# Securing the Corporate Network

by

A.J. Siroin

A Research Paper
Submitted in Partial Fulfillment of the
Requirements for the
Master of Science Degree
in

Management Technology

Approved: 3 Semester Credits

Steve Schlough

Dr. Steve Schlough

The Graduate School

University of Wisconsin-Stout

December, 2005

**The Graduate School**
**University of Wisconsin-Stout**
**Menomonie, WI**

**Author:** **Siroin, Arnold J.**

**Title:** ***Securing the Corporate Network***

**Graduate Degree/ Major: Management Technology**

**Research Adviser:** **Steve Schlough, Ph.D.**

**Month/Year:** **December, 2005**

**Number of Pages:** **34**

**Style Manual Used:** **American Psychological Association, 5th Edition**

## ABSTRACT

Security, security, security is all that we hear about in today's internet world. The need for security in any network is crucial. This project takes a look at what the industry is doing regarding security and what XYZ must do to maintain their corporate goals. The primary goal for XYZ is to make sure their corporate network is secure and highly available. Clients and customers must be able to access their information via a secure website or a secure connection back to the corporate network. Providing a highly available and secure network can only increase the service that is provided to clients and customers. XYZ's reputation was built on service. XYZ wants to maintain their quality of service, but still provide the best possible corporate access to their client's or customer's data. There are many tools out there to choose from and many vendors that provide the functionality needed. The goal is to make the correct decision in choosing a solution or direction. Know that what is put in today, may be obsolete tomorrow due to the ever changing world. The internet is a huge network in itself, but security is not its main attraction. Corporations utilize the internet for business. Securing XYZ's

information and restricting access back to XYZ’s corporate network is the goal of the researcher and XYZ.

## TABLE OF CONTENTS

# Chapter I: Introduction

We live in a world where the internet is a vast source of information that is easily accessible from almost anywhere in the world. The internet started as something small and has become the mammoth giant we all know today. Any kind of information can be found on the internet. Anything from newspapers, entertainment headlines, company information, and the list goes on.

The internet is not only an information repository, but it is also a media for data communications. The internet backbone is built upon multiple large networks that interconnect with each other. It is virtually impossible to map out each and every network that forms the internet because of its vastness. The key point is that the internet is based upon sharing of information and sharing of network infrastructure to create this massive information store.

Corporations utilize the internet to help run their businesses. The reason they do this is because the information they want shared to their customers can be easily accessible from the internet. Corporations spend valuable time and money developing websites that will provide their customers with the data and information they need to do business. The corporation is then left to support the website and allow their information be accessed by millions of people wherever they are in the world, as long as the customers have a computer and an internet connection.

The internet is a useful tool for many corporations. It provides a dynamic way for customers to access information located at corporate headquarters. If the internet is such a vast information store that is open to the world, how does the information get securely transmitted over this public information transport? Security is a colossal part of utilizing the internet. Corporations spend millions of dollars on securing their network to provide their customers with the information they need to maintain their business relationship.

Not only do corporations have information that they provide for their customers, but they also have information that they provide for their associates as well. Most corporations have associates scattered throughout multiple buildings, cities, states, and even countries. The same concept has to be applied when thinking of these associates and that is to give them secure access to the information. When associates are located inside the corporate infrastructure, they are considered to be on the Local Area Network (LAN). These associates are considered part of the corporate infrastructure.

There are associates that reside in different parts of the city or different parts of the country that need access back to the corporate infrastructure. When associates are located outside the corporate infrastructure, XYZ must provide a secure path back to the corporate infrastructure. These associates are considered to be on the Wide Area Network (WAN). These associates are still considered part of the corporate infrastructure but they are treated different because they are not connected directly to the LAN. Security is a crucial piece of every network infrastructure and it is vital in the WAN environment. The internet has become a viable option for corporations to use for their connectivity between their LAN & WAN.

Remote offices are typically offices that have their own LAN infrastructure (workstations, servers, printers, etc) deployed and communicate back to the corporate infrastructure via the WAN. Users located in the WAN that need information that exists in the corporate infrastructure are totally reliant on their own communications link. XYZ's remote offices have people who are normal users that just know the business

**Purpose of the Study**

The problem stems from the relationship between remote offices and the corporate business model. XYZ Corporation does not have total control over their remote sites. These offices operate as independent businesses and have the need to get back to XYZ network to receive e-mail and other specific business applications over a Virtual Private Network (VPN) and then communicate over the WAN to get back those applications. The trend for XYZ's business applications is to move them to web-based applications that would eliminate the need for their connection back to the corporate network over the VPN tunnel.

