

Engineering Management  
Field Project

# **Implementing an Improved Security for XYZ's Database and Telecommuters**

By

Mohamed M. Ali

Spring Semester, 2011

An EMGT Field Project report submitted to the Engineering Management Program  
and the Faculty of the Graduate School of The University of Kansas  
in partial fulfillment of the requirements for the degree of  
Master's of Science

---

Herb Tuttle  
Committee Chairperson

---

Terry Sullivan  
Committee Member

---

Daniel Schmidt  
Committee Member

Date accepted: \_\_\_\_\_

## **Acknowledgements**

I would first like to thank ALLAH for the opportunity to obtain my master's degree and the belief in furthering education and learning as much as possible while we are in this world.

I would like to thank my parents for developing and supporting my quest of learning. They are the ultimate role models and without their guidance and support, I wouldn't have the love of learning like I do. As a child, they always stressed education and because of this, everything that I do and desire is focused on furthering my education.

I would also like to thank all of my siblings who have challenged me to be my best and I want to be an example to them so they are motivated to further their education. In addition, I would like to thank my wife and children who provide unending inspiration. They have given up their time by supporting my schedule in order to further my education. I hope that my children will inherit the desire to learn.

Finally, I would like to thank the entire staff of Engineering Management at The University of Kansas, Edwards Campus. I am very grateful to all of those with whom I have had the pleasure to work during this project and other related projects. I am also very grateful to have Herbert Tuttle as my mentor and committee chairperson, Terry Sullivan, and Daniel Schmidt as the committee members. In addition, I would like to thank them for taking the time to offer constructive criticism which made such an important contribution to this project and taught me a great deal about scientific research.

## Table of Contents

Executive Summary .....	2
List of Abbreviations and Nomenclature .....	3
Introduction.....	4
Literature Review.....	7
Firewalls.....	8
Virtual Private Network (VPN) .....	10
Strong Password.....	10
System backup and Anti-viruses.....	11
External and Internal Attacks.....	11
Network Intrusion Detection System (NIDS).....	13
Network Sniffers and Proper Encryption.....	13
The Need for Security .....	17
Database Security & Integrity of XYZ's Database.....	17
Developing a Database Security Plan .....	18
Implementing the Improved Security .....	20
Application Security .....	20
Further Security Improvement.....	20
Findings.....	23
Conclusion and Recommendations.....	26
Bibliography .....	29
Appendix A – Survey .....	31

## **Executive Summary**

This research paper provides an overview of the XYZ database security and implementing the best security measures to maximize performance and Web security for telecommuters. This research paper further discusses telecommuting security, strategies of implementing security, various types of technologies utilized, basic security products, and benefits for telecommuters and businesses. It also provides information on Web security which will entail techniques of proper encryption, firewalls, and how these security measures will enhance the overall performance of XYZ's database. This research paper will further describe how the above security measures will ensure better security of data stored in the database server, improve the overall database design, and explore the different types of technologies available such as Virtual Private Networking (VPN), authentication methods, and firewalls. In addition, this research paper will list costs associated with the appropriate security implementation in order to provide a secure environment between the telecommuter and the workplace.

## **List of Abbreviations and Nomenclature**

DAP – Directory Access Protocol

DBA – Database Administrator

DES – Data Encryption Standard

DMZ – Demilitarized Zone

DNS – Domain Name System or Service

FTP – File Transfer Protocol

FWSM – Firewall Service Module

IDS – Intrusion Detection Systems

IPSEC – Internet Protocol Security

IT – Internet Technology

LAN – Local Area Network

LDAP – Lightweight Directory Access Protocol

NIDS – Network Intrusion Detection Systems

NIST – National Institute of Standards and Technology

NTP – Network Time Protocol

PC – Personal Computer

SPA – Special Protocol Assessment

VAN – Virtual Area Network

VPN – Virtual Private Network

## **Introduction**

The computer has become more of an everyday necessity in our personal world to communicate with other people and in our business world to help make the creation of advance documents, drawings, and storing the information. With this advancement of technology there has been an increased need for internet and file security. More businesses have developed a need for a fast and efficient way of transmitting information for various purposes within their business. With the increased use of the computer, there is a huge concern that the information that they have stored will be retrieved and misused. Thus, it is essential that companies incorporate security measures so users both within the company and outside the company do not obtain, change, and even destroy the data that is maintained on their database.

Telecommuting is becoming more and more popular in today's workplace. Broadband Internet access, secure virtual private networks, and mobile computing technologies are making it possible for many professionals to telecommute and work remotely. According to IT experts, by the year 2011 more than half of workers in the United States will spend two or more days a week working away from the office. However, experts estimate that even in ten years it would be uncommon to find workers who telecommute five days a week, suggesting that telecommuting would not fully eliminate the need for central office locations (Cole 2003).

XYZ is a state agency that is in charge of maintaining safety for the public transportation system. XYZ gathers and stores confidential information such as employee and client information. Therefore, the use of many security measures must be maintained and regulated so that unauthorized users are unable to gain access.

One issue that this research paper will discuss is the difference between data security and network security. There are many database security measures that a corporation can implement in order to provide adequate security and this will never end. The corporations will need to continue to update their security measures as new vulnerabilities are discovered or exploited. Corporations will also need to understand and consider that when it comes to security it is a continual process. Security is not a project where it will be completed on a certain day or time; rather, it is ongoing and ever-changing process.

Wireless networking is another growing reality for most telecommuters. This type of networking enables telecommuters to access the Internet from offsite. This type of technology gives both firms and telecommuters more flexibility and the ability to be innovative in unexpected ways. To meet the growing demand for telecommuting, safety and security issues must be addressed.

