Global Information Assurance Certification Paper

The Evolution of Network Security at Company X

Mike Engels
GSEC Practical 1.4b

Abstract

In today's world of targeted attacks and ever evolving blended threats, it is not sufficient to stand up a firewall, deploy an Antivirus program and believe that you are protected from computer infiltration. Companies must establish multiple layers of defense and dedicate valuable company resources to protect their environment.

This report identifies how one company is addressing security but can be used as a guide for any Windows 2000 Systems Administrator that needs to incorporate network security into their computer environment. It discusses Company X prior to any security implementation and follows a chronological timeline.

There are many aspects of network security discussed. Using a layered approach, this document discusses Company X's Network Use Policy and implementation of an Antivirus Solution, Operating System and Software Standardization, as well as Company X's existing backup strategy. It also includes an overview of the Windows 2000 Group Policy, Perimeter Defense, and a Patching Strategy. Finally it addresses the importance of in house security expertise. The Appendices of this report contain sample configuration for some of those topics discussed.

The Before Picture

Company X is a small research and development company located in British Columbia. Company X employs 50 people including scientists and office staff. Their IT department consists of two System Administrators (both generalist), and a Database Administrator. Neither of the two Systems Administrators had any formal security training.

The company network was comprised of four Windows 2000 servers and 75 workstations. The workstations featured Windows NT4 Workstation, Windows 2000 Professional, Windows 95 and Windows 98 as the operating systems. The servers consisted of two Domain Controllers, one database server, and one Microsoft Exchange 2000 e-mail server. This e-mail server serviced the company for their internal e-mail while a service provider handled external e-mail. One of the Domain controllers served as a File Server, while the other served as the DNS, WINS, and DHCP server. The server's power was regulated and protected by a large UPS. None of the servers were configured for automatic shutdown in the event of a power failure. The servers and workstations were

patched to various levels and there was no procedure in place to regulate operating system patches.

Similar to the operating systems, there were many versions of the same software title found on the company network, including Microsoft Office, and Internet Explorer. Once again there was no strategy in place to maintain patches for these programs.

Company X had no Antivirus plan in place. Norton Antivirus Corporate Edition (NAVCE) 7.0 could be found on some workstations but none of the servers. Further complicating the Antivirus situation was the fact that the original Antivirus server was a workstation and that workstation no longer existed. This meant that the existing Antivirus clients were orphaned, had inconsistent settings and did not have a consistent version of virus definitions.

The network infrastructure consisted of an Ethernet network. The network was primarily switched however a few hubs were still in production use. The workstations were served IP addresses by a DHCP server. Included in the DHCP lease were the addresses of the DNS server, WINS server, and gateway. All of the company computers were on a single 192.168.xxx.xxx non-routable network. Internet connectivity was provided via an ISDN connection. There was no firewall or IDS in use and Company X did not have a VPN.

Company X had no network documentation. There was no corporate computing policy and there was no disaster recovery plan.

The Plan

The following sections outline the changes that Company X implemented to their network security beginning in February 2002.

Policy

One of the most fundamental aspects of any security plan is a computer usage policy. The purpose of such a policy is to define acceptable use of IT assets within a company. As well, the policy defines what is expected of the computer users and finally the policy defines what are acceptable standards within a company.

Company X needed to develop a computer policy as the foundation of their security plan, and so they did. It was written to cover such topics as password management, acceptable email and Internet usage, software installation and licensing, Antivirus protection and general usage guidelines. As well, the policy included a list of approved software titles and a list of prohibited software.

In addition to the computer policy, Company X introduced an IT staff policy. This was deemed necessary because of the elevated privileges that the IT staff needed to be entrusted with. The IT staff policy covered such topics as password management, access permissions, software management, perimeter defense management, backup strategy, policy training and enforcement and Antivirus protection. Due to confidentiality reasons the full written policies are not available.

Antivirus

As was mentioned in the overview of the network there were sporadic installations of Norton Antivirus Corporate Edition (NAVCE) 7.0 throughout the company. Further complicating the Antivirus Deployment was the fact that there had been at least two prior Antivirus servers, and neither of those existed any longer. As a result all of the Antivirus clients in Company X were orphaned.

After researching various corporate Antivirus solutions [1] including solutions from Mcafee, Trend Micro and Sophos, it was decided to fully deploy Symantec's Norton Antivirus Corporate Edition 7.5 for File Servers and Workstations. In addition Norton Antivirus for Microsoft Exchange 2.5 was deployed to protect the corporate e-mail system.

The systems administration staff decided to do a complete uninstallation of existing Antivirus clients followed by proper deployment of NAVCE 7.5. The first step in the Antivirus solution was to install a corporate Antivirus Server. Company X's existing server infrastructure did not include an application server and due to budgetary constraints one could not be purchased. These factors led to a Windows 2000 Professional workstation being configured as the Antivirus Server. The new Antivirus Server was now ready to host antivirus clients. (See Appendix 1 for a sample configuration outline)

In order to ensure a good installation of the Antivirus client an administrator had to visit each workstation that had an orphaned Antivirus installation and perform a manual un-installation. Next, each workstation was configured with the new Antivirus client via the NT client install utility included with NAVCE 7.5. Furthermore the entire client configuration was set at the Antivirus Server and passed to the clients through the built-in configuration utility. The four servers were the highest priority to get protected. This required after hours work since the servers were in production use during regular business hours. In order to properly deploy NAVCE 7.5 to the MS Exchange server a second server group had to be created [2]. This special "Exchange" configuration set the correct file exclusions [3] so that NAVCE 7.5 would not scan the Exchange database and other unscannable Exchange files (see Appendix 2 for a sample NAVCE 7.5 configuration for MS Exchange).

