INFORMATION MANAGEMENT: STRATEGY, SYSTEMS, AND TECHNOLOGIES

DEVELOPING A NETWORK SECURITY PLAN

Frederick Gallegos and Stephen Tanner

INSIDE
Securing the New Distributed Environment, Review of Security and Control Threats, Countering Threats, Applying Methodologies in a Novell Environment, Security Tools

INTRODUCTION
Distributed environments security is becoming one of the greatest areas of concern for organizations around the world. The convergence and growing use of the Internet, microcomputer-based networks, wide area networking, intranets, extranets, and electronic mail have increased the security exposure of most organizations.

In this environment, IS managers and executives rely on the assistance of security and audit personnel to devise plans that effectively monitor the complex distributed environments of today and tomorrow. This article reviews the changing role of audit and security in distributed environments, the types of threats present in these environments, the range of methodologies available for securing a sample Novell network, and some of the current technologies and tools available for maintaining network security.

SECURING THE NEW DISTRIBUTED ENVIRONMENT

Over the years, the definition of distributed environments has changed. Technology has produced hardware and software to meet the needs of organizations to integrate automation of their work processes and data collection and storage. For the purposes of this discussion, a distributed environment is defined as follows:

A collection of computer hardware components joined together within a building or spread over a geographically diverse area with telecommunications software and cabling. The goal is to allow the

PAYOFF IDEA
Distributed environments add a new level of complexity to security and control. Using a typical Novell network environment, this article presents five models of increasing security, audit, and control levels that protect against several broad categories of security threats.
sharing of data, software applications, communications, and hardware to automate the manual processes of an organization in the realization of its mission and objectives.

An organization’s information assets have differing levels of value. On one level, there are the costs of hardware, software, and technology used to develop and store data to generate information. On another level, there are the human resource costs of actually collecting and interpreting data in order to store meaningful information for ongoing decision making. Finally, there is the value of keeping the information confidential and secret from outside entities.

The importance of network security is its goal of preserving the varying levels of investment, maintaining trustworthy and accurate data, and ensuring a sustainable level of trust in the automated systems used to collect, store, and disseminate accurate, reliable information.

REVIEW OF SECURITY AND CONTROL THREATS
Security threats take on many forms. The goal of developing this list is not to provide exhaustive sources, but to provide a framework for evaluating exposure in the major categories outlined. These areas present new roles for audit and security personnel in conducting their reviews and providing the IS executives and managers with assurances that controls are in place and working effectively.

The four main security categories are as follows:

1. Physical security (including hardware)
2. Operating system-level security
3. Communications security
4. Procedural security

Physical Security and Control Threats
Following are some of the areas of physical vulnerability:

• Hardware attack. In a hardware attack, someone attaches a device to the network to gather and siphon off data. Typical invasions include the installation of trojan horses and viruses.
• Software attack. In a software attack, workstation modules (operating systems, TSRs, and application software) are modified to gather data from the system and save it for later retrieval, or to deny network or data access.
• Masquerade attack. Here, the perpetrator uses the identity of an authorized user to obtain access to the network, and then reviews its structure and data.
• Unauthorized copying of software and data. In this case, the perpetrator installs unlicensed software or violates the licensing agreement through unauthorized copying of software; the person may also breach company confidentiality through the extraction of company data and information.

Operating System-Level Security Threats
This type of network attack results from unauthorized individuals installing software that circumvents operating-system-level security and allows them to go around restrictions designed into the operating system. Often, exposure to this threat is through commercially available software that has been written to take advantage of inherent bugs or loopholes in the operating system.

Communications Security Threats
These types of threats come in two forms:

1. Tapping. Tapping means that an open telephone line in a data communications system is accessed for the purpose of tracking data flow.
2. Spoofing. In this case, an outside party pretends to be a server or peer authorized for data or network access.

Procedural Security Threats
Although procedural security threats cover an enormous range of topics, the category can be broken down into four main elements:

1. How effectively has software been installed?
2. How well is the system being administered?
3. How are user rights and privileges being managed?
4. How is the system restored after a failure?

COUNTERING SECURITY AND CONTROL THREATS
Developing countermeasures to security threats can be a daunting task if attempted without a well-thought-out methodology. The initial phase is to begin developing a network security plan. According to the Gartner Group, several issues must be addressed in developing such a plan. The most important issue is to establish a policy that is endorsed by upper management and draws from security experts, CIS auditors, network managers, business-unit managers, and users from across the enterprise.

A security policy should address methods of achieving the following goals:
• Confidentiality: making information available only to authorized entities and ensuring the privacy of communications.
• Authentication: determining whether information is genuine (whether the source and destination entities are what they claim to be).
• Access control: permitting or denying access based on a variety of parameters. These include the identity of the source and destination, and the nature of the business relationship if the potential users are outside parties.
• Data integrity: ensuring that data is accurate.
• Nonrepudiation: providing proof of transmission and receipt.