Some of the threats for telecommuting are; computer viruses, password hacking, man-in middle attacks, identity theft, and social engineering. To overcome these threats, telecommuters and businesses need firewall protection, strong encryption, good authentication methods and anti-virus software. The security gurus at Tech Target's warn that the only way to make your computer completely hacker proof is to turn it off or disconnect it from the Internet. The real issue, they say, is how to make your computer ninety-nine percent hacker proof.

The following are the basic security products and method, which support my research. The items listed below are defined further in the paper.

1. Firewall
2. Virtual private network
3. Strong passwords (authentication and encryption)
4. Anti-viruses
5. Software to permanently erase files from the hard drive
7. System backup
8. Software patches, regularly applied to detect viruses and bugs
9. Hardening the “box” (the operating system)
10. Regularly scheduled operating system and application maintenance
11. File and printer sharing
12. Anti-theft devices
13. Security-conscious employees
14. E-mail and hardware encryption

XYZ must keep in mind that the information that they are storing within their system becomes less secure during transmittal over the network. A lot of research has been conducted within the computer security field to address this issue. Their goal is to figure out is how to make the database a more secure environment which makes the information more secure while stored and transmitted between networks. It is known that when you use a common design, the information is less secure. In order to increase security, XYZ needs to implement a combination of security measures that includes audit trails, database patches, IDS, firewalls, and other security measures which will be discussed within the scope this paper.

## Literature Review

Most people forget about adding security for their database because usually when people think about securing something within their computer systems, they believe that the top priority is securing the web server. Thus, the database is overlooked and left with numerous security vulnerabilities and risks. Also, individuals and corporations tend to overlook that the database is where the majority of business information is stored. If it is left unprotected, it could cause a lot of damage to the functions of the corporation as well as liability (or legal) issues. Another area to consider when implementing security to the database is that multiple entry points are available to the database information for employees and business partners. The difficulty that is associated with ensuring each of these lines are secure is the complexity of the system itself changes as the company grows (Afyouni 2009).

When XYZ stores all of the information in a single database in an encrypted format, there are some vulnerabilities that go along with this type of system. No matter how secure you try to make it, there will be risks involved. Although the database should be the most secure environment, they tend to be easy targets for attacks. When there is one database which contains all of the information that is confidential to the corporation there is bound to be security issues. For example, if an attack is made and access is gained to the database all of the company's confidential information can be obtained and misused.

Most security professionals realize that with the use of a firewall, they gain some level of security but to believe they have obtained complete security would be undermining the overall threats that are present. Also, when implementing a firewall, the

corporation has to decide how the firewall screens traffic and develops the firewall to accept or deny the incoming traffic to the system. Although this process may sound simple, it is a very crucial. For example, if a security policy is developed for the wrong reason, it could lead to the system being less secure and more open to attacks. In effect, a poorly designed firewall can lead to a system that is open to attacks from outside the system. The reason for this is because an individual may believe that because they have a firewall in place, the system is safe. However, as just stated that is the exact opposite of the actual situation if the firewall is administrated incorrectly (Maiwald 2004).

## **Firewalls**

A firewall is a network security product that acts as a barrier between two or more network segments. The firewall is a system (which consists of one or more components) that provides an access control mechanism between two networks. For those who do not know why it is important to have one, a personal firewall is defined as a technology that helps prevent intruders from accessing data on a personal computer (PC) via the Internet or another network, by keeping unauthorized data from entering or exiting the system.

The first security measure that XYZ has taken is the use of a firewall. It is believed within corporations and especially among professionals that a company cannot rely solely on the use of a firewall to complete their overall security measures. Firewalls provide the first line of defense for XYZ.

Firewalls can provide an excellent source of security as they are able to deter unauthorized users access to the database. As early discussed, alone they are unable to provide total security based on several reasons. For instance, the firewall has to allow

some files to pass through creating an environment where attacks could gain access if other layers of security are not present. Another reason firewalls don't provide total security is that there are always new threats or ways to attack the system that the firewall may not have been developed to stop (Hummel 2000).

In the book, *Implementing and Managing Telework*, by Bill Fenson and Sharon Hill, Steve Gibson, a security consultant and founder of Gibson Research Corporation, talks about work-at home computer security: "A personal firewall is important," he says. "It is like wheels to the car (p. 42)." He affirms that, in the near future, firewalls will automatically be included on computers.

As Jeff Sengstack stated in the article, "Make Your PC Hacker Proof," in *PC World*: The perfect personal firewall would be inexpensive and easy to install and use, would offer clearly explained configuration options, would hide all ports to make one's PC invisible to scans, would protect the system from all attacks, would track all potential and actual threats, would immediately inform user of any serious attacks, and would ensure nothing unauthorized entered or left the PC" (2000).

## **Virtual Private Network (VPN)**

A VPN may consist of one or many computers connected to a single computer or network of computers. A private network is a dedicated line and set of equipment with the sole purpose of allowing two or more devices to communicate securely. Dramatic increases in telecommuting have driven the use of VPN technology. VPN uses advanced encryption technology to make computer messages unintelligible while they are moving between computers. Although the VPN's traffic crosses the Internet, VPN protection prevents most unauthorized users from reading and/or modifying the traffic. Even though encryption is secure, hackers have techniques that can foil this security. In particular, spyware or viruses on the computer can sniff passwords and thereby circumvent the VPN security, putting the organization at risk.

