox to gain access to the system without having to know a valid user name and password. By filling the username field on the form with the string: ‘; shutdown; --’ and leaving the password blank, the following SQL statement is executed:

```
SELECT user FROM all_users where username ='';shutdown; ---' and pass=''
```

Note that after the shutdown with the semi-colon, there are two hyphens. In SQL two hyphens is a comment so anything after that is not executed. For Microsoft's SQL Server database with default system administrator account (sa) as the application login, the code above will shut down the

database server. Another malicious user input could be ' Or 1=1 -- for the user name and the SQL query becomes: SELECT \* FROM all\_Users WHERE UserName=" Or1=1 --' AND Password="

The expression 1 = 1 is always true for every row in the table, and OR will always return true if one of the expressions is true. This query will return rows that were not intended to return.

Guimaraes (2006) states further that “there are five measures that you can take to prevent SQL injection attacks. The author suggests that you implement as many of these measures as possible to have multiple layers of security in your application. That way if one of the measures is circumvented because of some vulnerability, you are still protected”. The five measures are the following:

First, you should never trust user input. You should never use input from a database query that has not been validated. According to the author, the best approach to validate user input is to ‘identify the allowable characters and allow only those characters’. Second, you should never use dynamic SQL. SQL injection attacks are dependent on dynamic SQL queries. The author suggests using stored procedures or SQL queries that accept parameters. Third, you should never connect to a database using an admin-level account. Fourth, don’t store passwords in plain text. The author suggests that you encrypt or hash passwords, encrypt connection strings and other sensitive data. Fifth and finally, error messages that the users see should display minimal information (Guimaraes, 2006).

If one is paranoid of their DBMS being breeched one can implement Multilevel Security (MLS). Guimaraes (2006) gave an explanation on MLS and how it works. The explanation is the following:

Traditional Databases allow you to consider data in two categories: sensitive or nonsensitive. Multilevel Security (MLS) is a feature that allows information with different classifications to be available in an information system, where users have different security clearances and authorizations, and are prevented from accessing information for which they have not been cleared or authorized. It was developed for the U.S. military and intelligence communities. The purpose of this policy is to separate data based upon its security classification. Classified data is stored on dedicated systems and access is prevented to users outside the immediate community of interest. The main drawbacks of this scheme are redundant databases, redundant workstations, high IT infrastructure cost and inefficiency. In MLS terminology, objects such as data tables, records and fields are referred to as passive entities. A subject is an active process that can request access to objects. Every object is assigned a classification and every subject a clearance.

Classifications and clearances are collectively referred to as labels. A label

consists of two components: hierarchical and unordered compartments, with hierarchical component specifying the sensitivity of the data. Other key aspects are Mandatory Access Control (MAC) and Poly-instantiation. Multilevel Security uses MAC access control to prevent the unauthorized disclosure of high-level data to low-level users. In MAC, security is enforced by the system as dictated in the security policy and not by the owner of the object. Polyinstantiation allows a relation to contain multiple rows with the same primary key where the multiple instances are distinguished by their security levels. Most DBMSs were not designed with multilevel security in mind and there is little support for MLS, which poses significant challenges to the database research communities. Another approach is to take advantage of new security features contained in new releases of the standard products. With the release of Oracle 9i, for example, Oracle implemented Oracle Label Security that allows us to simulate a multilevel database (at least to a certain degree). It is a built-in row level access control for high security applications, adding a new field for each row to store the row's sensitive labels. Row access can be granted or denied by comparing the user's identity and security clearance label with the row's sensitive labels (Guimaraes, 2006).

There is another form of DBMS security that may be implemented to add another level of security to a DBMS. This type of security is often implemented by the Database Administrator (DBA). These security measures are also the traditional DBMS securities. These include granting and revoking privileges to data objects and implementing row and column level security. "Traditional Database Security has focused primarily on creating user accounts and managing user privileges to database objects" (Guimaraes, 2006). These commands are simple and easy to execute. Granting roles and privileges allow the DBA to keep a leash on who gets to view or manipulate data. Application security focuses on protecting data while it is in use, storage or in transmission from unauthorized access.

Other security issues include stored procedure security; more specifically invokers and definers rights. Invokers and Definers rights pose security issues for the database. There are internal personnel that may need access to certain data; but there are some that engage in criminal activities. Invokers and Definers rights creates and internal database vulnerability. Oracle defines and gave a brief description of Definers rights as the following:

Definers rights stored routines are procedure or function that runs with the privileges and access rights of its definer, and not that of the executing user. This allows database programmers to call procedures or functions that can read and update the database on behalf of unprivileged users, i.e. perform tasks that the current invoker of the procedure is unable to perform themselves (Technical Corner, 2007).