XYZ's remote offices have a vested interest in being connected back to the corporate network due to the Service Level Agreement (SLA) that is provided to the remote offices. Under this agreement, support is provided to them for connectivity, business applications, and core LAN equipment they have at their location. Whatever solution would exist, the current SLA needs to be satisfied.

In August of 2003 when the SQL Slammer worm crippled XYZ's corporate network, it was because of remote offices that the virus did its damage. It seemed to cause stress within XYZ and looking at disconnecting these offices from the WAN seemed like the right option. Taking them off the WAN would eliminate their connection back to the corporate network. Providing website access where clients can get to anytime and any place is a strategic direction. Since August 2003, XYZ and its remote offices have made substantial gains in trying to prevent viruses, hackers, and useless traffic from hitting the corporate network. In speaking to a Director of Network Technology at XYZ Corporation, the goal of the network team is to make sure that the corporate data is secure, safe, and accessible. Do whatever it takes to make this happen. What technologies are out there? What is the best practice for securing networks? Is what XYZ Corporation doing today heading them in the right direction? Remote offices: do they need to change?

### Assumptions of the Study

Budgets are a major part of business. Not everything can be done in one month or even in one year. Corporations have a fixed amount they can spend on technology. For this study, let us take the stance that there is a fixed amount to spend, even though the amount is unknown.

All changes are not immediate. Normal change processes need to be followed so that other areas or parts of the business can remain functioning. For this study, the stance is going to be that there is a change process and it must be followed.

XYZ is a corporation in the United States and it has a product to offer its customers without actually saying what the product is. XYZ Corporation provides a service to their clients and customers.

The researcher is a major player in the Network Engineering team of XYZ Corporation. The researcher's theories and knowledge about engineering and supporting XYZ's infrastructure and clients have developed over the years. Every remote office is connected to the internet the same way.

### Limitations of the Study

The focus of the study will be on a corporation that will remain anonymous due to legal and technical concerns. Throughout this paper, the corporation will be known as XYZ Corporation.

**Definition of Terms**

*LAN – Local Area Network* – Local computer network for communication between computers; especially a network connecting computers and word processors and other electronic office equipment to create a communication system between offices.

*WAN – Wide Area Network* – A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

*SLA – Service Level Agreement* – A deal upon which two sides agree upon for either support or a product agreement.

*Routers* – A network infrastructure component that helps route packets through a LAN and WAN.

*Firewalls* – A security device to protect a LAN & WAN.

*Workstation* – A computer that conducts meaningful business processes.

*Server* – Stores information on a LAN so that multiple workstations can access the same information.

*Printer* – Gives users a hardcopy of what they see on their screen.

*SQL – Standardized Query Language* – A standardized query language for requesting information from a database.

*Client-Server Applications* – A relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request.

*Data Communication* – The transmission and reception of data between locations

*IPSec* – A tunneling protocol used in establishing & maintaining a VPN connection

*VPN – Virtual Private Network* – A private data network that makes use of the internet or any other IP network, maintaining privacy through the use of a tunneling protocol (IPSec) and security procedures.

*Remote Offices* – End users in a LAN that are totally reliant on the WAN connection to be functional and productive.

*Virus* – A computer program built with the ability to modify other programs usually to disrupt computer systems.

*Worm* – A computer program similar to a virus, it just keeps building upon itself to disrupt computer systems.

*Project Management* – A controlled process of initiating, planning, executing, and finishing a project.

*IPv6* – Internet Protocol version 6 – The latest iteration of IP for the internet. It is not a highly used protocol at this time.

# Chapter II: Literature Review

The purpose of this chapter will be to look at what XYZ is doing along the lines of securing their network. It will look at how they are handling their remote offices and protecting them from viruses, hackers, and useless traffic. The ideal situation would be to find out that XYZ Corporation is correctly and effectively securing their network. The researcher is going to try and find ways to tie in what XYZ is doing with what other corporations are doing in the network security realm.

## XYZ Corporation: Management View

In speaking to the top Director of Network Technology at XYZ Corporation, the goal of the network team is to make sure that the corporate data is secure, safe, and accessible. Do whatever it takes to make this happen. The main statistics that XYZ management cares about are network uptime and that data is never compromised. Network Technology management has reports they provide to higher management that help make the decisions whether or not to increase or decrease certain parts of the infrastructure where needed. These reports are used to develop goals and benchmarks to go by year after year. Each year the goals should increase. Incentives are usually based on these goals. The more the system is up; the more incentive it is for management to have a secure, safe, and accessible network.

The researcher also interviewed an Associate Director of Network Technology at XYZ Corporation. The director's concern was not the remote offices being looked at as the sole security risk, but the whole network as a security risk. The problem with viruses and spyware is workstations can get these infections from any place on the internet.