## **Strong Password**

As hackers try to penetrate into one's computers, telecommuters need to protect their systems with the use and selection of good passwords. Usually, strong passwords mean hackers can be deterred from entering the computer system because of the length of time that it takes them to break into a system. For telecommuters, the best advice for choosing good passwords would be a combination of upper and lower case letters, numbers, and special characters (Vernon 2005).

### **Anti-viruses**

For added protection, anti-virus software programs exist to protect telecommuter's computer systems from viruses, worms, and Trojan horses. Anti-virus programs are designed to scan a computer system to find and rid the system of such malicious programs. They are effective against known viruses but they are not effective on unknown viruses or on computer systems that have not been updated.

### **System backup**

Telecommuters need to have removable hard disks or devices to allow information to be kept separate from the computer. For security purposes, this also allows the telecommuters to have duplication in case of theft, damage, or destruction. As a means to educate telecommuters on how to secure their systems, the rest of the above list (starting from 8 to 13) should be very helpful in order to prevent hacking.

### **External and Internal Attacks**

To reduce the likelihood that hackers, either through internal or external attacks, will obtain confidential information from the database, companies should use multiple database servers. That way, you have some information stored on one server and other information stored on a different server. Thus, if a hacker gains access to the database, they will only obtain partial information.

One way that we have increased the security of the application server is through a simple measure of removing the protocol or encryption keys from it. That way even if an

attacker gains access to the application server there is no real information that they can retrieve. The only thing that the application server does is collect information or data from the web server and then transmits it to the database server. Thus, the only real information that the individual attack may be able to obtain access to is packets that are being collected and this is a very small level of compromise compared to if they were to be able to gain access to the whole database. With the encryption keys scattered among three different database servers, if access was gained to the database server the intruder would not be able to acquire the complete information from the company and would not be able to misuse information that they did obtain. The only way the attack would be able to gain confidential information that they would be able to fully use would be by obtaining access to all three database servers. The only way they would be able to gain access to all three database servers would be by getting access to all three addresses and then accessing the data. All of this would need to take place while not being detected, which is highly unlikely.

Similar to this procedure, the job of controlling the three different servers would be distributed to different individuals. That way if the information from one database server is compromised then it would only affect that one database server. There are security issues with the database because they lack settings that are controlled by company policy or government regulations. Furthermore, the user accounts are not controlled or secured by password controls which are supported by dictionary checks and the passwords do not expire. Thus, if a single user account is accessed the whole system is at risk.

## **Network Intrusion Detection System (NIDS)**

A very important part of security and an additional measure of security with the firewall that XYZ adds to their database security measures is the Network Intrusion Detection System (NIDS). The NIDS measure is designed to oversee the transfer of information over the LAN. The overall function of the NIDS system is to alert security personnel that an attack is being made and whether or not they have succeeded in breaking in or are in the process of breaking into the system. Also, the NIDS system can provide important information about the traffic that is coming into the network and if the traffic poses any security threats (Newman 2005).

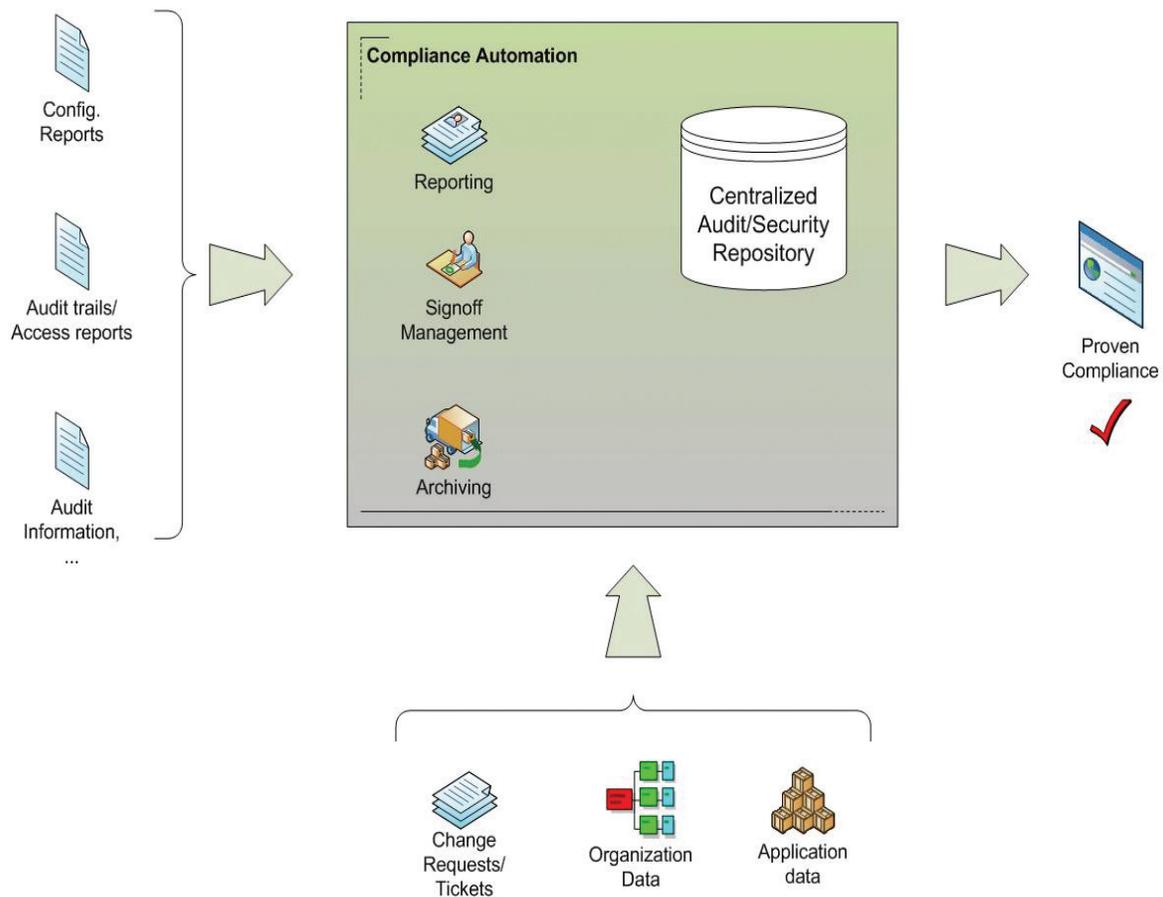
As with firewalls, the NIDS system cannot stand alone as the only defense mechanism because NIDS primary focus is on detection of the intrusion. Also, although the NIDS will notify security personnel, by the time they have time to respond it would be too late. In addition, the intrusion detection systems primarily protect against intrusion which were previously detected by the system. The system then has to be configured to detect attempts that are against the normal transmission of information. The normal transmission has to be set up and defined loosely. Otherwise, the system would generate too many alerts.