Invoker and Definers Rights pose a security issue. It is up to the DBA and security officials to implement proper stored procedure security. Another security technique includes locking. Locks can be either:

- Implicit locks are locks placed by the DBMS
- Explicit locks are issued by the application program
- Lock granularity refers to size of a locked resource
- Rows, page, table, and database level
- Large granularity is easy to manage but frequently causes conflicts
- An exclusive lock prohibits other users from reading the locked resource
- A shared lock allows other users to read the locked resource, but they cannot update it

DBAs and application programmers should decide whether locking the database is appropriate or not. It is important to note that these methods of database security are only a few from an evolving list; securing DBMSs are based on the organization's policies and the other issues such as regulatory compliances.

### **4.3 Management Tools and Technologies**

This section of the paper is not in any means trying to tell anyone what they need to protect their database; that decision is left up to management. This section propose a guide or something to consider for future implementation.

There are management tools that have been tested and have been approved in meeting regulatory compliance. Andress (2006) states that "NetIQ Vulnerability manager is one of the most well rounded product tested. While it did not stand out in any individual area, it performed solidly across the board in policy management, reporting, compliance checks, configuration and remediation".

Organizations are growing and it is unlikely that they will have one database or DBMS on their IT infrastructure. Thus, it would be more efficient to be able to manage all databases from a centralized area. This approach not only increase efficiency and productivity but also improves security because everything is monitored from one location. Dubie (2006) states that there are management tools that can perform the centralized Database management approach; an analysis of these tools is the following:

Computer Associates CA is making available a free distributed database management product that could help administrators manage multiple, heterogeneous databases across their networks. Unicenter Database Command Center (DCC) is a Web-based database management console customers can download to any workstation or laptop with access to a browser, and the software does not require any client software be installed

on databases.

DCC provides database administrators with a common look and feel when working across various systems. This tool allows you to manage and execute commands on various databases such as Oracle and DB2. While each database vendor provides management tools for its own offerings, CA says DCC lets customers perform administration tasks on DB2 UDB for z/OS, Oracle, DB2 UDB for Linux Unix, Windows and Ingres database.

Lastly this paper will take a look at VeriSign security service as a management tool. Many individuals at some point in time have entered credit card information over the web. Most of these websites are “secured”. Most of these websites use VeriSign as their “intelligent infrastructure services that enable people and businesses to find, connect, secure, and transact, by providing encrypted communications when viewing web pages, logging into your account and downloading reports” (Wikipedia, 2007). VeriSign is probably the most dominant certificate authority on the Internet at the present time. “VeriSign operates digital infrastructure that enables and protects billions of interactions every day across the world’s voice and data networks” (VeriSign, 2007). It is only fitting to use their product in this paper, because of their product reliability and goodwill.

Messmer (2006) states that “VeriSign expanded its log-management service beyond firewalls, operating systems and intrusion-detection systems to collecting log data related to applications and databases”. Messmer further states that VeriSign’s service is based on its Security Defense Appliance, which is placed inside a corporate network to collect, analyze and store logs. Expanding the log-management service allows the service to collect raw data or just the security-related events pertaining to applications and databases of corporate customers” (Messmer, 2006). christened her article by quoting Kelly Kavanagh, Gartner analyst in information security and privacy; where he states that ‘centralized logging and monitoring of application-level events is being driven by regulatory compliance, highly publicized data theft incidents and targeted application-level attacks’. Again this paper shows that regulatory compliance plays an important role in Network and Database security.

## **5. RESULT AND CONTRIBUTION - UNIFYING THE PROCESS OF DATABASE SECURITY**

There are misconceptions that Database security is securing the database. Guimaraes (2006) states that “Traditional Database Security has focused primarily on securing the Database, with minor emphasis on securing the Operating System and the Database Management System (DBMS)”. Database security should be a unified process, which starts from the corporate network infrastructure to pre DBMS activities (education and research) to DBMS programs and application security. Wikipedia states that “Database security can begin with the process of creation and publishing of appropriate security standards for the database

environment. The standards may include specific controls for the various relevant database platforms; a set of best practices that cross over the platforms; and linkages of the standards to higher level polices and governmental regulations” (Wikipedia, 2007). Selecting the proper DBMS may be influenced by government regulations. One must ensure that the DBMS meet the regulator’s minimum requirements, but it is up to us as professionals to implement technologies, procedures and best practices so that we operate at a higher standard than what is required.