In August of 2003, the viruses were spreading like wild fire and the remote offices were the biggest culprits. Odd enough, there were workstations on the campus network that caused some issues as well. XYZ's engineering department and business area management have done several things since August 2003 to help prevent such chaos in the network again. After all that has been done to solidify security and malicious traffic, only the servers on the corporate network are truly secured pieces of hardware. This is due to the fact that these devices never leave the network and have current patches and virus software. The problem with all the workstations is that some of them can leave the corporate network and plug into an unsecured network connection and become infected with a virus.

> The only truly secure computer is one that's unplugged and buried deep – or so it's been said. Unfortunately, you can't disconnect and bury your servers to keep them safe. You can, however, move access control from the user domain to the device domain. Anyone can punch in a user name and password and gain access to a secure resource, but if a device must be checked out and approved in order to connect to a host, you're in control of who accesses your network. (Schultz, 2005, pp 18-19)

Management in the engineering department has expressed its concern about the fact the servers are now a hardened part of the network infrastructure. The concern they have is the workstations on the network. Management's view is what can be done to prevent these workstations from infecting the corporate network. Scan & Block technology would eliminate the vulnerability for this bad traffic to come through. Cornell is utilizing the Scan & Block technology. There may be other terms that are used for this technology but for this paper the researcher is going to refer to it as Scan & Block. The basis of Scan & Block is to grant access to the network only if it passes the strict list of security policies that are defined on the Scan & Block system. If the device does not have the correct anti-virus software installed it will send it to a remediation area where the device can get the specified software and download it. Only then will access to the network be granted to the device. Corporate devices on the network are just as likely to cause issues on the network as devices that reside in remote offices. If a person has been on vacation for two weeks and has not been on the network to get the appropriate patches and downloads, then that person is a potential threat to the network. If it is a laptop device and the device is placed on an unsecured network connection during vacation and becomes infected with a virus or worm, then it is a potential threat to the network. Qualys and Vernier Joint Systems give a good explanation on what Scan & Block technology can do for a corporation.

> Enterprises have realized that providing hard-shell security at the perimeter and going soft on the internal LAN and remote (VPN) networks is not sufficient to ensure network integrity and thwart outbreaks before they occur. Even if an infected node exists on the network it can bring down the entire network. The notion of the outside world being bad and the inside being good is not true anymore. Guarding and protecting the internal network is critical in providing a pre-emptive, pro-active and reactive security infrastructure. Challenges in doing so include auditing the endpoints for their security posture enforcing usage policies, and setting up a quarantine and remediation infrastructure. (Network Access Management Solution, 2005)

XYZ Corporation has been looking into the Scan & Block technology for the last year or so due to the issues XYZ has had with affected workstations. It has become such a highly viable option for XYZ that a project is being started to look into Scan & Block for the corporate network. Scan & Block technology can secure the corporate network from workstations that are on the LAN, as well as push this technology out to the remote offices and have the same effect on them. XYZ can truly manage the risk at one central location instead of trying to rely on the users and workstations together getting the correct updates. Scan & Block will do all of this for them.

In speaking with upper management from the business side of XYZ Corporation, the researcher was given some good examples as to why security is an important component of doing business. Take for example the data that the clients access and the location of this data. If important corporate data is located at device level, this is a security concern. Client data located at the corporate headquarters behind numerous security devices is more appealing to the business areas. Thanks to complex perimeters, sophisticated application-level threats, and regulations that hold Chief Executive Officers (CEOs) and Chief Information Officers (CIOs) accountable for company data security, must now be regarded as more than a bunch of technologies tacked onto the network. "Companies are realizing they must approach security at the enterprise level" (Erlanger, 2005). The problem comes into play that clients have to be able to access their data. This means that the corporate network/security infrastructure must remain up at all times so that the data is always accessible to operate the business functions. Getting the corporate infrastructure secure is the best possible way to secure the data. This way, if the end user needs the information, it is just a secure connection back to the corporate network. With the internet becoming more and more a mainline communications path, corporations are utilizing web technology to provide clients secure access to their data. Client-server applications are starting to become more and more of a commodity than a viable application technology because of the use of websites from XYZ's perspective. "90% of the companies that are using aging systems could be forced off them within the next five years. If they don't evolve those systems, they will disappear" (Schwartz, 2005).

**Technologies used: Different Corporations**

The problem with trying to secure the network is that the virus makers and hackers in the world do not care about anything except for trying to maliciously interfere with the internet and its users. Take for instance the issues that New Orleans is going through right now after Hurricane Katrina. This was a natural disaster and all resources should be put to use to try to get them back on the map. No way, not from a hacker's standpoint. Information security staffers at the American Red Cross, which was hit by the Zotob worm, are working overtime to try to protect the organization's networks against attacks amid surges in usage of the networks following Hurricane Katrina (Vijayan, 2005b). This is proof that it doesn't matter what the occasion or disaster, malicious people are out there.