In order to deploy a comprehensive Antivirus solution Company X's Microsoft Exchange e-mail system needed to have Antivirus protection. Installing Norton Antivirus for Microsoft Exchange (NAVFMSE) 2.5 achieved this additional coverage. The Antivirus software for Exchange was configured to scan all incoming and outgoing messages, including attachments, for known viruses based on virus definition files and heuristic [4] matching.

Virus definitions for NAVCE 7.5 were set to update on the primary server of the main server group only. This meant there only needed to be one connection to the Internet. All of the client computers and Primary server of the "Exchange" server group updated their virus definitions via the Primary server of the main server group through the Virus Definition manager. NAVFMSE 2.5 was configured with the same update schedule as for the NAVCE 7.5. The Virus definitions for NAVFMSE 2.5 had to be monitored closely so as to prevent any virus definition version conflicts. In the event of a virus being detected it was immediately quarantined on the workstation (or server) it was found on. The quarantined file was then forwarded to the Quarantine server to be reviewed and dealt with by a Systems Administrator.

Due to the sensitive nature of the research lab environment no Antivirus software could be installed on those workstations. This caused great concern but additional steps to secure this environment were planned for and will be discussed later in this paper.

Once all of the clients were updated to NAVCE 7.5 the Antivirus deployment was complete. The only task that remained was to monitor the virus definitions to ensure that they were being updated correctly and to manage any virus occurrences.

Operating System and Software Standardization

One of the most labor intensive challenges that faced Company X in their security initiative was the standardizing of the Operating System (OS) and software installed on the workstations. Windows 2000 Professional was chosen to be the standard OS. This OS was already deployed to some of the workstations so compatibility with software packages used at Company X could be ensured. The OS was deployed along with Service Pack 2. Since no hotfixes had been tested it was decided not to deploy any, and later implement a patching strategy.

Along with the varied OSes there were various versions of MS Office, Internet Explorer, Netscape Navigator, Adobe Acrobat Reader, and Windows Media Player. In addition to these titles, there were many other programs including file sharing and instant messaging programs found throughout the network. In order to simplify patching of the software titles it was decided to deploy MS Office 2000 SR2, Internet Explorer 5.5 SP2, Adobe Acrobat Reader 5.0.5 and Windows

Media Player 7.1 as standard software for all workstations. In addition all software that was not on the list of approved software found in the IT Policy was immediately removed.

Fortunately the scientific software versions were standardized. Upgrades to these programs were generally for improved functionality; they were deployed immediately following their release.

The strategy to upgrade the workstations in Company X required the greatest labor investment. A checklist was prepared to outline the steps required for upgrading a workstation from each of Windows 95, Windows 98 and Windows NT Workstation 4 to Windows 2000 Professional. An administrator visited each workstation and performed a manual upgrade following the steps of the appropriate checklist. The diverse environment that existed was deemed to pose too many potential problems to attempt any automation. Furthermore there were only 75 workstations to upgrade.

The one exemption from the OS and Software standardization was the lab environment. Due to the change management program and the regulatory validation requirements, the lab computers were left unchanged. These workstations were already standardized to Windows NT4 Workstation Service Pack 6A and only had a special Analytical Chemistry software package installed on them. A plan to upgrade them to Windows 2000 was to be developed.