Policies are the foundation for securing information. Policies are comprised of a set of rules that dictates acceptable and unacceptable behavior within an organization. One can take a closer look at a policy as an agreement, on what is acceptable behavior, made between the organization and individuals who work in the organization. It is a code of conduct for the performance of individual users. Policies protect information, people, property and reputation. Establishing an EISP and SSPs and ensuring that personnel follow those policies may prevent upper level management from going to the guillotine. After policies are in place it is up to management to secure the perimeter of the corporate network.

Management must ensure that their network is tightly secured and their systems comply with regulatory standards. This paper is highly bothered by the Supplemental Case: TJX. The case shows lack of urgency and leadership. This paper initially stressed that IS professionals should keep abreast with current happenings in the industry and learn from the mistakes of others so that one does not make similar mistakes. This paper proves that TJX and others are not implementing measures to safe guard their Information Systems. The Citigroup case shows why it is important to encrypt data. It also shows that TJX did not learn from Citigroup mistakes. Brodtkin (2007) states that “hackers were able to access such a huge amount of data indicates TJX either failed to encrypt or truncate card numbers or did not secure encryption keys that can translate scrambled card information.” Brodtkin states further that “TJX says that they encrypted **some** card data, but they believe hackers had access to the decryption tool”. Hopefully, the hackers performed an extensive search to obtain the decryption tool, to perform their criminal acts. Hopefully, the decryption tool was not stored in the same databases that were hacked. This incident shows that if there were some form of intrusion detection system (that works) on their network, network administrators would have been able to detect that intrusion. This paper believes that TJX did not comply with the PCI Data Security Standard (PCI DSS). “The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.” (PCIsecuritystandards.org, 2007). Brodtkin (2007) strengthens this paper by stating in his article that “to comply

with the PCI DSS, companies must be audited annually and be scanned for external vulnerabilities by third party auditors at least once a quarter.” This paper firmly believes that TJX failed to comply with the PCI DSS. TJX may now face fines, sanctions, retrogress in goodwill and possibly lawsuits of gargantuan proportion. The Boston Globe (2007) reported that the cost of TJX breach soars to \$256 million, which includes law suits and computer fix. If TJX IS professionals were keeping abreast with current happenings in the industry and learn from the mistakes of others, they would not have found themselves in this situation. Obviously, TJX did not implement measures to safe guard their Information Systems; they did not comply with PCI DSS. Further analysis of the PCI DSS states that:

The PCI DSS January 2005 version has been enhanced in the PCI DSS Version 1.1. The PCI DSS January 2005 version may no longer be used for PCI DSS compliance validation after December 31, 2006. The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

**Build and Maintain a Secure Network**

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data

*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

*Requirement 3:* Protect stored cardholder data

*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

*Requirement 5:* Use and regularly update anti-virus software

*Requirement 6:* Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

*Requirement 7:* Restrict access to cardholder data by business need-to-know



*Requirement 8:* Assign a unique ID to each person with computer access

*Requirement 9:* Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

*Requirement 10:* Track and monitor all access to network resources and cardholder data

*Requirement 11:* Regularly test security systems and processes

**Maintain an Information Security Policy**

*Requirement 12:* Maintain a policy that addresses information security.

One must notice that the standards that govern securing information such as PCI DSS standards and other standards are a combination of Information Security, Network Security as well as Database Security best practices. Failure to comply with industry standards and best practices will place companies in a similar position of TJX and others named in Polstra's (2005) journal article. As professionals it is imperative to comply with standards; this further shows that Database security is a unifying process.

NAC and Outbound-content monitoring is an excellent way to detect if unauthorized and authorized users are trying to access sensitive information or to detect if sensitive information is leaving the Database or the network. Implementing NAC and Outbound-content monitoring or information-leakage prevention to the corporate security architecture may help prevent the monetary ramifications a company may face if confidential information is leaked to the public.

As a professional one cannot over look securing the DBMS programs and application. Data encrypting software is an excellent place to start when trying to secure one's database application. When transmitting data via any medium the data should be encrypted, especially when the data is sensitive material. If the Citibank had encrypt its data in the first place their whole incident would have "never happened", and possibly Polstra (2006) would have applauded them for taking proper security measures when transmitting sensitive data. There are vendors (Solix) that offer software that encrypt data, while it is in use, storage and transmission.

