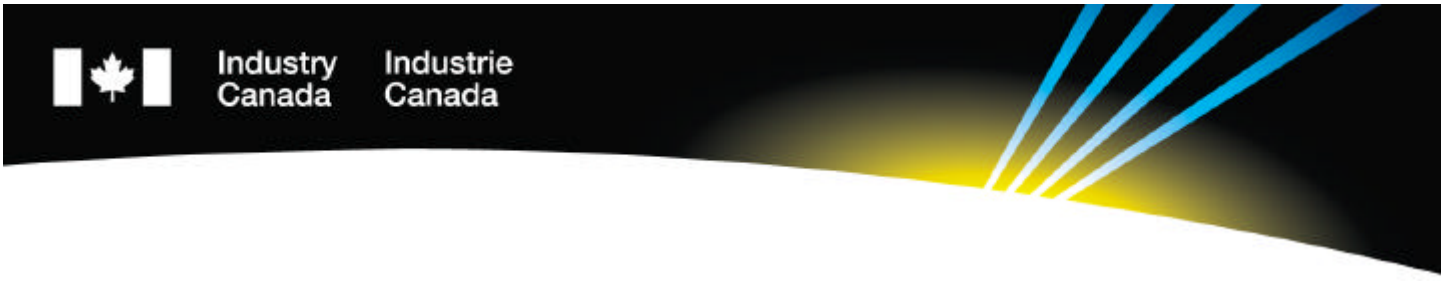

AUDIT
OF THE
CORPORATIONS DIRECTORATE
LOCAL AREA NETWORK (LAN) SECURITY

September 16, 1997

Audit & Evaluation Branch

Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Audit and Evaluation Branch conducted an audit of the controls surrounding the Local Area Network (LAN) in the Corporations Directorate during the first quarter of the 1997-1998 fiscal year. This audit was planned and approved in the 1997-1998 Audit and Evaluation Branch plan.

The Corporations Directorate has implemented many strong controls that minimize security risks. However, in a changing systems environment, security weaknesses can result. This report identifies effective controls used as well as areas where Corporations Directorate can strengthen systems security.

Effective Controls

The effective controls listed below serve to strengthen systems security because Corporations Directorate has ensured that:

- employees leaving the Directorate are immediately deleted from the list of authorized LAN accounts thereby reducing the risk of unauthorized access to the LAN;
- passwords are encrypted when transmitted from the workstation to the server during logon;
- physical security of the LAN server is strengthened by securing the server in a special computer room locked with a keypad. In addition, there is restricted access to the Directorate area resulting in double security for the LAN server;
- full backups for servers are performed on a daily basis and tapes are sent offsite to National Archives on a monthly basis;
- remote access by teleworkers is well controlled to the LAN as passwords and other controls are used to protect against unauthorized access; and
- access to the LAN is protected by enabling the 'intruder detection' feature of Novell.

Controls to Strengthen Systems Security

The Corporations Directorate can strengthen systems security by:

- ensuring that staff cannot be concurrently connected to the LAN from two workstations at the same time;
- monitoring intruder alerts;
- reducing the number of grace login attempts to the LAN to five from nineteen on initial sign-on and for new passwords; and
- protecting the computer room by changing the keypad code every 60 days and using a password to protect the LAN server console.

Management's Response

The Manager, Corporations Informatics Services of the Corporations Directorate, has agreed with the recommendations to strengthen security. Implementation of all recommendations has been made as indicated in the report.

Appendix A

To provide additional assistance to the Corporations Directorate, Appendix A is included in the report as a guide to be used when the Directorate converts from NetWare 3.12 to NetWare 4.x.

BACKGROUND

The Corporations Directorate of Industry Canada administers the Acts covering federally incorporated business and non-profit entities. It currently has one Fulcrum Pentium server, two Novell 3.12 servers with approximately 80 regular users, two Siemens application servers, an HP development server for a new architectural environment and an HP production server.

Following the participation of the Corporations Directorate in a pilot project of a systems security self-assessment process, the Audit and Evaluation Branch arranged with the Directorate to audit the security controls of the Local Area Network (LAN).