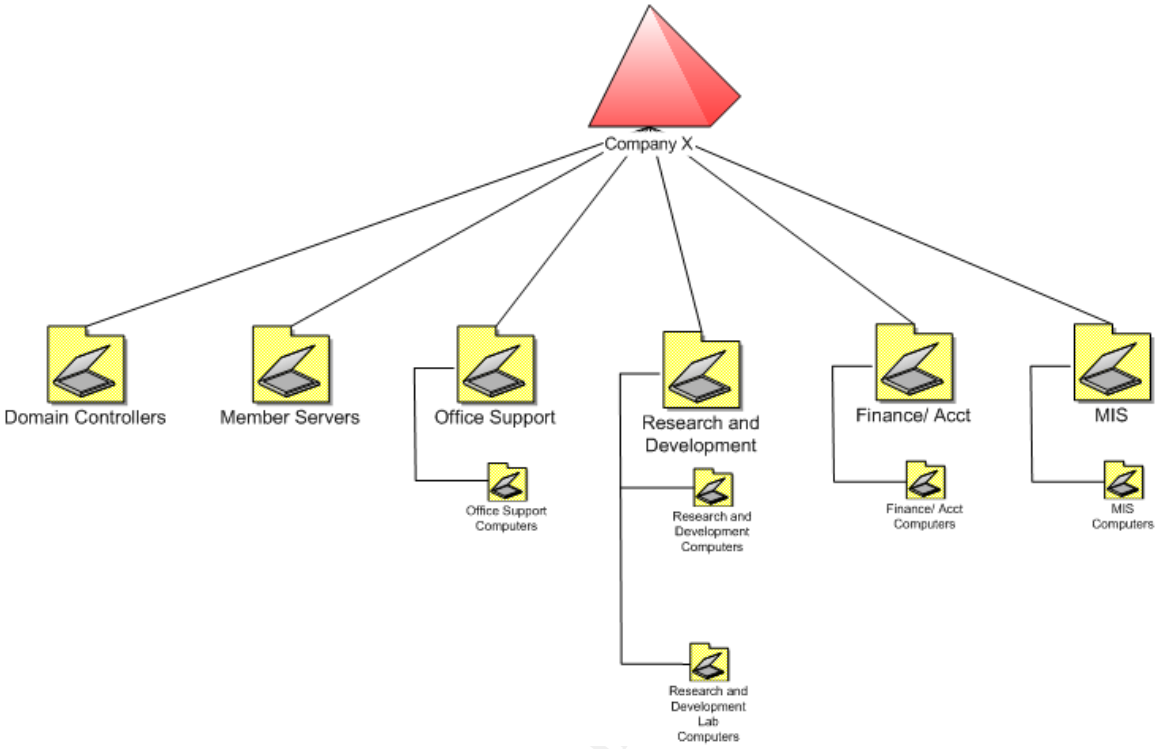
Backup Strategy

Company X had a good backup strategy in place for their servers. They used Retrospect's Backup Exec 8.0. The backup sequence included a full backup each Tuesday and Thursday with incremental backups on Friday to Monday, and Wednesday. Company X also employed Retrospect's Backup Exchange Server Agent for MS Exchange. The Exchange backup sequence included full backups each Tuesday and Thursday with incremental backups on Friday to Monday, and Wednesday. All full backups were sent to a secured off-site storage facility the morning following their completion, while the incremental backups were stored in a fire-proof safe on-site.

Windows 2000 Organization Unit and Group Policy Configuration

The existing Organization Unit (OU) structure included the default OU containers but no additional containers. In addition there were no Group Policy Objects (GPO) deployed.

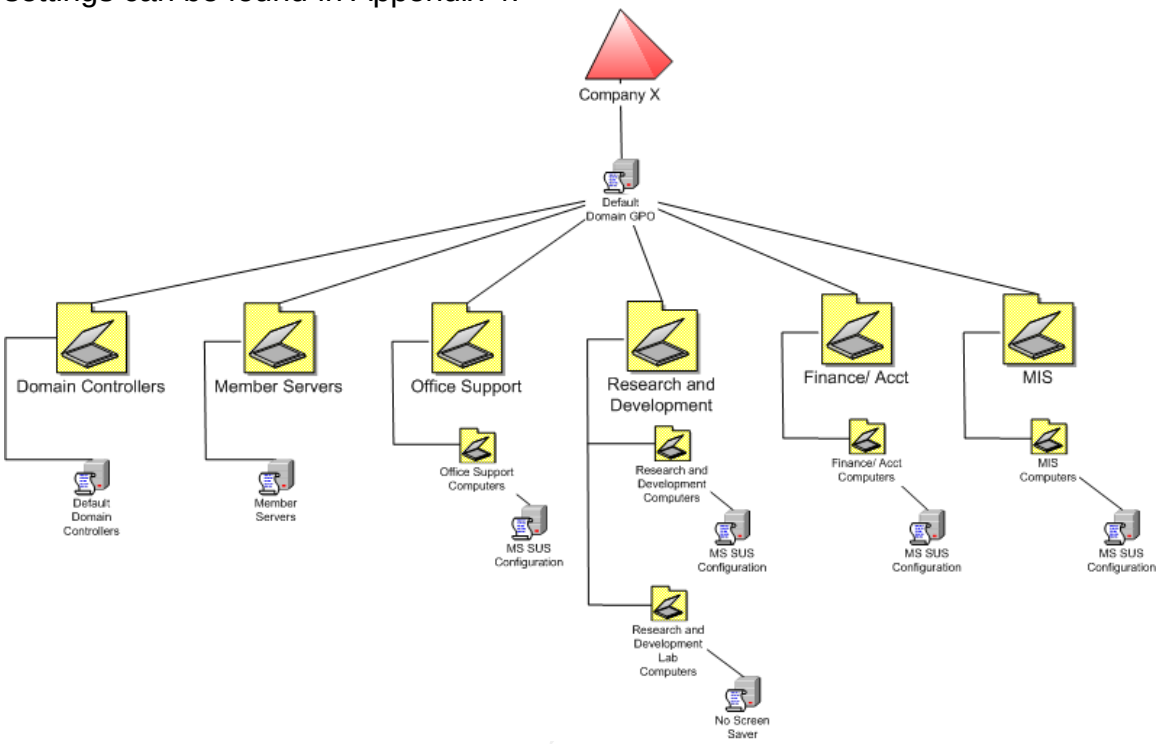
In order to effectively deploy GPOs there needed to be a well designed OU structure [7]. This structure needed to account for the various corporate departments, Domain Controllers, Member Servers, lab computers. The following diagram shows the OU Structure that was implemented at Company X.