Applying patches to systems so that worms and hackers cannot exploit vulnerabilities is vital. Patches help prevent the exploits of vulnerabilities especially in a SQL server environment. Vulnerabilities that include worms, Denial of service (DoS) attacks and Buffer overflow can be prevented by applying the vendor's patch. This paper explained and gave a detailed example of SQL injection. Guimaraes (2006) gave five measures that one can take to prevent SQL injection attacks. Guimaraes stated further that if one implements as many of these measures as possible to have multiple layers of security in

your application. That way if one of the measures is circumvented because of some vulnerability, you are still protected. It is good practice to follow best practices. Thus, it is good practice to change default passwords to strong passwords. This paper stated Microsoft's characteristics of a strong password. This paper reiterates that it is good practice to follow best practices. Locking techniques and issues regarding Definers and Invokers rights are dependant on the DBA.

Lastly, this paper states that the centralized management approach of database security is most appropriate because it provides the DBA with a unified solution to manage multiple distributed databases. Therefore, database management is equally important. Its importance is illustrated in the following quote where Dubie (2006) states that "with an ever-increasing number of databases being supported by enterprises, the need for unified administration is growing". Dubie 2006 stated further by quoting Noel Yuhanna, senior analyst at Forrester Research, recently wrote in the "Trends 2006: Database Management Systems" report, that "enterprises want a unified solution to simplify administration, reduce cost and improve operational efficiency" and security. NetIQ Vulnerability manager, VeriSign security service, Unicenter Database Command Center (DCC) by Computer Associates may be used as management and security tools when securing the database. These products and vendors offer comprehensive management solutions that can help you reduce the total cost of database ownership, manage day-to-day operations and increase overall service management responsiveness.

## **6. CONCLUSION**

One may assume that cyber terrorists as well as terrorists to ones identity will not stop plaguing networks and DBMS. Thus, it is important when selecting a DBMS, that it has security and other features that would help protect, improve performance, production and efficiency of the Database.

This paper believes that Database security starts with promoting a change in Database Curriculum Development trends. Class room discussion plays a role in helping secure databases. Classroom discussions open up real world strategies that have been proven effective in securing databases. Students who are apart of a masters program are required to have some form of industry experience. The student's industry experience is an asset within a masters program because it helps others learn and understand different technologies, strategies, and approaches when involved in classroom discussions. Some of these strategies start with DBMS selection and weighing the advantages and disadvantages of the DBMS. It is important to keep in mind that DBMS selection depends on the Database model chosen, because not all DBMS support all Database Models. This paper firmly believe that promoting a change in Database curriculum development trends to facilitate discussions on proven strategies used in the real world can be helpful in securing databases.

Instead of relying on the traditional Database Design and Implementation curriculum format, facilitate discussions and conduct meaningful research as a part of the class. Employers are always open to hear other strategies that were developed by other companies, especially when those strategies were a part of a meaningful discussion—a classroom setting; rather than a discussion that may be considered nefarious.

It is equally important to adhere to standards set forth by regulatory compliance, voices of these agencies and law officials. It is important to implement and meet the minimum standards of security that these regulatory compliances require, but it is equally important to implement and operate standards at a higher level. Thus, it is imperative that upper level management, network Administrators, DBAs, and other personnel to adhere to corporate policies. “Building a more security aware culture is finding the right mix of processes and technology that suit the business, and then educating the IT staff and user community on how to maintain secure practices” (Dubie, 2006). Dubie (2006) further states that “A first step in creating a security-minded culture is making it clear why certain policies are in place. It is important to make sure security measures don’t impede business process, but are aligned with the organization IS policies and strategies along with the alignment of the organization strategies”.

Experience is the best teacher. One should keep abreast with the latest trends and happenings in database and network security. As security professionals it is our duty. We must also learn from the mistakes of others and take preventative measures that those mistakes does not happen. This paper has shown cases where hackers are using social engineering techniques (2.2 Case II: ChoicePoint) to hack or gain sensitive information.

Database security is a unified process. Securing both the network and the database goes hand in hand. Hackers must penetrate the perimeter before getting to the database, thus, it is important for network administrators and DBAs to implement technologies whether it is hardware or software that can detect, monitor, and prevent abnormal behaviors on the network perimeter and within the DBMS. The careful management of database is important because it provides DBAs a unified solution to simplify administration, reduce cost and improve operational efficiency and security. Hackers have no regard for privacy and identity; their nefarious acts are crimes against freedom. They have the mindset of terrorists that plagues homeland security and life itself. Hackers are on top of their game, and so should we. Therefore, this paper has discovered that Regulatory Compliance, Network and Database Security is a unifying process, that may help mitigate the increasing threats and database breach that we as professionals should work to achieve.