## **Network Sniffers and Proper Encryption**

Network sniffers try to steal information as it is transmitted through the network from the client to the application server. Once they gain access to the information, they will misuse it. In order to try to deter these network sniffers, XYZ will want to

implement the use of encryption of the data while they transfer it through the system (Maiwald 2004).

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. An encryption process can be reversed or decrypted only by someone who has the security key. Based on the cost of encryption services, XYZ will determine which information is the most important to have encrypted. The figure below shows the process of managing the entire lifecycle for (Natan 2010)



**Figure 1 Compliance lifecycle**

The system that XYZ will use is confidentiality protection, integrity protection, and non-repudiation protection. What that means is that the information that is

considered confidentiality will receive protection from revealing information to unauthorized entities. Thus, the encryption will be via VPN. The information that is integrity level protection is at a level where preventing data from being modified or manipulated from its original state. In some cases, only integrity protection may be required, and then confidentiality protection would not be required. The non-repudiation protection level contains proof that a third party was the originator of a transaction and that the message was not modified.

Database administrators believe there are different ways to counter the act of having data directly accessed through the operating system by having the information encrypted. Encryption should be used whenever data is communicated to other sites, this way if someone gains access, they will not be able to understand the data that they obtained. Therefore, encryption requires a chipper system which consists of the following elements (Afyouni 2009).

1. **Encrypting algorithm:** This takes the normal text, as input, performs some operations on it and also produces the encrypted text, which is usually a cipher text, as output.
2. **Encryption key:** This is basically the part of the input for encrypting the algorithm, and usually chosen from a large set of possible keys.
3. **Decrypting algorithm:** This usually operates on the ciphertext as input and can produce the plain text as output.
4. **Decryption key:** This is basically part of the input for the decrypting algorithm and usually is chosen from a large set of possible keys. Currently, there are many encryption algorithms available in the market. There are some that are widely used

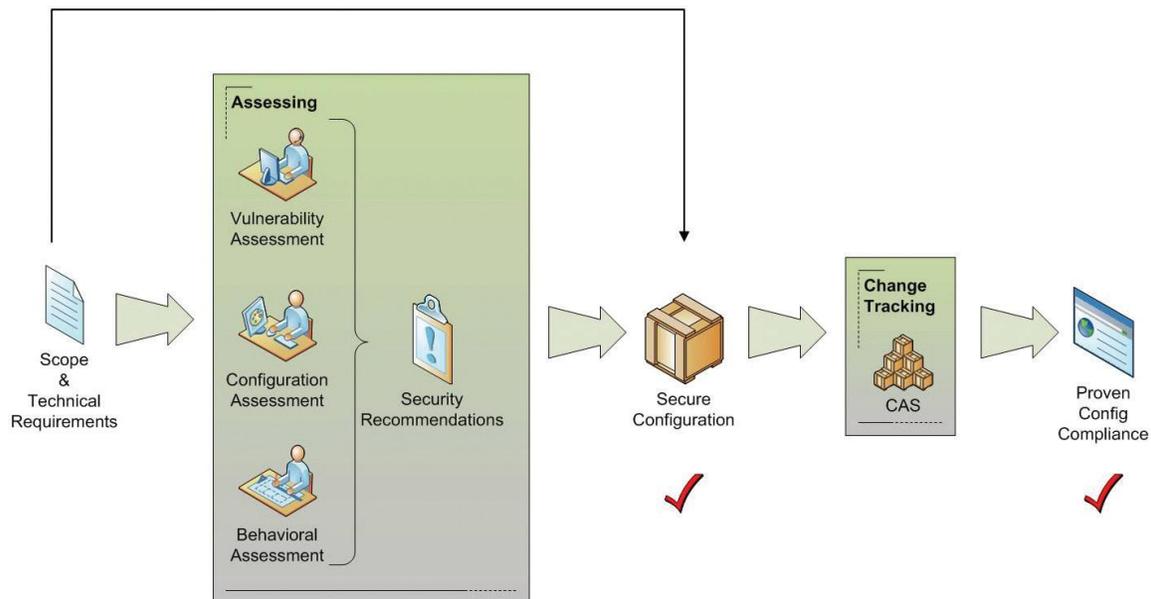
such as those developed and supported by Oracle. Also, there are different categories of algorithms such as private key and public key. The private key would probably be strong enough for my corporation's needs. This type of private key is commonly called symmetric. With this type of encryption, you use a key to encrypt the information and then with the same key, you can decrypt the original information. The only way to decrypt the encrypted information is by having the exact key that was used to encrypt the information and the only way to obtain the key is to have it transmitted to you.