Objectives

The objectives for this audit were to ensure that controls:

- prevent unauthorized alterations of data;
- provide a sound basis for change control;
- satisfy the business requirement that all data remains complete, accurate, and valid;
- provide a sound physical environment to protect the equipment and data;
- will result in important LAN administrative functions being performed regularly by a schedule of support activities;
- will provide an effective security and internal control framework policy;
- result in only authorized individuals having access to information technology assets (including data); and
- provide an adequate framework to prevent and detect viruses.

Scope

The scope of the audit covered all LAN servers, remote access, and workstation security located in the Corporations Directorate. Since Lotus Notes and Internet Access are administered centrally, these were excluded from the audit. The Electronic Commerce project, which will be developed in late 1997-1998, was also excluded from this audit.

METHODOLOGY

Auditors began this project by becoming familiar with the LAN and security environment and by gaining an understanding of the main roles, responsibilities, mandates, mission of the Corporations Directorate within Industry Canada and relevant policies and standards pertaining to LANs within the Department.

A preliminary meeting was held between the audit team and Directorate staff to understand the Corporations Directorate environment and get agreement of the audit scope and objectives. A review of the self-assessment questionnaires, completed by Corporations Directorate staff, and

documents of all relevant policies and standards pertaining to Local Area Networks included in Lotus Notes were completed.

A preliminary assessment was made of the security control framework by evaluating controls for:

- LAN operations including the communications network;
- integrity (completeness, accuracy and authorization) of system data and processing;
- availability of data and services (contingency planning and back-up);
- confidentiality of data (to protect against unauthorized disclosure); and
- integrity of data (protection against corruption and unauthorized modification of data).

The audit team developed audit criteria by using various sources such as:

- corporate priorities and themes;
- generally accepted private sector practices;
- standard LAN security guidelines;
- "best practices" used throughout private industry;
- other relevant published information; and
- extensive experience of the audit team members (from Progestic International).

The overall situation was analysed based upon the security control framework assessed and audit criteria developed (see Appendix B for a complete listing of audit criteria).

Auditors then evaluated the audit issues and lines of inquiry by reviewing documents, interviewing staff, collecting evidence, analysing detailed information, and conducting audit tests.

A sample of managers and users that were involved in the design and installation of the LANs were interviewed (see Appendix C for a list of the staff interviewed). Audit testing was conducted as required and fieldwork continued by reviewing and evaluating the following:

- location of file servers;
- backup/recovery process including the use of Uninterruptable Power Sources (UPS) and automated backup processing for the workstations and file server;
- equipment maintenance procedures;
- password administration;
- security logging and audit;
- security tools used in Corporations Directorate;
- virus protection;

- remote access controls;
- connectivity controls; and
- generic Internet access controls.

A debriefing of the observations made during the audit was completed with staff of the Corporations Directorate prior to preparing the audit report.

ISSUES

1.0 *ENSURE CONTROLS PREVENT UNAUTHORIZED ALTERATIONS OF DATA.*

1.1 Concurrent Connections

The staff can be simultaneously logged onto two LAN workstations at the same time. Data residing on the LAN can be corrupted if the same person is attempting access from two different sources. In addition, if an authorized person is logged concurrently on two machines then one machine is either dormant or attended by an unauthorized person. If the account name and password of a user are discovered at the dormant workstation, the Directorate is at risk of having an unauthorized individual gain access to the LAN. The authorized individual would then be accountable for the actions of the unauthorized person.

Recommendation

Each LAN user should be prevented from simultaneously logging onto two workstations. This can be accomplished by setting the “concurrent connections parameter” to '1'. By implementing this recommendation, there is neither an additional overhead placed on the LAN, nor is any cost incurred when changing this parameter.

Management’s Response

This recommendation has been implemented.

2.0 *ENSURE CONTROLS PROVIDE A SOUND BASIS FOR CHANGE CONTROL.*

2.1 Novell Patches

A patch is a fix or modification to the Novell Operating System (NetWare). Sometimes patches are installed because of problems found in NetWare and sometimes patches are installed to enhance the performance and functionality of NetWare. As part of the audit testing, auditors reviewed the list of patches installed on both the LAN server and the workstations. Auditors found that the latest patch for client authentication is not the most recent Virtual Loadable Module (VLM) version. The VLM version found was version 1.20 (941108). Novell confirmed that the most recent VLM version is 1.21. Although Corporations Directorate is not experiencing a threat to the integrity of its LAN data, the VLM version 1.20, in lieu of version 1.21, may cause an increase in administrative overhead and greater possibility of trouble for LAN Administrators.