A complete security policy also contains provisions for ongoing updating, such as the indoctrination of security awareness among all users and the establishment of standards and procedures for security training.

In addition to a strong security plan, an organization must look at its particular environment and technology to develop specific approaches for countering possible security threats inherent within that technology. In the following sections, general principles to address a typical Novell network environment are reviewed. This illustration reflects the current majority of microcomputer-based networks in North America and in many parts of the world. The general principles and audit, security, and control steps outlined are transferable to all network environments.

**APPLYING METHODOLOGIES IN A NOVELL ENVIRONMENT**

In securing a network, specifically a Novell network, different models of security can be identified to meet the various levels of maintenance costs and security requirements appropriate to a particular organization. Five such models are presented in the sections that follow; each subsequent model builds on and enhances the level of security of the preceding model. Again, the resources to perform such functions can come from consulting services, security staff, and CIS auditors.

**The Simple Model (Minimum Security)**

The simple model comprises the following steps:

• Buy an antivirus package for the network that can be auto loaded in the login script.
• Give every user a log-in script.
• Always install network application software to specification.
• Place the server in a safe area (where it will not be tampered with inadvertently, bumped, or otherwise interfered with).
• Choose a password for ADMIN that is not common or easily discernible by anyone. Require that end users do the same with their own passwords.
• Place the server and backup device in a secure area. Keep the backup devices and backup software in a secured location apart from the server.
• Make regular backups.
• Restore the first backup to another directory as a test just after it is made.
• Move backups and a copy of backup software off site on a regularly scheduled basis.
• Lock the file server console from within the MONITOR.NLM.
• Do not store the file server console password in the AUTOEXEC.NCF file.
• Set up some form of education about computer security.

Basic Model
The basic model includes the simple model and the following additional steps:

• Educate the organization about passwords and computer viruses.
• Require users to log out and lock up stations not in use.
• Test the backup process by creating a directory, filling it with nonessential data files, backing up the files, deleting them, and restoring them from the backup device.
• Maintain a second archive of all data and applications off site for disaster recovery.
• Learn and understand the file system directory and file attributes.
• Install software in its own directory.
• Remove DOS from the server by typing REMOVE DOS at the console.
• Ensure that the console password is different from the ADMIN's password.

The Protected Model
The protected model comprises the basic model and the following steps:

• Implement proper security education.
• Implement a premise key distribution system.
• Require passwords for print servers.
• Make sure all users exit from the system log-in script or use their own personal log-in scripts (an empty log-in script is better than no log-in script).
• Limit the number of concurrent connections.
• Provide the system administrator with the capabilities and security equivalencies of the ADMIN user object and then delete the user ADMIN.
• Check access control list (ACL) rights in NDS for all users other than ADMIN.
• User accounts of terminated employees or otherwise unused accounts should be disabled or deleted.
• Keep a list of detailed accounts, users, and other pertinent information for use when restoring backups.
• Use only Novell-certified and tested NLMs.
• Enable intruder detection.
• Enable the SECURE CONSOLE feature on the server to restrict the loading of NLMs.
• Disable all remote console capabilities or assign RCONSOLE a unique password.
• Set network time restrictions.
• Remove write and create rights for the MAIL directory from the [Public] trustee.
• Use a network analyzer to produce a list of clear-text passwords.
• Train users to log out whenever they leave their computer, or provide some kind of automatic locking utility for everyone’s computer.
• Require regular password changes for all accounts.
• Do not allow reuse of a password.
• Verify size for installed executables with the manufacturer. Check them periodically to ensure they have not changed size.

Audited Model
The audited model builds on the protected model. It includes the following additional steps:

• Have the network audited regularly by CIS auditors.
• Monitor access to the server room, cable, and workstations.
• Monitor executable files.
• Provide security training for end users and administrators with annual refreshers.

Secured Model
The secured model is the most secure. Its high level of security is derived from the audited model and the following steps:

• Remove disk drives from workstations when not in use.
• Restrict physical station addresses.
• Ensure that only trusted users have workstation access.
• Eliminate untrusted user accounts from trusted networks.
• Secure all workstations.
• Institute trusted-connectivity components in the network.
These models review the main areas of security in a local area network (LAN) or a zone within a wide area network (WAN). Additional issues must be considered when dealing with outside access to the network through the Internet, intranet, extranet, E-mail, or telephony. These include confidentiality, authentication, access control, data integrity, and nonrepudiation.