The Domain Controllers and Members servers OUs were created to isolate the Domain Controllers and Member Servers respectively. This isolation allowed for a more stringent GPO implementation for the servers. The other OUs were created based on functional departments within the company. The computers OUs were established to isolate the computers from the users making for a cleaner OU structure. As well, the majority of the GPOs that were to be implemented were computer GPOs and this structure helped to maintain more granular control over the GPO deployment. Finally a Research and Development Lab OU was created to house the Research and Development Lab computer accounts. This special OU was required to prevent any unwanted configuration changes to the Research and Development Lab computers as a result of a GPO modification or implementation (the exception being the Default Domain GPO)

Following the modifications to the OU structure, Company X was ready to proceed with the deployment of several GPOs to enhance security. The need for a Default Domain GPO that would encompass security settings company wide, a Default Domain Controllers GPO that would tighten security on Domain Controllers, and a Member Servers GPO that would tighten security on Members Servers was identified. In addition, an MS SUS GPO to configure the Microsoft SUS service and finally a No Screen Savers GPO to disable screen savers in the lab environment were implemented. The Center for Internet Security (CIS) [8], National Security Agency (NSA) [9], and Microsoft [10] had templates and documentation to guide the administrators in configuring the different GPOs.

The following illustration shows the OU structure as well as the GPOs and to which OU the GPOs are deployed. A matrix of GPOs and their applicable settings can be found in Appendix 4.



Perimeter Defense

At the beginning of Company X's security initiative, they were also undertaking an Internet connection upgrade. Due to the upgrade from ISDN to corporate ADSL, it seemed irrelevant to address the security of the ISDN connection. Company X chose to focus on securing the ADSL connection.

Company X chose to install a D-Link Express Ethernetwork DI-604 Ethernet broadband router/firewall. This router/firewall provided high-speed connectivity to the entire company. As well, the appliance allowed for customizable firewall rules, content filtering, NAT, virtual server support and DMZ host support.

The entire configuration of the firewall was done through its web interface using the D-Link Express Ethernetwork DI-604 manual [11]. The first step in the configuration was to change the administrator password, following that, the BIOS of the firewall was flashed to the current version. Next, a host name was given to the firewall and the static IP information (including DNS) that was given by Company X's ISP was entered. This concluded the WAN setup.

The LAN setup consisted of assigning the firewall a static IP address and subnet mask. As well, the local domain name was inputted.

The final step of the initial configuration was to disable the DHCP server on the firewall. The existing DHCP server handled all dynamic addressing on Company X's network and needed to have its scope options updated to reflect the new gateway address. As well, the DNS server needed to be updated to reflect the routable DNS addresses provided by the new ISP.

Following this initial configuration a more advanced setup was undertaken which involved applying a filter to deny the lab computers access to the Internet. This blocking was required because of the extra sensitive nature of the lab computers and because the lab computers had no Antivirus software. The filter was configured to block the MAC addresses of the lab computers. Since the lab computers were the only group of computers that Company X felt needed special attention, no other rules were set. Furthermore since the lab computers were blocked by their MAC address no additional firewall rules were needed. However a configuration change was made to block the firewall from responding to PING requests. Selecting the "enable" radio button for the "discard ping from WAN side" line under the tools menu disabled this. After the firewall was configured to the level that Company X desired the configuration was saved to its local hard drive. This backup allowed for the original configuration to be restored if subsequent changes caused problems.

The final step in configuring the DI-604 firewall was setting up the logs. The firewall was configured to log system activity and attacks. A new daily activity for one of the network administrators was to save the logs. This entailed using the email function of the firewall and sending the logs to themselves. Having the logs saved in a separate location allowed for easy immediate log analysis, and, it provided the ability to do trend analysis on a monthly, quarterly, and annual basis.

Patching Strategy

Company X had no patching strategy. As part of the Software and Operating System standardization all workstations (except for the lab environment) were brought up to the Windows 2000 Professional SP2 level with no hot fixes. In June 2002 Microsoft released Software Update Services (SUS). A client-server application, SUS allowed for controlled, automatic deployment of Administrator approved patches from an internal server. The internal server was configured to contact a Microsoft Update Server and synchronize available patches for an Administrator to approve for deployment to the client workstations.

MS SUS deployment and configuration was achieved with the use of the provided Group Policy templates. The SUS server was installed on the E-mail server (it had to be installed on a server but could not be a Domain Controller). Following this installation a Windows Update template became available to be added to the Windows Components of Administrative Templates under Computer Configuration. These Windows Update templates allowed for the configuration of

how clients would download and install patches, from where they download these patches and the intranet statistics server which to report to. Sample installation and configuration information for MSSUS deployment can be found in Appendix 3. (The original Microsoft Software Update Services Deployment Guide is no longer available from Microsoft. A link is provided [5] to the Deployment Guide for SUS with SP1. SUS with SP1 includes the ability to deploy the SUS server to a Domain Controller as well as some additional templates for client GPO configuration that were not deployed at Company X and therefore go beyond the scope of this paper.)

In order to ensure full application compatibility with the hotfixes to be deployed, a test environment was needed. Due to resource constraints a separate test network was unattainable, and so it was decided to select a user from each department in the company to deploy the patches to, for a period of 6 weeks. These users would evaluate the impact of the patches on the applications they use. Each of the computers in the test group was imaged prior to a set of hotfixes being installed to ensure the ability to undo the effects of the patches.

The test environment was not ideal but was significantly better than having no period of testing at all. Since Microsoft is continually releasing patches it was decided that the patches would be monitored for their impact on Company X's network. If a patch were deemed to be critical it would be deployed to the test group immediately. All other patches that were determined to be applicable to Company X but not critical would be logged and deployed to the test group on a quarterly basis. After a 6-week evaluation period the patches would be deployed via SUS Company wide.