The LIBUPC.EXE patch, the STRTL5.EXE patch, and the VRPUPI.EXE patch are the most current versions on the LAN server. The SMSUP.EXE patch date on the LAN server is

March 1, 1996. The most recent patch should be July 23, 1996.

Although only two patches were not current, not updating the Novell patches exposes the Directorate to the risk of LAN functions that are error prone, and to the risk of not having functionality provided by Novell.

Recommendation

Corporations Directorate should install all current versions of patches on a timely basis. To manage this process, the Directorate should establish a log documenting the:

- dates patches are received from Novell and installed
- reasons for the patch and justification for not installing a patch; and
- signature of the LAN Administrator.

Management's Response

This recommendation has been implemented.

3.0 *ENSURE CONTROLS SATISFY THE BUSINESS REQUIREMENT THAT ALL DATA REMAINS COMPLETE, ACCURATE, AND VALID.*

3.1 Processing and Intruder Detection Logs

The LAN server error log and the console log file are automatically produced by the Novell Operating System. These logs contain important information including: account, date/time of access, files accessed, applications used, errors, logoff time, and other important information. For example, the SYS$LOG.ERR file notifies LAN administrators of intruders attempting to access the network. The CONLOG.TXT file captures commands used at the server. It is important to review this file to verify the commands that are being issued at the console, and possibly foresee any threats to the LAN environment

The intruder detection log also is configured to lock a valid account using an invalid password after a predetermined number of consecutive attempts. After the expired time has elapsed, the user can login into the network again.

One method used by people attempting to gain access to a LAN is to use a password cracker. This software will attempt to guess passwords of users by reading the password file located on the Novell file server. Auditors attempted to use a password cracker to ensure that passwords were difficult to guess. Since the intruder detection is invoked, the password cracker was not able to run. This is an effective preventive control.

Auditors found that these logs are not monitored on a regular basis. This puts the Directorate at risk of not detecting unauthorized accesses, problems, or patterns of usage. Auditors reviewed

the console error log file and found that there were two intruder lockouts that were active. If the LAN Administrator reviewed the same log file, he/she could have investigated why the lockouts occurred.

Recommendation:

The Corporations Directorate should establish a policy stating that the LAN Administrator will regularly review the logs, document any findings observed and seek preventive procedures when the errors are of a significant nature.

Management's Response

The Directorate has implemented this recommendation. It will document the dates when these logs have been monitored. In addition to implementing this recommendation, Corporations Directorate has installed a LAN analyser to monitor the efficiency of the network.

3.2 Automatic Logoff / Screen Saver

When users leave their workstations unattended for a period of time, an effective control would cause a workstation to logoff automatically from the LAN to minimize risk of unauthorized access from the inactive workstation. This control is not used in many cases as it is considered impractical.

However, a screen saver software with a password is an alternative control to an automatic logoff. Using a screen saver software also reduces the wear on the screen and, if a password is used, locks the workstation from unauthorized use. A few workstations were selected to test this control. The result of the test showed that the screen saver with passwords was not used. The LAN Administrator believes that only about 40 % of users have enabled their screen savers.

To use the screen saver with password effectively, one must set a time limit after which the screen saver is enabled automatically. If the time limit is too long, the benefits of the screen saver with a password are lost as the workstation will still be exposed to unauthorized access. To use this control practically, one can set a longer time limit and show the user how to activate the screen saver whenever a pre-planned long absence from the workstation occurs.

Since the Directorate operates behind secure doors, the risk is minimized that someone can access data if this control is not used.

Recommendation

Although the Directorate operates behind secure doors, Corporations Directorate should encourage users to enable a screen saver with a password to strengthen unauthorized access.

To facilitate the use of the control, the LAN Administrator should advise users about an appropriate time limit and how to activate the screen saver lock whenever the user wishes.