Corporations need to be better prepared for these types of occurrences to happen. They need to be able to utilize new technologies to help their cause before another attack damages their infrastructure again. "The Red Cross is implementing new technologies such as intrusion-detection and prevention systems – some of them donated by vendors – to bolster network security," said Ron Baklarz Washingon based CIO (Vijayan, 2005b).

The more people develop and tighten their security policies and look at these potential threats, the more secure their networks are going to be.

Corporations may have good policies and procedures in place. Are many corporations looking at the possible technologies that exist out there before a Zotob comes up to bite them? Chief Information Security Officers (CSCOs) at federal agencies are taking a stance on trying to improve their security. After many years of struggling to implement a basic security framework, government agencies are turning to more complex issues (Carlson, 2005). Another thought is that you have to do more than just deploy firewalls at specified locations and have them magically fix any problem that occurs. More has to be done with the technology than just set it in place. Administration is a key to being able to support the firewall. "Before, people thought you could just put a firewall at the edge of the network. [Now] you need intrusion detection mechanisms on each machine," said Roy Stephen, Cyber-Security Director at Intelligent Decisions, in Ashburn, VA (Carlson, 2005). Anything that can be done to help prevent malicious traffic from getting into the corporate network is a step toward success.

Maybe there is a way to redo the way the internet is built today in hopes that all hackers and viruses would not know how to spread throughout the internet. Internet Protocol version 6 (IPv6) is something that has been talked about for many years now and the U.S. Department of Defense has been pushing for the use of it. Many corporations do not want to go down that path because of the complexity. The National Science Foundation (NSF) has proposed a plan for creating a next-generation internet with built in security and functionality that connects all kinds of devices (Gross, 2005). There is a project that is in the works from the NSF and it is called Global Environment for Networking Investigations (GENI). GENI would basically be the lead project that would look at new internet technologies like the introduction of IPv6. NSF is looking at getting the project funded. The initiative was recently announced in August at a conference of a special interest group on data communications in Philadelphia. Technologies are new every day. There are some great minds in this world and to take advantage of this would not be a bad use of resources. The goals of the GENI initiative include new core internet functionality, such as naming, addressing and identity architectures; enhanced security and high availability; and new internet services and applications (Gross, 2005).

The good part about viruses or attacks that cripple corporations is that sometimes the people get caught and then have to pay for what they did to the victims. Remember the Zotob worm that the researcher introduced earlier in this section. The creators of this worm were found and prosecuted. The problem will continue to exist even if the internet was to be redesigned. There will always be the kind of people that try to create malicious traffic on the internet. The Zotob criminals were found, but there are thousands more people in the world just trying to find new ways to create havoc on the internet. The goal is to put the necessary policies in place first and then get the correct technologies in place on the corporation's network. This will help protect the network from hackers. Be proactive when at all possible. To achieve its goal of more proactive security, General Motors launched a sweeping overhaul of its processes, including the manner in which it authenticates users and systems, enforces security polices, controls access to network services, patches holes, spots intruders and responds to incidents (Vijayan, 2005a). LAN security is playing a serious game of catch-up relative to the innovation that has taken place in the WAN. While the perimeter of enterprise networks has borne witness to the advent of firewalls, Intrusion Prevention System (IPS), and VPN technologies, viable LAN security technologies are only now being rolled out (Using Identity-Based Networking, 2005).

Take the University of Cornell for example in trying to help secure their network. They are utilizing some of this new Scan & Block technology to help with their network security. Stephen Schuster from Cornell University (Roberts, 2005) defines it as follows:

> Students may be asked to update their operating system patches or even install anti-virus and anti-spyware software before being allowed to access the campus network. Asset databases are used to track down and fix compromised systems. IT administrators work with the heads of each department in the university to determine what their computing needs are and then implement access–control lists on edge routers for those departments that filter out any traffic that isn't needed by department staff. Cornell is using new technology to help secure their network and yet still provide their law governed openness to any information on the internet, regardless of the type of data. (p 12)

**Remote Office Security**

This then begs the question, why would remote offices have to be treated differently than the users on the LAN? From a support perspective in talking to the management of the remote offices area, their biggest concern was the quality of support that XYZ provides to their remote offices. These offices are their own business entities, but still rely on our partnership. In order for XYZ's remote offices to succeed, XYZ has to provide quality service to them, whatever technology model is in place. With Scan &

Block technology out there, the answer to the question to how to secure the remote offices could be answered for XYZ. Leave them connected like they are today and keep the same level of service that is present today and utilize other technologies to help better protect the corporate infrastructure. Management for the remote offices, from a support standpoint, maintains that XYZ must stay competitive by providing their offices excellent service. Maintaining a strong partnership that has been built over the years, and adding value to them by maintaining their virus patches, spyware, and operating system patch management is a priority. The stability of the end device itself is a security concern, since unwanted plug-ins, spyware, malware and other software the user might knowingly or unknowingly load can create unnecessary help desk headaches – and open new holes through which corporate data can pass (Mitchell, 2005). XYZ has a commitment to these offices to provide them with the best service possible allowing them to succeed in business.