Further complicating the SUS deployment were the lab computers. This group of workstations was regulated by a change management system. The software that was running on these workstations was a very sensitive analytical chemistry software that would not maintain its validation if changes were made to the computer. To address this issue patches were deployed to the lab computers manually, semi-annually, just prior to their semi-annual validation. SUS was not deployed to the lab computers.

The patching strategy for Company X's servers followed a similar course to that of the lab computers. SUS was not deployed to the servers because there was no environment to test the patches in, and Company X could not tolerate downtime due to a bad patch. The servers were manually updated on a quarterly basis as part of regular server maintenance.

Security Training

Company X realized that in order to maintain an active security program a higher level of security expertise was going to be needed in house. Company X's network administrators researched and recommended appropriate training [6].

This training needed to address a broad range of security topics including policy, disaster recovery, windows specific issues, intrusion detection, Antivirus, incident handling and perimeter defense. Sans Security Essentials training was recommended because it best addressed all of Company X's training requirements. One of the administrators was chosen to attend and then appointed lead of Company X' network security program.

Looking Forward

During the initial steps taken toward securing their environment, Company X realized the need to account for network security as a process of their business. It was recognized that this process would require constant management. Analysis of logs, research of current threats and foresight to identify emerging threats were all requirements for maintaining a proactive security posture. Another key aspect of addressing security as a process is maintaining an evolving security plan.

Company X had several plans going forward. The first item on their list was to isolate the roles of their servers, which would allow for more stringent hardening of the servers. Also they planned to implement the recommendations for file system and registry security as outlined in the NSA Guide "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set". Another step to was the creation of virtual LANs (VLANs). The VLANs would allow Company X to isolate the sensitive lab environment, and have better control of network traffic on that segment. Company X planned to implement a Network Intrusion Detection System (NIDS). Due to budgetary concerns, they decided that SNORT would be the solution of choice. Even though SNORT is open source there is excellent documentation available at http://www.snort.org/docs/. Another topic on their list was to have an independent security audit. Although the audit would not directly improve the network security it would help them to identify areas that need attention. Furthermore the audit would help the network administrators prioritize their plans going forward.

Since the installation of NAVFMSE 2.5 Symantec release Symantec Antivirus Filtering for Microsoft Exchange. This new antivirus program added e-mail filtering functionality to the existing Antivirus scanning capabilities and was to be tested and deployed.

Company X was planning on developing a Disaster Recovery plan for their network infrastructure. The plan would allow the company to efficiently recover from a major interruption to business.

Conclusion

Company X identified security as a vital aspect of their business and therefore established a pro-active plan for network security. Their network security plan involved implementing a people plan as well as a technology plan.

The people plan incorporated a network policy as part of the company policies and procedures. The policy established acceptable and expected practices on the network. The inclusion of an IT staff policy highlighted the understanding that the MIS staff needed elevated privileges to be able to do their job. At the same time it also identified the level of conduct to be followed by the IT staff. Also, Company X made a substantial investment in the human capital of their IT department. By sending one of the administrators for SANS security training they invested in the development of that staff member while at the same time establishing in-house expertise.

The technology plan involved a wide array of implementations. First and foremost an Antivirus solution was deployed. With Norton Antivirus detecting an estimated 62000 viruses and countless new viruses being created daily, Antivirus software was essential to Company X's security solution. Company X took steps to simplify their environment. By standardizing the workstations Operating System and office productivity software, they greatly simplified the patching process. This patching process, automated by the Microsoft technology Software Update Services, installed administrator approved patches to the workstations.

Company X employed another Microsoft Technology. Group Policy Objects were created to harden the servers and workstations and to set security options that were enforced company wide. The addition of group policy objects enhanced the overall security environment by establishing a pre-configured baseline that would be applied to every computer in the company.

Perimeter defense came in the form of a D-Link DI-604 Ethernet Router/Firewall. This device protected Company X against malicious invasion. The firewall also allowed for customizable rules preventing specific computers from connecting to the Internet.

Finally Company X maintained a comprehensive backup system. Although backups are not directly related to securing a computer network, they are an essential aspect in recovering from a failure or a breach.

Company X's security implementations began the process of securing their corporate network. The inclusion of policy as well as technology was essential to a comprehensive security plan. Securing a network is a constantly evolving, challenging task that Company X will continue to address proactively .

Appendices

Appendix 1

Sample Norton Antivirus Corporate Edition Server (configuration)

Configuration Procedure:

1) Update the Virus Definitions
   a) Navigate to the Symantec website
   b) Download and install the intelligent updater virus definition that is for NAVCE7.5
2) Make the server a Primary Server
   a) Right click on the NAVCE server
   b) Select “Make server a Primary Server”
3) Configure the Virus Definition Manager
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Virus Definition Manager
   b) Select “Update the Primary Server of this Server Group Only”
      i) Click configure and schedule for automatic updates everyday at 8:00am
   c) Under How Clients Receive Updates
      i) Select “Update Virus Definitions from Parent Server”
         (1) Click the Settings button and set “check for updates” to 120 minutes
      ii) Select do not allow clients to manually launch Live Update
4) Create Scheduled Scans
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Schedule Scans
   b) Server scan set to occur every Wednesday at 3:15
   c) Client scans set to occur every Wednesday at 3:15
5) Configure Server Real Time Protection Options
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Server Real Time Protection Options
   b) Enable File System Real Time Protection should be enabled
   c) File types should be set to all file types
   d) Drive types should include Floppy and CD ROMs
6) Configure Client Real Time Protection Options
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Client Real Time Protection Options