Above all, I believe the strongest and the best algorithm is the one used by Oracle which is called Data Encryption Standard (DES). DES is very well known and is the most widely used encryption since it was developed more than two decades ago. This algorithm usually requires a 64-bit key, and usually discards 8 of them, creating an encryption key using 56 bits. In this type of encryption algorithm the (DES) is a very strong and powerful algorithm. Also, National Institute of Standards and Technology (NIST) would have the best technology to come up with the best encryption algorithm which will continue to remain the best.

# The Need for Security

## Database Security & Integrity of XYZ's Database

There are security issues in making one individual in charge of securing the database. Generally, administrations entrust the database administrator (DBA) to do the best that they can to protect the privacy of the company. This person will either do their best in protecting the database system or they could cause the most harm. If the DBA is given too much authority and control without any restrictions, the whole system could become compromised. Thus, the whole system could become compromised if a DBAs account is compromised. If you want to add more security to this type of system, you would want to use segregation of duties and systems as shown in Figure 2 (Natan 2010). This way, there are more than one DBA and not one of them can make changes without the permission of the other DBAs. That way more security is added because not one person is entrusted with all of the power.



**Figure 2 Vulnerability Assessment**

Within XYZ, DBAs are responsible for the development, maintenance, and integrity of the database. They are responsible for system security in the designing, developing, organizing, managing, and controlling the database in accordance with company's security policies. They are also responsible for providing the security access administration function with the necessary information to maintain user IDs and privileges. Lastly, they are responsible for recovering databases in a secure manner when damaged or compromised. Furthermore, at XYZ there are a number of DBAs who work as a team. They all share the above duties and as this paper has already described, they share the responsibilities so no single DBA has too much power. They all have to agree on the changes to any security measures before the change can occur.

### **Developing a Database Security Plan**

XYZ has installed several audit trail devices into their working database system. Some of these devices are Top Secret and CA-Unicenter or other Windows security tools. These tools are able to record and report all security administration activities. Also, they are able to retrieve current and historical information about security administration and activities in the event that a system fails.

In order to save disk space or increase performance, auditing capabilities of the database are sometimes forgotten about or left out. The audit trails are a very important part of any database system for the simple fact that they increase the ability to track data and who accessed what information. Also, the forensic capabilities would be decreased if there were no audit capabilities activated.

Security administration products and procedures must log all security violations. Resultant log files are reviewed by security administrators and data owners to detect any unusual or inappropriate activity. In addition, it checks against authorizations and pays special attention to unusual times, frequency, and length of accesses.

Furthermore, procedures currently exist at XYZ that are able to maintain the integrity of access tables within security enforcement software. The procedures also include triggers to ensure userids for Users terminating their existing responsibilities are suspended or deleted. In addition, each Division, Bureau or Office shall assign a person who will have the responsibility of contacting the Computer Services Department when changes of this nature occur.

The most basic network security includes measures such as intrusion detection systems (IDS) and firewalls. Both of these are the first step in creating mechanisms that will block the first attack to the system. Although, as previously discussed, there are many measures or different devices that can aide in the overall protection of the database. As a state agency, XYZ has taken many steps in protecting the overall database information that is stored. Some of the confidential information that XYZ stores are: employee information, client information such as police records, accident reports, community resource information, and statistical information. Thus, there are many things that XYZ needs to consider when developing the most secure network. The following are the steps that XYZ has taken and implemented so that it has a multiple level security design.

## **Implementing the Improved Security**

### **Application Security**

XYZ is trying to integrate a level of security that does not have just one application rather instead they will use several different layers that work together to make a more secure environment. For instance, they may start with a firewall and then add a process of securing the application servers. With this type of approach, the corporation hopes that the overall result will make the secure environment less accessible by unauthorized users. A company's image can be damaged if confidential information is obtained by an unauthorized user. Thus, as we all know the first step in making an environment more secure is to first identify the corporations' vulnerabilities and then develop ways to reduce the vulnerability to make it less likely that an attack will be made. Also, security professionals all agree that the best security measure is not one but multiple measures to create the most secure environment.

There are a number of ways to increase security within XYZ. According to one of XYZ's DBAs, the more that you aim at securing the transmission of data from a Web server to the application server and also securing the information that is stored in the database, the more the company will be able to decrease the risks that are present for unauthorized users to gain access.

### **Further Security Improvement**

Lightweight Directory Access Protocol (LDAP) is often used to gain access and to interact within a directory. For instance, a client would access the directory using LDAP to find a specific certificate. The old system was the Directory Access Protocol

(DAP) was used until the University of Michigan came up with the LDAP. The LDAP proved to be much more efficient in retrieving information than the DAP. Thus, it is now considered to be the more acceptable way of retrieving information on a directory (Afyouni 2009). Also, as the author mentioned, LDAP is easily distributed to many network servers such as Apache Servers, Windows Servers, etc.

In order to implement the LDAP, there first has to be set policies that outline the use within an organization and its users. These policies would include the following:

- **Confidentiality** which would outline the way employees could access the information. This policy would inform the users that the information in the server is very sensitive and should not be given out to others. Thus, employees awareness of the importance of confidentiality would prevent, deter, or detect the misuse of information that was obtained off the server that could include giving the information out when they shouldn't have.
- **Integrity** of the information would ensure that the user does not change any information without going through the proper channels. Some type of access control would be implemented to help control the integrity.
- **Authentication** which is automatically built into the LDAP. They include general, simple, and strong. The general is read only. With the simple, the user would be connecting only after the correct ID and password were entered. With the strong, the user would only be connected after entering the certificates or public keys.
- **Non-repudiation** is one measure that would ensure that the user was actually the one who sent the information. Non-repudiation, which is the use of a digital

signature, does not provide enough proof of who signed it and would not hold up in the court of law because they cannot prove who signed it or sent the information.