Today there are different connection methods other than IPSec VPNs. IPSec has been a reliable way of communicating with the remote offices, yet there could be other alternatives out there to take advantage of. Something that XYZ has been looking into is the possibility of using the Secure Socket Layer (SSL) VPN technology. The researcher takes SSL into consideration as an alternative way of accessing applications such as e-mail and other client server based applications. The researcher has doubts that the SSL VPN will totally replace the IPSec VPN due to the complication of how remote offices and the whole XYZ WAN infrastructure need to be able to communicate with one another. The partnership of XYZ Corporation with their remote offices has to remain intact. The firewall/VPN switch out at each remote office is managed and maintained by

XYZ support staff. If SSL VPN would be used, IPSec VPN would still have to exist because of the XYZ's need to administer the WAN piece of the SLA. Application access is one thing, but to push out support of a firewall/VPN to novice users is not realistic. Support processes and access to these remote offices must be maintained, as well as the WAN architecture, because of the way the WAN is built. Some of the remote offices have sub-offices that need connection back to the main remote office. XYZ is partially responsible for this communication path. The researcher says partially because XYZ is not responsible for their bandwidth out there. XYZ is just responsible for the network equipment that makes up the WAN portion of the site. The printers, workstations, and servers are all supported by the remote office staff. XYZ is not staffed to take on all of this support and it is not part of the SLA out to the main offices. The fact remains from XYZ management that security is a must, and changes in the way security is enforced need to happen. Nobody likes change in today's society. End users must be aware of these changes and not question that they are needed. It may slow their work day down a little, but in the long run it is what is best for the organization. All of the tools and approaches can be helpful, but the trick is balancing your organization's risk tolerance against the desire for end-user flexibility. While a total lockdown may not be feasible in your company, tighter controls are the way of the future. Ultimately, most users will have to accept that. If they don't, well, it's a new era. They'll just have to suck it up and deal (Mitchell, 2005).

Wireless LAN technology is a very hot topic today in the industry. XYZ Corporation is no different than any other organization. XYZ corporate does not have a need yet for the wireless access points. The remote offices for XYZ have a need to be able to access their servers, printers, and scanners from anywhere in their LAN. What is the best approach for this from a security perspective? There are many different vendors out there with many different types of boxes to accomplish what the remote offices are looking for. The biggest issue faced is not so much what box to get, but how to secure the box when they do get it. Even the people who designed WEP (Wired Equivalency Privacy, the first-generation wireless security protocol), admit that it is a weak protocol that is easily outwitted. The next generation, WPA (Wi-Fi Protected Access), is a much better solution but it is not necessarily available for your old Wi-Fi equipment (Steinhart, 2005). XYZ's remote offices will not be affected by old Wi-Fi equipment because a wireless solution has not yet been identified.

From a business perspective, it gives the end-users an advantage when it comes to being able to access their information from anywhere. If they have a client in their office and want to meet in a private room, the LAN user can have the added benefit of utilizing the wireless access point to fulfill the client's request. Wireless technology is becoming a hot topic more and more in every aspect of business. XYZ wants to provide wireless LAN access to their offices, but the lack of knowledge out at the remote office is a huge hurdle. Whatever solution is chosen, it cannot be managed by the remote site because the lack of expertise exists at these locations. Being able to monitor networking devices, especially a wireless access point, is a huge responsibility due to the security concerns. Using WEP or WPA and not being able to see how the boxes are configured is the wrong direction to go. Stories about hackers and identity thieves abound, yet the vast majorities of deployed networks remains completely unsecured and open (Ellison, 2005).

## Securing Networks: Best Practices

It is hard to say what the best practices for any corporation are because every corporation is different. A retail store has much more to protect due to their online transactions than a cabinet maker does. To have an effective security plan, anything that can be thought of for security concerns should be addressed. Just putting a firewall out at a site is not good enough, unless you have a strict rule base to deny traffic to unneeded locations or information. If a hacker gets on your network, you want to be able to protect your network at all costs. Someone gets on the network, do not allow them to get past without another way to defend against their attack, ie. two factor authentication and passwords. There is no such thing as an overprotected network.