Periodically testing this control by selecting a random sample of workstations would verify how well the users are adapting to this control.

Management's Response

This recommendation has been accepted by the Directorate. The LAN Administrator will encourage the use of a screen saver with password and will periodically test this control.

4.0 *ENSURE CONTROLS PROVIDE A SOUND PHYSICAL ENVIRONMENT TO PROTECT EQUIPMENT AND DATA.*

4.1 Access

Access to the computer room is controlled by a locked door that has a keypad access. Only staff requiring access know the keypad code. In addition, maintenance staff are supervised at all times when requiring access to the computer room.

The keypad access code is only changed when staff leave. Infrequent change of the keypad access code exposes the Directorate to unauthorized people gaining access to the computer room.

For further protection, the LAN server console can be password protected to restrict access. This control was not used. Combining the infrequency of changing the keypad access with the unlocked server console exposes Corporations Directorate to greater risk of unauthorized access.

Recommendation

The Corporations Directorate should change the keypad access code at least once every 60 days or sooner if staff leave. It should also ensure that the LAN server console is password protected at all times.

Management's Response

This recommendation has been implemented. In the future, Corporations Directorate will record, in the hardcopy log book, the date the keypad access code and LAN server console password are changed. This will be done once every 60 days or sooner if staff leave.

4.2 Electrical Power

Corporations Directorate has connected the LAN servers to an Uninterruptable Power Supply (UPS). This will keep the servers operating for about five minutes in the event of a power interruption. Auditors believe that five minutes is not sufficient time for an orderly shutdown of the file server.

Recommendation

The UPS should provide for a minimum of 20 minutes of time for servers to continue operation in the event of a power interruption.

Management's Response

The LAN Administrator tested the five minute time frame and found that an orderly shutdown occurred. However, Corporations Directorate agrees that a longer time limit would be better. It will seek to change the time limit.

5.0 *ENSURE CONTROLS WILL RESULT IN IMPORTANT LAN ADMINISTRATIVE FUNCTIONS BEING PERFORMED REGULARLY BY A SCHEDULE OF SUPPORT ACTIVITIES.*

5.1 Backup Processing

Full server backups are performed daily Monday to Friday. After every backup, the person performing the backup signs the backup log book. Monthly backup tapes are stored offsite at the National Archives.

Review of the backup logs found that backups have been successfully signed-off in the log book for the last three months. Auditors also verified that there are four daily and one weekly backup tapes. These were clearly labelled.

Staff are encouraged to place all their data onto the LAN "P:" drive. This ensures that the data is backed up on a regular basis as part of the normal LAN backup process. However, we found that a few individuals save their data to their local hard disk ("C:" drive). There is no evidence that these individuals are backing up their locally stored data.

Recommendation

Corporations Directorate should remind staff that data on their local hard disk "C" drive is not backed up by the LAN Administrator.

Management's Response

Corporations Directorate is planning quarterly reminders about security issues such as reminding staff that no backups are done on the "C" drive by the LAN Administrator to encourage staff to save data on the server P drive.

5.2 Password Maintenance

Corporations Directorate policy states that passwords should be changed every 90 days. This is good practise for users. However, we found that the LAN supervisor password is only changed when an employee or consultant leaves the Directorate. We believe that this is insufficient and exposes Corporations Directorate to greater risk of unauthorized people learning the Supervisor password.

Recommendation

The Corporations Directorate should implement a policy requiring the supervisor password be changed at least once every 30 days.

Management's Response

Corporations Directorate implemented this recommendation.

6.0 *ENSURE CONTROLS WILL PROVIDE AN EFFECTIVE SECURITY AND INTERNAL CONTROL FRAMEWORK POLICY.*

6.1 Novell NetWare Utilities

NetWare utilities like SYSCON, NETCON, RCONSOLE are read-only in order to protect them from accidental modification or deletion.

NetWare client configuration files located at the individual workstation level (like Net.cfg and Startnet.bat) are not protected and can be accidentally erased. If these files are accidentally modified or deleted then Corporations Directorate is exposed to the risk of having users lose their LAN connectivity. The LAN Administrator must then reconnect the user. In addition, if a user loses his/her connectivity in the middle of modifying data, then the data may become corrupted.