- **Backdoor Access** indicates that an organization would want to ensure that the organization upholds confidentiality, the organization must make sure that there is no way that someone can gain access to the network or the server and retrieve information from the directory.
- **Gateway Layer:** This layer determines who is allowed into or access to the system. Regulations that you need to consider within this layer are where the access is going to be granted such as network or host-based connections. The security measures that are usually used within this layer are firewalls, VPNs, physical access, and intrusion detection systems. When developing security for this layer, you would need to look at protecting against Denial of Service attacks. You must ensure that the firewalls are configured correctly. If the DoS attack gets through at this level, the damage may be minimized at the control level.
- **Control Layer:** This layer determines which layers can be accessed within the server. The security that needs to be considered at this level is the need of confidentiality and integrity of the data and someone trying to hack the system. Some of the security measures that need to be considered are removing any unnecessary services or programs, not running LDAP on the same host as other services that you have, keeping some of the information isolated such as the file store from the network, and being objective when determining what administrative rights you give to the server.

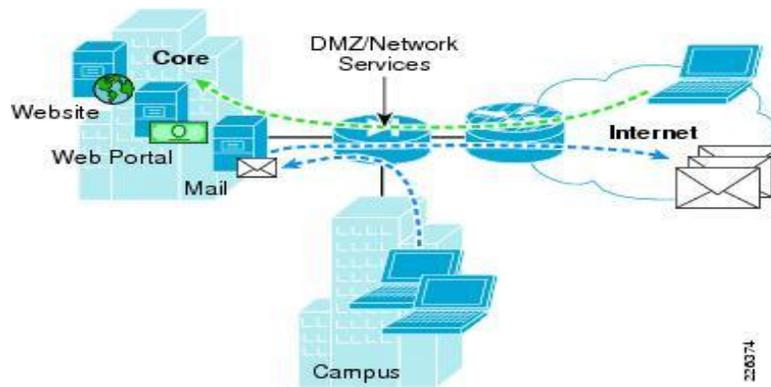
- **Data Layer:** This layer determines what can be done to the information that can be accessed. Some things that you will want to consider are you will need to consider what information you want to keep private and what information you want to keep public. With the public information, you could consider having that information be obtained outside the firewall. You will also want to consider using LDIF (LDAP Data Interchange Format) which are files used to transfer information between directories or into the directory. If using the LDIF, you will want to verify all the information received from an outside source given the LDIF does not use any method to authenticate the information. Lastly, you will want to consider running directories as a single-application kernel-only machine that fail to a halt. That way you would lose access to the data rather than losing the integrity of the information.

Above all, the policy and implementation methods that I discussed are just the beginning to providing a secure LDAP system. The policies will need to continue to be constantly updated and protected as new threats are detected within the system or changes need to be made to the data.

## **Findings**

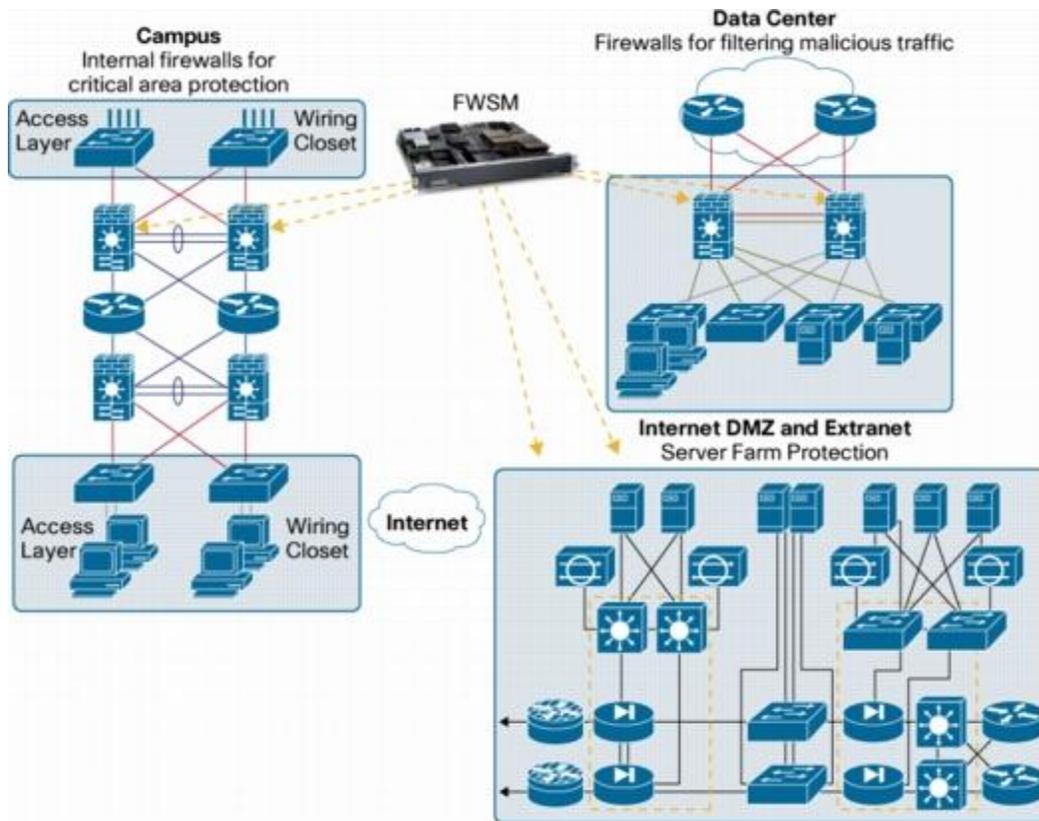
There are always additional measures or features that you can add to help insure extra security. One additional measure would be to add an extra firewall which would be configured to a separate network which is detached from the demilitarized zone (DMZ). Please see Figure 3 for DMZ Topology (Cisco Systems 2009). According to Bradley Mitchell from Computer Networking, he reports that with a DMZ configuration the