A good security policy is only as good as the people that put it in place. Corporations that have set a policy and defined security rules and regulations are doing the correct thing. "You cannot just sit back any longer and wait for your LAN to go down or for your employees to complain," says Ed Amoroso, CISO at AT&T Corp (Vijayan, 2005a). "You need to be looking at things before they become a problem" (Vijayan, 2005a).

# Chapter III: Methodology

## Introduction

What can be done to better protect our XYZ's corporate network from internet attacks? What does XYZ Corporation have to do to secure their corporate network? In trying to accomplish the task of researching this issue, the researcher found that using the knowledge of XYZ's management and using some of the researcher's own experience are the tools used for this study. The purpose of this project is to make sure that XYZ Corporation is providing the best security possible for their network.

## Company Information

Without divulging any information regarding XYZ Corporation, the researcher will give some background on XYZ. XYZ Corporation is a Financial Services/Insurance company that provides quality service to its customers and clients without compromising security. Customer data does reside on XYZ's network and many of the customers trust XYZ to store their financial information on their network. XYZ Corporation has been around for a long time and has built a reputation for being trustworthy and very solid when it comes to new technology. XYZ has to remain solid in securing customer/client data to keep the company loyal to its roots. Security is an integral piece of any financial institution in today's world.

## Topic Selection & Description

Since July 1995, the researcher has worked in XYZ Corporation's network areas. It was the researcher's first job out of college and the researcher is very versed in what is happening on the network. The main focus of the researcher's job is to maintain the remote office's network and make sure connectivity back to their applications is up and functioning. This topic was selected for research because of the researcher's extensive involvement in remote office communications and networking in general.

## How to Secure the Corporate Network

Many corporations must first look at building their networks from the ground up with two things in mind, speed and security. A good network is a network that is fast in response time and does not allow hackers to get in and hurt the performance of the network or compromise any data. XYZ has built the network with speed and security as its number one priorities. XYZ has kept the network infrastructure pieces down to one vendor which is a definite support advantage. All network switches and routers are maintained by one vendor. This is an advantage in the researchers mind. The ability to go to one vendor for support eliminates any finger pointing in the future. The network infrastructure was built for speed and redundancy. The network will remain up at all times even if one building or one segment of the network goes down.

XYZ makes the second piece of the network, security a very integral part. The network can run without this piece of equipment, but remember what the internet brings us, potential for hackers getting into the network and compromising data and hurting business. Security is an important part of the network. To do business today, firewalls are the piece of the network puzzle that must be in place. The firewall acts as a stopping point for hackers that do not have allowed access into the network. If you try to get into XYZ's network and the firewall does not allow that traffic, that traffic will be dropped. For many years, the Data Security Team was responsible for all facets of the firewalls. With firewalls being a main piece of the network infrastructure, it was determined that security should remain with Data Security and the network control of the firewall remains in the Network Engineer's hands. XYZ's management gave the network team power to administer the firewalls and have Data Security administer the rules on the firewalls. It makes sense from a security perspective to allow each area do what they know best.

Hackers are everywhere in this world. They try to get into companies networks and gain information or just try to disrupt things because they have nothing else to do. XYZ should look into ways of making sure hackers cannot get into the network and compromise data or disrupt network performance. Intrusion detection and prevention is imperative for this organization. Before intrusion detection and prevention came about, there was nothing good enough to help prevent or even monitor the bad traffic from entering into the infrastructure.

> Today's threat environment is about threats that emerge from inside the network, either through penetration of the perimeter or, more commonly, by introduction from a source that directly accesses the inside of the network. The first development to address this area was ***intrusion-detection*** systems (IDS), an array of servers and sensors deployed across a network to watch for and report on network traffic. The natural evolutionary path of the IDS was to improve accuracy by reducing false positives and to develop a way to respond to alert information in a timely manner. Thus, the ***intrusion-prevention*** system (IPS) was born, which incorporated the traffic-monitoring functionality of its predecessor, while adding application-layer inspection and proactive attack protection that was lacking in legacy firewalls. (Bring on the Security Gateway, 2005)

IDS technology has been inline for many years at XYZ, but nothing is set in place to get the IPS inline. In order to better protect XYZ's network, IPS has to become installed on the network. XYZ's management has to make this a priority in the near future.

Viruses are abundant on the internet. Every time you turn around another virus is out there trying to infect organizations. The key is to make sure virus scanning software is current on all workstations and servers on the network. This is a factor in trying to secure XYZ's network. The ability to have a centrally managed virus scanning system has to be in place. This has been done and is getting better everyday. The engineers working on the product are dedicated to making sure that all devices which need virus scanning on them are actually running them.