Recommendation

Corporations Directorate should ensure that NetWare client files are protected from accidental modification.

Management's Response

The LAN Administrator has changed these files to be read-only on all workstations. In addition, copies of these files for each user now reside in a new directory on the LAN server. This acts as a backup to ensure that if a user accidentally erases his/her files, the LAN Administrator can copy the files from the LAN server back to the user workstation.

7.0 *ENSURE CONTROLS RESULT IN ONLY AUTHORIZED INDIVIDUALS HAVING ACCESS TO INFORMATION TECHNOLOGY ASSETS (INCLUDING DATA)*

7.1 Login

Critical LAN login scripts, like NET$SYS.DAT, are protected. Users can view their login scripts but cannot modify, delete or rename them. They are protected from accidental modification or deletion.

7.2 Remote Access

Users have the ability to remotely dial into the LAN for access to mail and network resources. Effective controls of the remote access software (ReachOut) are used. The user enters a password and then the remote access software dials back to a pre-designed number. Where users are calling from a switchboard, a security card with a pass number is synchronized/associated with the given code number of that user. These are effective controls.

The RCONSOLE command enables a user to access the Novell LAN server console from a network connected workstation. If this command is allowed to be performed by everyone, then the LAN environment is at risk of having unauthorized people performing console commands.

Corporations Directorate has password protected the RCONSOLE command, and normal users do not have access to this command. This is a strong control.

7.3 Salvaging Deleted Files

When files are deleted they are not permanently deleted but remain on the hard disk. Only their directory entries are deleted. DOS allows people to recover files if the files have been accidentally deleted. This UNDELETE command is not permitted by Novell.

Novell works in the same way as DOS. Deleted files are retained until the disk space they occupy has to be reused. However, Novell does not allow the use of the UNDELETE command but has its own command called “salvage”. This is a useful command for LAN Administrators to recover accidentally erased files. Users can only “salvage” files to which they have create access.

7.4 Inventory

The Industry Canada corporate inventory report was verified to the Corporations Directorate inventory report. No discrepancies were found. In addition, auditors were able to physically locate all equipment listed on both inventory reports.

7.5 Grace Logins

Grace logins is the NetWare parameter that provides someone with the ability to log onto the LAN a certain number of times with an expired password. This is used primarily when passwords are automatically changed and also for new users.

We found that grace logins on initial sign-on and new passwords to the LAN is set at 19 attempts. This means that a person has 19 attempts to gain access to the LAN. In the case of automatically changing a password, this can amount to several weeks.

Recommendation

This parameter should be changed to a maximum of five grace logins for greater protection.

Management’s Response

This parameter has been changed to five as recommended.

7.6 Access Rights

Users are currently granted full rights, except for supervisor “S” rights, to their own home directory and files. This means they have the ability to read, write, create, erase, modify, scan, and provide access (to their files) control to other users.

Having the "access" right enables one user to give other users rights to the home file/directories or to modify that file/directory's inheritance rights. In other words the user becomes a mini

supervisor. For example, John has "A" rights to his home directory and can grant full rights to Sam. Sam can then modify and delete John's files.

Although most users within the Corporations Directorate do not know how to perform this function, granting "A" rights still exposes Corporations Directorate to the risk of having unauthorized people given access to LAN files.

Recommendation

Corporations should not permit normal users to have the access control right "A" to their home directories.

Management's Response

This recommendation has been implemented.

8.0 *ENSURE CONTROLS PROVIDE AN ADEQUATE FRAMEWORK TO PREVENT AND DETECT VIRUSES.*

There are currently over 6,000 known viruses with three new viruses being discovered everyday. In order to minimize the possibility of a virus attack, Corporations adheres to the Industry Canada policy on viruses found in the "*ISTC Handbook on IT Security For Shared-Facility (LAN) & Application Managers*". This policy indicates that users must be instructed to systematically run recommended, updated antivirus scanning programs. The Directorate regularly scans their hard disks using the Norton Anti-Virus (NAV) software. This is a strong control.