computer runs on a LAN that has a firewall behind it. The computers that are outside of the firewall intercept traffic and broken requests for the rest of the LAN thus adding extra security. This way, when you configure to only allow very limited traffic, XYZ will end up with a more secure database server. Thus, if an attack is made to the DMZ, the second firewall will help protect against the intruder gaining access to the database server.



**Figure 3 DMZ Topology**

Network services that are normally provided through the DMZs include DNS, FTP, and NTP. DMZs usually include services such as email and other web security appliance as shown in Figure 3 (Cisco Systems 2009). You can expect to receive reliable service availability through the use of the DMZ design; there will be regulatory compliance of set standards, and a strong security. Some of the security that you can expect to receive while using the DMZ design includes: the ability to prevent intrusions, data linkage and fraud, and unsure user confidentiality and data integrity (Mitchel 2007).



**Figure 4 Secure LAN Deployments in the Data Center**

Enterprise campuses, data centers, or service providers rely on network topologies such as the Cisco Firewall Modules (FWSM). The reason why they depend on the FWSM is because of its ability to maximize capital investment while providing the best price performance ratio in a firewall (Nadimi 2009). An additional convince in using the Cisco FWSM is that companies can set appropriate policies for the different VLANs that the company may use. Furthermore, the data centers require firewall filter traffic that poses a security risk thereby adding additional protection to the company's data in the Demilitarized zones (DMZ) and extranet server farms. Also, to further enhance security, the FWSM can be added to the Cisco IPSEC VAN SPA to enforce firewall policies per VAN tunnel defined by VRF

## Conclusion and Recommendations

As we know, there is no database that can be created that will keep out every attack. We also know that attackers will always try to gain access to any company. The reason behind security is so that the risk to the company can be reduced and so they can take all measures possible to keep their environment free from attacks. There are a number of things that companies must consider, such as cost effectiveness, vulnerabilities present and most confidential information. A company also has to keep in mind that the effort to keep an environment safe is a continual process. The computer environment is constantly changing. In order to meet budget considerations and a changing environment, companies also need to consider two important questions such as “is this a measure that I can continue to add and build upon” or “am I going to have to add a completely new product/measure in the future as attacks change or the company grows?”

Also, as a telecommuter, the companies should recommend providing their employees with the best firewalls available to their employees working outside the office. The best software is the one which serves business needs and is based on the network infrastructure and business environment. Personal firewalls are designed in such a way that it is easy to install and operate, and can significantly reduce the risk of intrusion. The rationale of having a firewall is to keep out hackers and permit or deny certain traffic in/out of the network. The firewall is one of the building blocks of a well-designed security structure.

The table below briefly gives the different types of firewalls and its availability whether it costs or not. The table also lists the supporting features of all the chosen products.

### Manufacturers of Software Personal Firewalls

<b>Personal Firewall Products</b>	<b>Website</b>	<b>Cost</b>	<b>Platforms</b>
McAfee Internet Security Suite	<a href="http://www.mcfree.com">www.mcfree.com</a>	\$49.99 - \$69.99	Windows
Norton Internet Security 2011	<a href="http://www.symantec.com">www.symantec.com</a>	\$69.99 - \$99.9	Windows
ZoneAlarm Internet Security Suite 6	<a href="http://www.zonelabs.com">www.zonelabs.com</a>	\$49.95	Windows
Trend Micro PC-cillin Internet Security 2011	<a href="http://www.trendmicro.com">www.trendmicro.com</a>	\$49.95 - 124.95	Windows
Smooth Wall	<a href="http://www.smoothwall.org">www.smoothwall.org</a>	Free	Linux
Sygate Personal Firewall	<a href="http://www.sygate.com">www.sygate.com</a>	Free	Windows
Tiny Firewall	<a href="http://www.tinysoftware.com">www.tinysoftware.com</a>	Free	Windows

Some of the security products mentioned in the table are the newest releases of McAfee, Norton, and ZoneAlarm and are available for telecommuters and businesses. Currently, Norton and ZoneAlarm are the best products for telecommuters and businesses. Both of the products offer competitive prices and excellent features such as anti-virus, spy ware, spam filters, e-mail security, intrusion detection, and built in firewalls. Based on the analysis and comparison from the table above, Norton seems to be the best fit based on price and excellent features for XYZ.

Additionally, Norton offers anti-virus tools at start-up, works in the background, quarantine suspicious files, watches for downloaded viruses and automatically configures itself to handle a wide variety of e-mail accounts. Many businesses recommend Norton for their needs.

Finally, I believe that the approach that has been recommended for XYZ's database server such as the firewall, multiple servers, encryption, NIDS, and extra security by

adding the second firewall to a separate network creates the most secure environment possible given their current business size and needs. Thus, once XYZ implements these recommendations, it will be more equipped to handle the possible attacks made and reduce the risks that are present.