XYZ is looking into a concept that the researcher described earlier as Scan & Block technology. This is a strategic piece of securing the network by utilizing new and better technology. It has not been set for a 2006 project because the network infrastructure is not built yet to support the emergence of this new technology. XYZ has to replace a lot of network switches in the wiring closets of each user floor to accomplish this. It will need to be budgeted for due to the expense.

### How to Secure the Remote Offices

XYZ Corporation has many remote offices that are just an extension of the corporate network. These offices connect back to the corporate network via a VPN tunnel and then utilize the corporate IDS and firewalls for their protection. The workstations and servers are all managed by XYZ. The other set of remote offices that are connected back to the corporate network are different from a support and business perspective. These offices are not managed by XYZ. All workstations and server are purchased and maintained by these remote offices. In saying this, remote offices that are not controlled by XYZ are where the security needs to be more extensive. The researcher for simplicity purposes will call these specific remote offices "agent networks." XYZ looked at the risk of having these agent networks connect back to the corporate network and realized the risk was high. The way business runs for these agent networks is that they need access back to the corporate network for e-mail and various other applications. VPN is being used on all remote offices, but something needed to be done to limit what the agent networks could access back at corporate. Firewalls accomplish this goal. Having firewalls out there gives XYZ the ability to limit what the agent networks have access to back at corporate. The other consideration was to still be able to maintain the VPN infrastructure that was built for all remote offices. Many vendors that were researched had to be a firewall/vpn appliance. A vendor was chosen and the solution is being implemented. The same rules apply to how the firewalls are managed. The network infrastructure is supported by the network team and data security administers the firewall rules.

The Scan & Block technology described earlier should be looked at for these agent networks as well. If XYZ can stop the malicious traffic from even leaving the remote network, this would cause the network performance on the whole to run more efficiently. This technology will not be deployed to the remote offices for at least the next year or so. This will be a management decision based on where XYZ stands after the firewall/vpn appliances are deployed.

Virus management is very difficult for these agent networks. Since XYZ does not have full control, it is a challenge to administer the virus software on these devices. XYZ must make sure that all virus software is up-to-date with virus monitoring technology. Along with virus management, operating system security patches need to be addressed. The management team for the agent networks is beginning a project that will be able to deliver security patches on a timely basis. They are going to utilize a technology that will be managed by XYZ and each workstation/server will be able to update their operating systems behind the scenes without prior knowledge and with minimal interruption.

## Chapter IV: Results

The purpose of this chapter is to give results on the implementation of security for XYZ Corporation. Security is something that does not remain stagnant. There are viruses, worms, and malicious traffic affecting corporations everyday. The important result that needs to be known here is that XYZ is doing the best they can with the technology that is available right now. New technologies are being built even as the researcher is writing this paper. The key is to make sure that the corporation is doing the best they can to make sure that the security is in place so hackers cannot compromise data. By putting the necessary technologies in place for security and network performance, client data should be well protected.

Corporations that do not look to the future and look to just maintain their security measures set at status quo will most likely suffer. XYZ is heading in the right direction. XYZ implementing firewall/vpn appliances on the agent networks is an important step to prevent bad traffic from getting back to the corporate network. Website access has to be there because clients and customers are relying on the websites to be present and accessible. Scan & Block technology is going to happen at XYZ, it is just a matter of time before this becomes a reality. Budget concerns and other projects are the two main factors in the delay of this product evaluation. Other measures need to be put in place before Scan & Block can be a realistic option for XYZ. Virus and patch management are being pursued as business crucial projects. These workstations/laptops and servers are going to be getting the attention that is required. They will not continue to be an issue when it comes to spreading viruses or worms throughout the network due to their lack of virus patches or operating system security patches. The goal of keeping the network running at 100% uptime is something that most corporations strive for but never accomplish. The more security that is put into the network, the better XYZ will do from the business standpoint. XYZ puts money into technology and will continue to do so. XYZ Corporation has made promises to their customers and will never compromise those values. Network availability and security are key words that this researcher has ingrained repetitively. XYZ is doing what needs to be done to make sure their clients and customers are able to do business without all the hurdles.

## Chapter V: Conclusions & Recommendations

The researcher has observed that projects do not move quickly at XYZ Corporation. They are slow and very deliberately thought out. XYZ has dedicated Project Managers (PMs) that make sure no stone is left unturned. The PM's job pertains to the successful implementation of the product or service in question. Without a person leading a project, typically projects get out of hand and even fail or take years to complete. XYZ's PMs focus on managing the projects and making sure all the resources and requirements are being fulfilled. XYZ's management has made it abundantly clear to all areas that project management is vital to the success of doing business. This is how XYZ has thrived throughout the years. In saying this, the security thoughts and security technologies in this paper will be implemented someday. Even ideas and technology that have not been thought of yet will be used in the future. No one can predict when a person will decide to create a malicious attack on a corporation's network. If XYZ continues to implement the best researched network security, they will be ahead in the long run. Control remote offices, stop the viruses, keep unwanted people off of the network, and do what is right when it comes to security and in the long run XYZ will remain profitable. Corporation's network security makes a real difference with what the business world likes to call, "the bottom line."