## **ACKNOWLEDGEMENTS**

First of all I would like to thank god for the strength, wisdom and patience in writing this paper. Without him this paper or none of my accomplishments were possible. I would like to thank my past Database Professors; the late Dr. William Burg, and Dr. Mario Guimaraes for pouring their knowledge of Database Management Systems, Database Design and Implementation, and Database Security on me. Special thanks to Dr. Mario Guimaraes for advising me to submit this paper to the 2007 InfoSec CD Conference. Special thanks to Dr. Michael Whitman and Herb Mattord for pouring their knowledge of Information Security in their books, classroom, and lab sessions. Thanks to the InfoSec CD for accepting this paper for the 2007 conference. Thanks to KSU writing center for correcting grammatical errors. Special thanks to ACM SIGCHI for allowing me to modify templates they had developed.

## **REFERENCES AND CITATIONS**

- Federal Trade Commission (FTC). (2004). National and State Trends in Fraud & Identity Theft January -December 2003. Retrieved March 28, 2007 from [http://www.consumer.gov/idtheft/pdf/clearinghouse\\_2003.pdf](http://www.consumer.gov/idtheft/pdf/clearinghouse_2003.pdf)
- E-government in New Zealand. (2007). Appendix E - Glossary of Terms: Chapter15.html - SQL Injection. <http://www.e.govt.nz/> retrieved April 4, 2007 from <http://www.e.govt.nz/services/authentication/library/docs/authentication-bpf/chapter15.html/view?searchterm=SQL%20injection>
- MSDN Library. (2007). SQL Server 2005 Books Online: Strong Passwords. Retrieved March 30, 2007 from <http://msdn2.microsoft.com/en-us/library/ms161962.aspx>
- Netproject. (2007). G. Glossary. Proxy Server. Retrieved April 5, 2007 from <http://www.netproject.com/docs/migoss/v1.0/glossary.html>
- PCI Security Standards Council. (2007). About The PCI Data Security Standard (PCI DSS). <https://www.pcisecuritystandards.org/tech/>
- Solix, (2007). About Us. Retrieved March 30, 2007 from [http://www.solix.com/company\\_overview.htm](http://www.solix.com/company_overview.htm)
- Technical Corner. (2007). Stored Procedure Security. Retrieved April 4, 2007 from [http://www.oracle.com/technology/products/rdb/pdf/stored\\_procedure\\_security.pdf](http://www.oracle.com/technology/products/rdb/pdf/stored_procedure_security.pdf)
- Wikipedia, (2007). Database security. Retrieved from Wikipedia, the free encyclopedia. [http://en.wikipedia.org/wiki/Database\\_security](http://en.wikipedia.org/wiki/Database_security) from
- VeriSign. (2007). About VeriSign. Retrieved March 30, 2007 from <http://www.verisign.com/verisign-inc/index.html>