## References/Bibliography

- Afyouni, H. (2009). Database Security and Auditing. Boston, MA. Thomson Course Technology.
- Chapple, M. (2010). Guide to Databases. Accessed on June 10, 2010  
<http://databases.about.com/od/security/a/aasecuritytest.htm>
- Cole, L. (2003). Fast forward: 25 Trends That Will Change the Way You Do Business. *Workforce Management Magazine*, pp.43. Accessed on June 12, 2011 from Lexis-Nexis
- E-Week (2006). Database Security. Accessed on June 18, 2010  
<http://www.eweek.com/article2/0,1895,1916991,00.asp>
- Fenson, B., & Hill S. (2003). Implementing and Managing Telework. Connecticut: Praeger Publishers.
- Hummel, R. (2000). How It Works: *Personal Firewalls*. Accessed on June 27, 2010  
<http://www.pcworld.com/howto/article/0,aid,17012,00.asp>
- Maiwald, E. (2004). Fundamentals of Network Security. McGraw-Hill.
- Mitchel, B. (2007). Demilitarized Zone (DMZ). Accessed on July 5, 2010  
[http://compnetworking.about.com/cs/networksecurity/g/bldef\\_dmz.htm](http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm)
- Newman, A.(2005). Database Activity Monitoring. Accessed on July 6, 2010,  
[http://www.appsecinc.com/presentations/DAM\\_wp82305.pdf](http://www.appsecinc.com/presentations/DAM_wp82305.pdf)
- Nadimi, A (2009). CMO Enterprise Solutions Engineering, Cisco Systems
- Natan, R. (2010). 8 Steps to Holistic Database Security. Guardiam (IBM)
- Palmer, M. (2003). Guide to Operating Systems Security. Boston, MA. Course Technology.
- Phifer, L. (2003). Securing Teleworker Networks. *Business Communications Review* Vol.33, Iss.10, pg.28. Accessed January 10, 2010 from ProQuest.
- Rohan, R. (2004). Letting the Telecommuters into the Network. Accessed on January 12, 2011, <http://www.ciscopress.com/articles/article.asp?p=354571>
- Riley, C. (2003). Best Damn Cisco Book. Everything You Need to Know About Cisco Internetworking Technologies. Rockland, MA. Syngress Publishing, Inc.

Sengstack, J. (2003). Make your PC hacker-proof. *PCWorld.com*. Accessed on February 17, 2010, <http://www.pcworld.com>

Shinder, D. (2003). Lock IT Down: Create Security Policies to Address Telecommuting Trouble Spots. *InformationWeek Magazine*, Accessed on February 15, 2011 <http://www.informationweek.com>

Vernon, M. (2005). Financial Services Telecommuters Require Strong Policies and Business Processes for Success. Accessed on February 21, 2011 [http://techrepublic.com.com/5100-10878\\_11-5882860.html?tag=search](http://techrepublic.com.com/5100-10878_11-5882860.html?tag=search)

## **Appendix A – Computer Security Survey**

When looking at what security measures a company should install, they should come up with a set of questions that will ask some basic questions and assess what security issues might be present. This Appendix A includes a survey that can be used as is or modified to better meet the company's needs for improved security.

### **Demographic Information**

#### **Age**

- A. less than 18
- B. 18-23
- C. 24-32
- D. 33-41
- E. 42-51
- F. 52-63
- G. 64 or older

#### **Job Status**

- A. Student
- B. Employed Full Time
- C. Employed Part Time
- D. Self Employed
- E. Other

#### **Education**

- A. High School
- B. Some College

- C. Attained Associates
- D. Attained Baccalaureate
- E. Attained Masters
- F. Attained Doctorate

**Estimated Hours Spent on the Computer**

- A. 0-5
- B. 6-10
- C. 11-15
- D. 16-20
- E. 21-30
- F. 31-40
- G. 41-50
- H. Over 50

**Do you use a computer regularly at?**

- A. Home
- B. School
- C. Work
- D. Other

**You connect to the internet by:**

- A. Dial up Modem
- B. Cable Modem
- C. DSL service
- D. Satellite

- E. WebTV
- F. Don't connect
- G. Other

**How many people are in your household?**

- A. 0-5
- B. 6-10
- C. 10-15

**How many computers are in your household?**

- A. 0-3
- B. 4-6
- C. 7-9

**Do you have a home network?**

- A. Yes
- B. No

**How many total usernames/passwords do you keep track of?**

- A. 1-5
- B. 6-10
- C. More than 10

**How many of the passwords are unique (not using any of them more than once)**

- A. 1-5
- B. 6-10
- C. More than 10

**Do you use email regularly?**

- A. Yes
- B. No

**If yes, do you use**

- A. Web-based (Hotmail, yahoo, etc.)
- B. Other (Outlook, Lotus Notes, Netscape)

**Do you use any kind of portable information management device?**

- A. No
- B. Palm OS based
- C. Pocket/ Windows CE

**How often do you “patch” software?**

- A. Daily
- B. Weekly
- C. Monthly
- D. Quarterly
- E. Yearly
- F. Wait for new version
- G. When I have to
- H. Don't

**Yes/No Questions**

Are any of the passwords you keep track of shared among a few or many individuals?

Do you often leave your home or work computer logged on?

Has your computer ever been infected by a computer Virus, Trojan, or another malicious computer program?

Do you know of somebody who's computer has been infected by a computer Virus, Trojan, etc.?

Do you perform any kind of backup of your personal data?

Do you use any wireless technology at home or work?

Do you use any kind of Firewall at home?

Do you run some sort of Virus Scanner?

Do you use any kind of encryption?

Do you believe that it is possible to have secure transactions on the internet?