Information reporting viruses that have been detected is placed onto the Lotus Notes Knowledgebase. This allows Corporations to monitor statistical information concerning the detected viruses and research detected viruses.

8.1 Internet Viruses

Files downloaded either from the Internet World Wide Web or attachments from e-mails received from the Internet should be scanned by each individual employee before executing the file or reading the file. This is automatically accomplished by the Norton Anti-Virus utility used at Industry Canada. NAV automatically scans files before files are opened.

In most cases the afore-mentioned procedure is adequate. However, in some cases a virus could slip through. Industry Canada, like many other government departments, does not have a process to automatically scan files before these reach individual workstations.

The *Norton AntiVirus for Internet E-mail Gateways* product would ensure that files are scanned for viruses before reaching the individual workstations. This product automatically scans files at the Simple Mail Transfer Protocol (SMTP) gateway. It automatically intercepts and destroys incoming and outgoing viruses hidden in e-mail attachments before they cause damage and spread.

There is practically no impact on network or firewall performance. This product is transparent to users and stops viruses before they reach individual workstations. It even notifies both the sender and receiver of the e-mail that a virus was detected.

The NAV for Internet E-mail Gateways can be downloaded from the Symantec website for a free 30 day trial.

Recommendation

Since SMTP gateway is not the responsibility of the Corporations Directorate, Audit will forward this recommendation to the people responsibile for the gateway.

Management's Response

To strengthen this control even further, the Corporations Directorate will add a column in the "log book" to indicate when the Lan Administration has installed the updated version of the NAV software on the Directorate's network.

APPENDIX A

Guide to be used when the Directorate converts from NetWare 3.12 to NetWare 4.x.

This Appendix is intended for use by technical personnel. It describes differences between NetWare 3.12 and NetWare 4.x. It includes the preparation for the migration and the differences of migration methods and security features.

The following is a brief summary of the differences between NetWare 3.12 and NetWare 4.x:

- ease of administration, with more enhanced NetWare utilities (NetWare Professional Reference - 4th Edition, Karanjit Siyan, PhD - New Riders Publishing, 1995 pg 345);
- NetWare Directory Services (NDS). Users now log into NDS (NetWare Directory Services) which authenticate to all servers on the network;
- improvements in NetWare file system management;
- improved file system security and management;
- support for network auditing;
- simplified and more efficient memory management architecture;
- greater levels of disk utilization and maximization due to sub-block allocation and file compression; and
- higher levels of fault tolerance with System Fault Tolerance level III (SFT III) where there can be any single point of failure.

Preliminary Preparations

Run bindfix and vrepai

These are utilities supplied by Novell for fixing any corrupted files, bindery, and hardware issues. They ensure the integrity of the bindery files and delete mail directories and trustee rights of all users who no longer exist on the server.

Clean up the file system

Scan through directories on the server and delete files and directories that are no longer required. The in-place migration strategy install program needs approximately 50 megabytes of free disk space on the SYS volume. Therefore, run the purge utility from NetWare to clean up unnecessary files and help free limbo blocks.

Before migrating, make backup copies of STARTUP.NCF and AUTOEXEC.NCF. For backup purposes, print a copy of the system login script called NET$LOG.DAT in the SYS:PUBLIC directory.

Testing

Test the Virtual Loadable Modules (VLM) and client authentication files like net.cfg and startnet.bat. Net.cfg is a configuration file containing all the non-default settings for the Corporations Directorate environment. Contact all your software vendors to get assurances that their applications will work with VLM.

Naming Conventions

Naming conventions are a set of rules that govern how objects will be defined on the network. NetWare 4.x allows you to have full object names that are up to 255 characters long. By establishing naming conventions, you can ensure that across the network there will be consistency, usability, and ease of use in the names assigned. Naming conventions cover such objects as user names, server names and printers. Naming conventions should be established before the migration to NetWare 4.x since it will be impossible to affect changes after implementation. Some general suggestions for naming conventions include:

- keep the name short and descriptive;
- be consistent throughout the network; and
- use alphabetic and numeric characters where possible.