Access control continues to be the serious concern among organizations using telecommunications to connect their networks across geographically diverse operations. The point of a distributed environment is to facilitate the transfer of information between systems; however, things get complicated when connecting to systems outside the organization. The challenge is to restrict access to hackers and viruses without degrading the overall performance of the network for those authorized to use it.

**FIREWALLS**

Firewalls are becoming the method of choice for organizations determined to maintain security from outside intruders. A firewall is a compilation of hardware and software components designed to work together in maintaining security of an internal network from attacks from outside. Their use and implementation varies, but the principle by which they are designed is to place a gateway between the internal network and the outside world.

The firewall can restrict traffic that is not explicitly permitted, or allow traffic that is not explicitly blocked. For maximum safety, the first option is more secure because it allows services to be enabled on a case-by-case basis after a careful assessment of need and risk. Furthermore, the network administrator knows what accesses are permitted.

Firewall vendors such as Raptor describe five domains of network security:

1. Internet security
2. Workgroup security
3. Mobile PC security
4. Remote site security
5. Integrated enterprise security

CIS auditors and IS security personnel can play a key role in monitoring the integrity of the firewall and ensuring operational and security compliance. Each of these domains has specific requirements, but common elements among firewall installations include suspicious activity monitoring, encryption, multiple authentication options, proxy software to foil spoofing attacks, real-time alarms to catch hackers in the act, tools to secure remote data communications, and network management tools.
SECURITY TOOLS
As security risk exposures have increased in distributed environments, so have tools to monitor and correct them. Diagnostic tools can be used to assist an organization in identifying specific security weaknesses within its distributed environments. One example is the Security Administrator Tool for Analyzing Networks (SATAN). This is a public domain software security tool released through the Internet. This tool has many administrators concerned about its availability to potential hackers, but it can be more of an aid if used before a hacker attempts to attack a distributed environment.

SATAN gathers information about Internet-connected hosts and detects the presence of Unix services such as remote log-in and file transfer. The program then outlines the ways in which these services can be misused, and identifies other security flaws such as bugs in system or network utilities. It also identifies poorly configured systems that lack passwords or other basic precautions, and unauthorized activities by inside users such as opening unprotected Internet connections. SATAN then displays information about the nature and seriousness of the flaws it finds and offers suggestions on how to correct them.

From a management standpoint, vulnerabilities identified by SATAN should not be tolerated. They are normally elementary weaknesses that any competent hacker can circumvent. A network that is vulnerable to SATAN is not protected from the most casual intrusion.

CURRENT ISSUES AFFECTING SECURITY
As technology continues to become more pervasive, and end users become more sophisticated, internal and external security risks will likely increase. End users are able to navigate and access databases as never before. Available technologies becoming industry standards include Windows 95, open database connectivity (ODBC), object linking and embedding (OLE), client/server technology, and other desktop technologies. The challenges to organizations attempting to implement network security are becoming even greater than they have been in the past.

Many security experts are suggesting that distributed environments are becoming virtually impossible to fully secure. Network security has become a dynamic process as new technologies allow the breach of existing security measures. The use of CIS audit and CIS security expertise can help monitor the quality of security and control within the distributed environment and aid IS executives in determining the relative importance of the necessary adjustments, modifications, and improvements needed for planned strategic systems of the future.

CONCLUSION
Though the challenges of securing a network are becoming greater than ever, it is not too late to begin formalizing a plan to secure an organiza-
tion’s current environment. CIS auditors and security consultants and staff can play key roles in helping managers maintain a secure and controlled environment. By developing a network security policy that becomes the framework for a proactive plan, IS executives and managers can integrate the skills and resources of audit and security personnel in maintaining the plan. Vendors, such as Novell, are working with clients and security professionals to develop new and improved tools to assist in securing networks developed with their products.

Network security administrators and CIS auditors are using tools such as SATAN in their fight against common security infiltration by hackers and others. The Internet is providing a tremendous medium for those researching issues specific to their circumstances. It is also allowing professionals to share information with each other on reducing and eliminating security risks within their network environments.

Network security can be approached by following the guidelines outlined in this article. Once a network has reached a certain level of security, managers must continue looking for ways to keep up with other potential security risk exposures. Network security is a dynamic process with continuous opportunities for its improvement.

Notes
3. Novell Application Notes — Special Edition — Building and Auditing a Trusted Network Environment with Netware 4 — Figure 3.1 p. 48.

Frederick Gallegos, CISA, CGFM, CDE, is an adjunct professor and the MSBA-information systems audit advisor for the Computer Information Systems Department, College of Business Administration, California State Polytechnic University, Pomona, CA. He has more than 25 years of experience in the IS audit, control, and security field as both an educator and writer.

Stephen Tanner is president of Argus Consulting in Arcadia, CA, and has worked in the IS consulting field for 10 years, specializing in network design and development issues.