- Andress, M. (2006). NetIQ suite tops test of security compliance wares. Retrieved March 30, 2007 from Network World Magazine. [http://findarticles.com/p/articles/mi\\_qa3649/is\\_200606/ai\\_n17171660](http://findarticles.com/p/articles/mi_qa3649/is_200606/ai_n17171660)
- Bertino, E. Sandu, R. (2005). Database Security-Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing. Washington: Jan-Mar 2005. Vol. 2, Iss. 1; p. 2. Retrieved March 28, 2007 from ProQuest® Smart Search. <http://proxy.kennesaw.edu:2057/pqdweb>
- Bishop, J.F, T. Warren, J. (2005). Identity Theft: The Next Corporate Liability Wave? The Corporate Counselor March 30, 2005. Retrieved, March 29, 2007, from Corporate Counsel Magazine, <http://www.law.com/jsp/cc/pubarticleCC.jsp?id=1112090711870>
- Brodkin, J. (2007) TJX breach: Rethinking corp. security. Retrieved April 5, 2007 from Network World magazine, April 2, 2007. Vol24, Num13. [www.networkworld.com](http://www.networkworld.com).
- Connor, D. (2006). Solix adds security features: Archiving software guards data via masking or encryption. Retrieved March 29, 2007 from Network World magazine, 08/14/06 <http://www.networkworld.com/news/2006/081406-solix-archiving.html>
- Dubie, D. (2006). CA offers free database mgmt. tool. Retrieved March 28, 2007 from NetworkWorld magazine, April 24, 2006. Vol23, Num16. [www.networkworld.com](http://www.networkworld.com). <http://www.networkworld.com/news/2006/042406-ca-database-management.html>
- Dubie, D. (2006). Managing risk: new reality for IT security executives. Retrieved March 28, 2007 from NetworkWorld, September 11, 2006. Vol23, Num16. [www.networkworld.com](http://www.networkworld.com).
- Guimaraes, M. (2006). New Challenges in Teaching Database Security. Retrieved March 30, 2007 from The ACM Digital Library. <http://proxy.kennesaw.edu:2230/10.1145/1240000/1231060/p64-Guimaraes.pdf?key1=1231060&key2=4419225711&coll=ACM&dl=ACM&CFID=18658173&CFTOKEN=67659094>
- Messmer, E. (2007). UPDATE--TJX data theft called largest ever: 45.7M credit card numbers Security breach detailed in financial filing. Retrieved March 30, 2007 from NetworkWorld, September 11, 2006. Vol23, Num35. [www.networkworld.com](http://www.networkworld.com). <http://www.networkworld.com/news/2007/032907-tjx-data-theft-largest.html?page=1>
- Messmer, E. (2006). VeriSign security service expanded for apps, databases. Retrieved March 28, 2007 from NetworkWorld, September 11, 2006. Vol23, Num35. [www.networkworld.com](http://www.networkworld.com).

- <http://www.networkworld.com/news/2006/090706-verisign-security-service.html>
- Mbuthia, S. (2007). Selecting a DBMS. Retrieve March 28, 2007 From <http://csmoodle.kennesaw.edu/mod/forum/discuss.php?i=1639>
- Ogbuji, U. (2001). Choosing a database management system. Retrieved March 28, 2007 from <http://www-128.ibm.com/developerworks/webservices/library/ws-dbpick.html>
- Polstra III, M. Robert. (2005). A case study on how to manage the theft of information. Proceedings of the 2nd annual conference on Information security curriculum development InfoSec CD '05. ACM Press. 139-141. Retrieved, March 29, 2007, from <http://proxy.kennesaw.edu:2230/10.1145/1110000/1107653/p135-polstra.pdf?key1=1107653&key2=9181415711&coll=ACM&dl=ACM&CFID=18548384&CFTOKEN=44816403>
- Price, J. (2007). DBMS selection—James Price. Retrieved March 28, 2007 from <http://csmoodle.kennesaw.edu/mod/forum/discuss.php?d=1678>
- Schultz, B. (2007). New ways to protect data from insider attacks: The toughest security problem is the insider attack. These emerging tools promise to eliminate the threat Retrieved March 25, 2007 from Network World, 03/19/07 <http://www.networkworld.com/supp/2007/ndc2/031907-data-leakage-protection.html>
- Silverthorn, A. (2007). Solix extends archiving software Retrieved March 29, 2007 from infostor magazine March 19, 2007. [http://www.infostor.com/display\\_article/287507/23/ARTCL/Display/none/Solix-extends-archiving-software/](http://www.infostor.com/display_article/287507/23/ARTCL/Display/none/Solix-extends-archiving-software/)
- Snyder, J. (2006). The pros and cons of NAC: Bottom Line. Retrieved March 29, 2007 from Network World 06/12/06, <http://www.networkworld.com/columnists/2006/061206snyder.html>
- Whitman, M.E., & Mattord H. J. (2004). Management of Information Security.
- Whitman, M.E., & Mattord H. J. (2004). Readings and Cases in the Management of Information Security
- Woon, I. and Kankanhalli, A. *Trust, Controls, and Information Security*, Readings and Cases in the Management of Information Security, M.E. Whitman & H.J. Mattord (Eds.), Course Technology, Thomson Learning, 2006.
- Bi, C. Vrbsky, S, V. Jukic, N. (1999). A security paradigm for Web databases. *The ACM Digital Library*, Article No. 46. Retrieved from ACM Southeast Regional Conference archive Proceedings of the 37th annual southeast regional conference (CD-ROM).

Kerber, R. (2007). Cost of data breach at TJX soars to \$256m. Suits, computer fix add to expenses. The Boston Globe.  
[http://www.boston.com/business/articles/2007/08/15/cost\\_of\\_data\\_breach\\_at\\_tjx\\_soars\\_to\\_256m/](http://www.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/)