XYZ has to always look into new ways of stopping the attacks on their network. IPS is a perfect example and will prevent any attacks from getting into the network rather than just detecting attacks. To prevent an attack is better than to react to the detected issue. If we know that the bad traffic exists, there needs to be a way to proactively eliminate that traffic from interfering with business processes. XYZ could even look into the possibility of getting a prevention system out to the remote office locations. These offices always seem to be the biggest culprits of useless traffic. Be proactive and not reactive is what XYZ needs to do for the IPS infrastructure. Utilize the technology and be wise on how it is implemented.

All of the technology and all of the security that is put in place for XYZ Corporation have been good business decisions. Two things have to happen, the business areas must be able to do their business and XYZ must be able to maintain the level of service they have always provided. Service to their clients is what XYZ has made their livelihood on and this cannot be compromised when dealing with access to the network. There was talk about totally disconnecting the remote offices and only providing them with web site access to information. As stated previously, service is a very important part of doing business. The relationship with the remote offices has to be solid. To totally disconnect them is a good strategy, but the way it is presented to them has to be done strategically. These remote offices are reliant on XYZ to provide a service to them and that service is what attracts them to stay with XYZ. The remote office technology philosophy can follow the "total disconnect" model, but portray it to the remote office management as an attractive technological advance. Making sure that XYZ will still be there to support them and provide the same service that has been there for years, is why success of securing remote offices is so important. Technology will always be there and anything can be made possible with the appropriate budget available. Service is what sells in the industry that XYZ is a part of. XYZ provides a secure, safe, accessible network to end users. Security has been considered one the most important concerns surrounding a network. XYZ is doing what is needed to be done. Focus on what is most important to keep the business processes functioning to the best of their ability.

XYZ has been around for a long time and has seen many changes in the way business is done. In order to stay competitive, XYZ must remain true to their core values and invest in technology. If a certain technology is needed to help out a business area, go out and get that new technology. It does not mean rush out and get the first product available. XYZ has to keep the processes that exist today in the network world and make sure that security is always looked at as a potential problem. Research new technologies and make sure they are on the right track themselves from a security perspective. Change is inevitable, people change, technology changes, and viruses are created everyday. XYZ has to be ready for whatever is thrown at their network. The researcher's stance is that XYZ needs to keep on the path they are on right now. Security, security, security is all that we hear about in today's internet world and XYZ is on the right path towards "Securing the Corporate Network." Be proactive and not reactive.

## References

Bring on the Security Gateway. Retrieved November 22, 2005, from http://www.comnews.com/stories/articles/0905/0905bring_on_security.htm

Carlson, Caron (2005). Information Security Matures. *eWeek,* 22(35), 30-31.

Ellison, Craig (2005). New Utilities Make Wireless Setup, Security Easy. *PC Magazine,* 24(11), 36-37.

Erlanger, Leon (2005). Secure Architectures. *InfoWorld*, 27(11), 42-44

Gross, Grant (2005). NSF Proposes Ambitious Internet Project. *Computerworld*, 39(36), 15-15.

Mitchell, Robert L. (2005). Endpoint Security: Let the Users Grumble. *Computerworld.* 39(43), 38-38.

Network Access Management Solution for Effective Scan & Block Security. Retrieved October 18, 2005, from www.qualys.com/docs/qualys-vernier-solution.pdf.

Roberts, Paul F. (2005). Lockdown on campuses. eWeek, 22(34), 12-12.

Schultz, Keith (2005). Protection From the Unknown. *InfoWorld*, 27(25), 18-19.

Schwartz, Ephraim (2005). The Legacy Continues. *InfoWorld*, 27(31), 10-10.

Steinhart, Michael J. (2005). Network & Wireless Security (cover story). *PC Magazine,* 24(21), 94-95.

Using Identity-Based Networking for Secure LAN Control. Retrieved November 7, 2005, from www.securitypipeline.com/showArticle.jhtml?articleID=173403086

Vijayan, Jaikumar (2005a). A Good Offense. *Computerworld.* 39(12), 36-38.

Vijayan, Jaikumar (2005b). Red Cross Works to Better Protect Its Networks From Attacks, Scams. *Computerworld,* 39(37), 7-7.