Tree

Since NetWare 4.x authenticates users into a tree and not a server, developing naming standards is extremely important. NetWare 4.x uses the Network Directory Structure (NDS) tree for defining all objects. The NDS is called a tree because of the way it is logically defined similarly to an upside-down tree. When you install the NetWare 4.x server, you will name the tree and define the context (or location within the tree) in which the server object will reside.

Backup

Ensure that a full successful backup has been completed before performing the upgrade.

Disable logins and shut down any e-mail gateways, virus, Internet, lotus notes running on the server. It is important to shut down anything that keeps files open on the server. This ensures that no files are skipped during backup

Migrating Methods

There are three ways of migrating to NetWare 4.X:

1. In Place Upgrade

This method uses the install program (install.nlm) to install the version of NetWare right over your existing 3.12 server. All bindery information and file system information is upgraded in place on your existing server.

The disadvantage of this method occurs if something goes wrong and you need to return to your previous version of NetWare. You must restore from the backup made prior to the installation of NetWare 4.X. Reverting to the previous version of NetWare can be very time consuming.

The advantage of this method is that only one server machine is required and user passwords are retained. This method is not recommended because of the many disadvantages.

2. Across the Wire method

For this method you need to set up a new NetWare 4.1 server using new hardware while the old server continues to function. Therefore, you need a source server and a destination server. Information from the existing 3.12 server is migrated to the new server using the dsmigrate and the file migration utilities run from a workstation attached to both servers. This is the safest method except it requires an extra piece of hardware.

The bindery information is first moved to the working directory on the workstation that is running the MIGRATE utility, translated to the NetWare 4.x format, and then migrated to the destination server. This migration method allows you to preserve the original server environment meaning. There is minimal risk of data loss during the migration process.

Steps for Across the Wire migration:

A. Plan your NDS tree. (Note: you do not have to plan your entire tree at this point simply plan the structure.)

B. Install NetWare 4.x on the new server

C. Login to your destination and source servers. Before you can run DS migrate and file migration, you must be attached to the appropriate servers. From a workstation login as Admin to the new NDS tree that contains your destination server, then set this tree as your preferred tree

.D. Start DS migrate and run the discover option. Start the NWADMIN utility and select DS Migrate from the tools menu

E. Model the off-line tree

F. Configure the live NDS tree

G. Start the file migration utility

H. Select a source volume

I. Select a destination directory

J. Migrate the file system data

Note:

After the backup is complete ensure that latest patches are applied.

Although the sub-block allocation and the file compression are enabled by default, ensure that this has occurred. One can verify this by using the NetWare utility SERVMAN. This will maximize disk utilization.

3. Same Server Method

This method moves all data off-line, upgrades the server operating system/hardware, and then migrates the data back to the same server. This is used when upgrading a server that will be installed on the same hardware as the old source server. Although you only use one server with this method, there are some risks involved. You also may not be able to migrate file attributes and trustee rights. If for any reason, there is a failure in the migration process, you may not have a server on which to rely and will have to reinstall the original operating system and restore from tape. You will need to use a third party backup program when performing this process since NetWare backup tools are not supported by this migration utility.

To accomplish this method you first need to backup the data files onto a tape drive and migrate the bindery information to the working directory on a workstation. Then you install NetWare 4.x on your original server. Finally, you restore the data from tape and translate and migrate the bindery information from the workstation back to the new NetWare 4.x server

Security Issues

- NetWare 4.x adds an additional component called Network Directory Services (NDS) security. The three elements of NetWare 4.x security are: Login Security, NDS Security, File System Security

    1. **Login Security** - This controls who can gain initial entry into the network. The login authentication of a user must be done against the user object stored in the global NDS database. Login restrictions are done on NDS objects and include: account restrictions, password restrictions, station restrictions, time restrictions, and intruder limits.

    2. **NDS Security** - This is used to determine what network resources (NDS objects) the user is allowed access to. The kind of operations a user is permitted to perform on an NDS object are called rights.

3. **File System Security** - It is very similar to NDS security. This applies to files/directories outside of the user's home directory.