Under the File System Tab

   b) Enable file system real time protection
   c) Under file types select all
   d) Under options neither “display message on infected computer” nor “exclude selected files and folders” should be selected
   e) Drive types should include Floppy and CD ROMs

Under the Microsoft Exchange Tab

a) Enable Microsoft Exchange Real time Protection should be enabled
b) Under file types choose selected (the default selected files are sufficient)
c) Under notifications enable "display message on infected computer", enable "send e-mail to sender", and enable "send e-mail to selected" (under the addresses button enter the addresses of the people that you want to receive notifications of e-mail viruses)

7) Configure Client Administrator only Options
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Client Administrator Only Options
   b) On the General tab under "Display" enable "Show Norton Antivirus Icon on Desktop"
   c) On the Security tab under "User Disable/Uninstall"
      i) Enable "lock the ability of users to load and unload Norton Antivirus Services" and enable " Ask for password to allow uninstall of Norton Antivirus Client"
      ii) Under Scan Network drive enable "ask for Password to scan a mapped network drive"
8) Configure Quarantine Options
   a) Right click on the NAVCE server and select All Tasks/Norton Antivirus/Quarantine Options
   b) Enable Quarantine or Scan and Deliver should be enabled
   c) Select "allow forwarding to a Quarantine Server"
   d) Browse to the NAVCE Server that you want to be the Quarantine Server
   e) Enter XXXX as the port
   f) Enter 600 as the retry
   g) Select IP as the protocol
   h) Select automatically repair and restore silently

Appendix 2

Norton Antivirus Corporate Edition Server (exchange server group configuration)

Installation Procedure:

Follow the same installation procedures as outlined in the Norton Antivirus Corporate Edition Server Installation documentation with the following modifications:

1) Create a separate server group with a separate primary server (can be an Exchange Server) (This server group will contain only Exchange Servers)
   a) Do not install Central Quarantine Locally
3) Follow the instructions in Symantec article 2000110108382448 to set the appropriate exclusions.

4) The exclusions are set in the Server Real-time Protection Options under options by selecting the exclusions
   a) Click the exclusions button
   b) Click the “check for file exclusions before scanning” check box
   c) Click the files/folders button
   d) Navigate to and select the appropriate files and folders to exclude

Appendix 3

Sample Configuration of Microsoft Software Update Services (SUS)

Configuration Procedure:

SUS Server:

SUS Server must be installed on a computer running Windows 2000 Server or better and running IIS. The installation file is SUSSetup.msi and can be found in the software directory on the main file server (or can be downloaded from the Microsoft web site).

Installation and Configuration of SUS Server

2) Execute SUSSetup.msi from ***server name**softwareshare*\MS Software Update Server\Server**
   After the installation is complete further configuration is done from http**://SUS Server/susadmin** through any web interface
2) From the administration website the following configurations need to be set

Heading		**Configuration**
Synchronize Server	Synchronization schedule	Daily at 03:00 with retry attempts set to 3
Set Options	Proxy Server configuration	None
	Specify the name your clients use to locate this update server	SUS Server.companyx.com
	Select which server to synchronize content from	Windows Update Server
	Select how you want to handle new versions of previously approved	Automatically approve new versions of previously approved updates

	updates	
	Select where you want to store updates	Save updates to a local folder
	Synchronize packages only for these locales	English

3) After the synchronization has completed the downloaded updates need to be approved.
   a) From the administration website navigate to the approve updates link
   b) Select the updates to approve and click on the approve button at the bottom of the page

SUS Client

SUS Client is installed via GPO. The GPO is located in Active Directory and is applied to the departmental "computers" OU.

4) Installation of the SUS Client
   a) The SUS Client will be automatically installed on all client computers that reside in departmental "computers" OUs by a GPO
   b) The configuration of the SUS Client Installation GPO is as follows:
      From the GPO MMC Snap in for the departmental "computers" OU in Active Directory navigate to
      Computer Configuration
         Software Settings
            Software Installation
               i) Right click software installation and select new package
               ii) Navigate to the location of the installation msi file **(*server name**softwareshare*\GPO Installation Files\Client\WUAU22.msi)**
               iii) Select open
               iv) Ensure that the GPO is assigned and click OK

Configuration of the SUS Client

5) The SUS Client will be automatically configured on all client computers that reside in the Install OU by a GPO
6) To be able to set up the SUS Client GPO the SUS Client must first be installed on the SUS Server
   a) To install the SUS Client on the SUS Server navigate to ***server name**softwareshare*\MS Software Update Server\Client** and double click on WUAU22.msi

The configuration of the SUS Client Configuration GPO is as follows:

7) From the GPO MMC Snap in for the Install OU in Active Directory navigate to Computer Configuration
   Administrative Templates

Windows Components

(i) Windows Update (if the windows update folder is not available then right click on administrative templates, click add\remove templates, click add, select wuau22.adm, click open, click close)
(ii) Double click Configure Automatic Updates
(iii) Select enable
(iv) Under Configure Automatic Updating select 4-Auto download and schedule for install
(v) Set the scheduled install day to everyday
(vi) Set the schedules install time to 03:00 and then click OK

(2) Double click Specify Intranet Microsoft update service location
(a) Select enable
(b) Set the intranet update service for detecting updates to the SUS Server
(c) Set the intranet statistics server to the Server running IIS

Appendix 4

Company X Group Policy Configuration Settings

Due to the length of the following table lines that have no settings associated with them have been deleted.