- **NDS** - Be aware that utilities such as NWADMIN are very powerful and should have limited access. Consideration should be made to move this utility out of public and to a separate directory with only administrator access.
- Ensure a strategy is implemented for assigning rights by means of group assignments.
- Consider moving other NetWare utilities such as NETADMIN and RCONSOLE into separate directories along with NWADMIN.
- Consider creating IRF (inheritance rights filters) to block rights to NetWare SYS:SYSTEM.
- Create accounts for Administrators with the "S" right other than ADMIN (default), stay away from generic accounts having the "S" right due to the lack of accountability.
- New with NetWare 4.X is **"AUDITCON"** this enables auditors to trace the steps of users and/or administrators. In other words AUDITCON will let you see the files and directories which an individual has been looking at.
- NetWare 4.X provides the highest level of Fault tolerance (SFT III). This is a complete mirror of the entire server. Therefore, should any component in the production server fail, the backup server will take over, leaving users with no down time.
- **Password encryption -** When users log into Netware versions 3.0 and later, their password is encrypted before being sent across the wire. This prevents hackers from deciphering the password when using a protocol analyzer or other device that intercepts network packets.

  However, encryption can cause problems if there are servers running Netware versions prior to 3.0. Therefore, Netware 4.x allows the manager to change the default and unencrypt passwords. This can be accomplished using the SERVMAN utility which provides a way to change the server's startup parameters including the encryption of passwords. The default for Netware 4.x is to have the Allow Unencrypted Passwords parameter set to *Off*. Meaning that passwords are encrypted.

  In addition to using passwords as a first line of defence, Netware 4.x provides enhanced security features. One of these features is authentication to verify that users are authorized to use NDS. This is referred to as Network based security. Authentication assigns a unique identification to each user for each login session. It is the identification, not the user's password, that is used to authenticate each of the user's network requests. Security is enhanced because the password is never transmitted across the entire network where it could be monitored. It is only transmitted to the server. Authentication guarantees that a user's password never goes beyond the login process.

APPENDIX B

AUDIT CRITERIA

The following audit criteria were used to determine the effectiveness of controls:

SECURITY

1. Logical access to and the use of the LAN should be restricted by implementing adequate authentication mechanisms associated with access rules.
2. Procedures should be implemented to comply with the security policy that provides access security control based on an individual's demonstrated need to view, add, change or delete data.
3. Procedures should exist to ensure timely action relating to requesting, establishing, issuing and closing of user accounts.
4. There should be a control process in place to periodically review and confirm access rights.
5. Controls should be in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a central manner to obtain global access control.
6. The Corporations Directorate security administration should assure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity.
7. A computer security incident handling capability should exist to address security incidents. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and orderly response to security incidents.
8. Management should establish a framework of adequate preventive and detective control measures.
9. All personnel should be trained and educated in system security principles. The training program should include: ethical conduct of the information services function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.

MANAGEMENT

10. Management should define and implement a problem management system to ensure that all events which are not part of the standard operation (incidents, problems and errors) are recorded, analysed and resolved in a timely manner. Incident reports should be established in the case of significant problems.

11. Management should ensure that there is adequate protection of sensitive information during transmission and transport against unauthorized access and modification.

12. Management should implement procedures to ensure the non-disclosure of sensitive information. The procedures should guarantee that media containing data marked for disposal are reviewed and handled accordingly to avoid sensitive data being retrieved by a third party from the disposed media.

MEDIA

13. Procedures should be established to assure that contents of the media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion and that measures are taken to maintain the integrity of magnetic media stored in the library.

14. Back-up procedures for media should include the proper storage of the data files and software. Backups should be stored securely, and the storage sites periodically reviewed regarding physical access security and security of data files and other items.

PHYSICAL SECURITY

15. Appropriate physical security and access control measures should be established in conformance with the general security policy. Access should be restricted to individuals who have been authorized to gain such access.

16. Sufficient measures should be put in place and maintained for protection against environmental factors (e.g. fire, dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment should be installed.

17. Uninterruptable power supply batteries and/or generators should be installed to secure against power failures and fluctuations.

APPENDIX C

LIST OF INTERVIEWEES

- Louise Bedard, Data Base Administrator
- Gilles Lacroix, Technical Manager
- Patti Pomeroy, Manager, Corporations Directorate Informatics Services
- Martino Rafael, LAN Administrator
- Jean-Pierre Lafrance (consultant), Desktop Support