Section headings are colored with blue being the highest level, followed by red, teal and green. If a cell is blank then there is no setting associated with that option for that Group Policy Object.

		Default Domain	Default Domain Controller	Member Servers	SUS	No Screen Saver
Computer Configuration						
Windows Settings						
Account Policies						
Password Policy						
	Enforce password history	7 passwords				
	Maximum password age	90 days				
	Minimum password age	1				
	Minimum password length	9 characters				

	Passwords must meet complexity requirements	enabled				
	Store password using reversible encryption for all users in the domain	disabled				
Account Lockout Policy						
	Account lockout duration	0 min				
	Account lockout threshold	3 invalid				
	Reset account lockout counter after	180 min				
Kerberos Policy (DC only)						
	Enforce user logon restrictions		enabled			
	Maximum lifetime for service ticket		600 min			
	Maximum lifetime for user ticket		10 hours			
	Maximum lifetime for user ticket renewal		7 days			
	Maximum tolerance for computer clock synchronization		5 min			
Local Policies						
Audit Policy						
	Audit account logon events	success/failure				
	Audit account management	success/failure				
	Audit directory service access		failure			
	Audit logon events	success/failure				
	Audit object access	failure				
	Audit policy change	success/failure				
	Audit privilege use	failure				
	Audit process tracking	not defined				
	Audit system events	success/failure				
User Rights						

Assignments						
	Access this computer from the network	Administrators, Users	Administrators, Authenticated User, Enterprise Domain Controllers	Administrators, Enterprise Domain Controllers, Users IUSRXXX, IWAMXXX		
	Back up files and directories	Administrators	blank	blank		
	Bypass traverse checking	Users	Authenticated Users	Users		
	Change the system time	Administrators	blank	blank		
	Create a pagefile	Administrators	blank	blank		
	Enable computer and user accounts to be trusted for delegation	blank	Administrators	blank		
	Force shutdown from a remote system	Administrators	blank	blank		
	Increase quotas	Administrators	blank	blank		
	Increase scheduling priority	Administrators	blank	blank		
	Load and unload device drivers	Administrators	blank	blank		
	Log on as a batch job	blank	blank	IUSRXXX, IWAMXXX		
	Log on as a service	Blank	blank	blank		
	Log on locally	Administrators, Users	Administrators	Administrators,		
	Manage auditing and security log	Administrators	Administrators Exchange Enterprise Servers)	Administrators		

	Modify firmware environment values	Administrators	blank	blank		
	Profile single process	Administrators	blank	blank		
	Profile system performance	Administrators	blank	blank		
	Remove computer from docking station	Administrators, Users	blank	blank		
	Replace a process level token	blank	blank	blank		
	Restore files and directories	Administrators	blank	blank		
	Shut down the system	Administrators, Users	Administrators	Administrators		
	Take ownership of files or other objects	Administrators	blank	blank		
Security Options						
	Additional restrictions for anonymous connections	No access without explicit anonymous permissions				
	Allow system to be shut down without having to log on	disabled				
	Allowed to eject removable NTFS media	administrators				
	Amount of idle time required before disconnecting session	30 minutes				
	Audit the access of global system objects	enabled				
	Audit use of Backup and Restore privilege	disabled				
	Automatically log off users when logon time expires	disabled				
	Automatically log off users when logon time expires (local)	disabled				
	Clear virtual memory	enabled				

	pagefile when system shuts down					
	Digitally sign client communication (always)	disabled				
	Digitally sign client communication (when possible)	enabled				
	Digitally sign server communication (always)	disabled				
	Digitally sign server communication (when possible)	enabled				
	Disable CTRL+ALT+DEL requirement for logon	disabled				
	Do not display last user name in logon screen	enabled				
	LAN Manager Authentication Level	Send LM & NTLM – use NTLMv2 session security if negotiated				
	Number of previous logons to cache (in case domain controller is not available)	0				
	Prevent system maintenance of computer account password	disabled				
	Prevent users from installing printer drivers	enabled				
	Prompt user to change password before expiration	10 days				
	Recovery Console: Allow automatic administrative logon	disabled				

	Recovery Console: Allow floppy copy and access to all drives and all folders	disabled				
	Restrict CD-ROM access to locally logged-on user only	enabled				
	Restrict floppy access to locally logged-on user only	enabled				
	Secure channel: Digitally encrypt or sign secure channel data (always)	disabled				
	Secure channel: Digitally encrypt secure channel data (when possible)	enabled				
	Secure channel: Digitally sign secure channel data (when possible)	enabled				
	Secure channel: Require strong (Windows 2000 or later) session key	disabled				
	Send unencrypted password to connect to third-party SMB servers	disabled				
	Shut down system immediately if unable to log security audits	disabled				
	Strengthen default permissions of global system objects (e.g. Symbolic Links)	enabled				
	Unsigned driver installation behavior	warn but allow				
	Unsigned non-driver installation behavior	warn but allow				
Event Log						
Settings for						

Event Logs						
	Maximum application log size	1024 kb	819200 kb	819200 kb		
	Maximum security log size	1024 kb	819200 kb	819200 kb		
	Maximum system log size	1024 kb	819200 kb	819200 kb		
	Restrict guest access to application log	enabled	enabled	enabled		
	Restrict guest access to security log	enabled	enabled	enabled		
	Restrict guest access to system log	enabled	enabled	enabled		
	Retention method for application log	as needed	as needed	as needed		
	Retention method for security log	as needed	as needed	as needed		
	Retention method for system log	as needed	as needed	as needed		
	Shut down the computer when the security audit log is full	not defined	not defined	not defined		
System Services						
	Alerter	disabled				
	ClipBook	disabled				
	Computer Browser	disabled				
	Fax Service	disabled				
	Internet Connection Sharing	disabled				
	Messenger	disabled				
	NetMeeting Remote Desktop Sharing	disabled				
	Routing and Remote Access	disabled				
	Telnet	disabled				
Public Key Policies						
	Encrypted Data Recovery Agents	blank				
	Automatic Certificate	blank				

	Request Settings					
	Trusted Root Certificate Authorities	blank				
	Enterprise Trust	blank				
IP Security Policies on Active Directory						
Administrative Templates						
Windows Components						
Netmeeting						
	Disable remote Desktop Sharing	enabled				
Internet Explorer						
	Disable Periodic Check for Internet Explorer software updates	enabled				
	Disable showing the splash screen	enabled				
Windows Update						
	Configure Automatic Updates		disabled	disabled	Enabled set to level 4 auto download and schedule for install	
	Specify intranet Microsoft update service location		disabled	disabled	Enabled (company x SUS Server)	
System						
	Disable Autoplay	enable for all drives				
	Don't display welcome screen at logon	enable				

Group Policy						
	Group Policy refresh interval for computers	enabled				
	Internet Explorer Maintenance policy processing	enabled				
Network						
Network and Dial-Up Connections						
	Prohibit configuration of connection sharing	not defined				
Printers						
	Automatically publish new printers in Active Directory	enabled				
User Configuration						
Windows Settings						
Folder Redirection						
Application Data		\\servername\users…				
Desktop		\\servername\users…				
My Documents		\\servername\users…				
Administrative Templates						
Start Menu & Task Bar						
	Disable and remove links to Windows Update	enabled				
	Add Logoff to the Start Menu	enabled				
	Disable changes to Taskbar and Start Menu Settings	enabled				
	Do not keep history of recently opened	enabled				

	documents					
	Clear history of recently opened documents on exit	enabled				
Display						
	Activate screen saver	enabled				disabled
	Password protect the screen saver	enabled				
	Screen Saver timeout	enabled (900sec)				
System						
	Disable Autoplay	enabled				
Group Policy						
	Group Policy slow link detection	enabled				

References

[1] West Coast Labs Checkmark Antivirus comparison URL: http://www.check-mark.com/cgi-bin/redirect.pl
SC Magazine Product Reviews January 2001 Test Center URL: http://www.scmagazine.com/scmagazine/2001_01/testc/prod2.html - Norton

[2] "Best Practices for Norton Antivirus Corporate Edition realtime protection on Microsoft Exchange Server", Symantec Knowledgebase, last modified 02/13/2003 URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002051609590948?Open&src=ent_hot&docid=2002112210583948&nsf=ent-security.nsf&view=docid&dtype=corp&prod=Norton%20AntiVirus%20Corporate%20Edition&ver=7.5&osv=&osv_lvl=

[3] "How to prevent Norton Antivirus Corporate Edition from Scanning the Exchange Directory Structure", Symantec Knowledgebase, last modified 05/15/2003 URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2000110108382448?Open&src=ent&docid=2002051609590948&nsf=ent-security.nsf&view=552ba2f7636bedf088256818006f78bf&dtype=corp&prod=Norton%20AntiVirus%20Corporate%20Edition&ver=7.5&osv=&osv_l

[4] "Understanding Heuristics: Symantec's Bloodhound Technology" Symantec knowledgebase URL: http://securityresponse.symantec.com/avcenter/reference/heuristc.pdf
WhatIs.com, definition of Heuristics URL: http://whatis.techtarget.com/definition/0,,sid9_gci212246,00.html

[5] "Deploying Microsoft Software Update Services", Microsoft Inc. URL: http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

[6] SANS home page outlining security courses URL: http://www.sans.org/
MIS Training Institute home Page outlining security courses URL: http://www.misti.com/

[7] "Planning Organizational Unit Structure" Microsoft Windows 2000 Server Documentation, Microsoft Inc. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?URL=/windows2000/en/server/help/sag_ADdeploy_9.htm

[8] Center for Internet Security home page with links to Windows 2000 Server and Professional configuration documentation (I am unable to link directly to the documentation) URL: http://www.cisecurity.com/

[9] Windows 2000 Guides, National Security Agency Security Recommendation Guides URL: http://www.nsa.gov/snac/win2k/download.htm

[10] "Step by Step guide to using the Security and Configuration Tool Set", Microsoft TechNet Microsoft Inc. URL: http://www.microsoft.com/technet/treeview/default.asp?URL=/technet/prodtechnol/windows2000serv/deploy/walkthru/seconfig.asp

[11] Ftp location for D-Link 604 User Manual URL: ftp://ftp.dlink.com/Gateway/di604/Manual/di604_manual_204.zip