BY EVERETT WOODARD

Network Security: Policies & Procedures

Since the majority of hacker attacks occur within an organization, it is critical for company personnel to have a code by which to abide while performing their daily tasks via the network. Before developing code hacks and different methods to find network vulnerabilities, review your company's Network Policies and Procedures manual to determine your best defense. This article provides a "short course" on what should comprise this manual.

"IT'S 10 p.m. Do you know where your network is?" plays off an old question intended to ensure that children were safe and not getting into any mischief. In today's world of Internet, intranet, extranet and e-commerce, CIOs, MIS managers and front-line engineers are asking that same question regarding the security of their networks.

Almost daily, newspaper and nightly news reports tell the public about a network, whether government or commercial, that experienced a "hack attack" or a "Denial of Service" (DoS). Can you guess who the culprit is in these attacks? Chances are it is not the NASA rocket scientist sitting behind a supercomputer with nothing better to do than spend our tax dollars on a little excitement. More than likely it is the 15-year-old next door with less than $5,000 in hardware and software who gets his kicks by exploiting networks and bragging to his peers about how easy it is to get into XYZ Company's network.

Nevertheless, how does one defend a network against an invisible enemy? Consult your *Network Policies and Procedures* manual first before you develop code hacks, port scanning, war dialing, different methods to perform network penetration and different methods to find network vulnerabilities. Although news media typically focus on attacks from outside a company's network, 75 to 80 percent of all network attacks occur within an organization. Therefore, it is critical for company personnel to have a code by which to abide while performing their daily tasks via the network.

POLICIES AND PROCEDURES

Policies and procedures in network security are integral to how the network will operate, as well as how the people who are using it should function, and should answer such questions as:

- What is the structure of passwords and how often should passwords be changed?
- What type of accounts and access are set up on the network?
- Who has which levels of security and authority?
- What actions are to be taken when there is a breach against policy and procedures?

Policies and procedures in network security are integral to how the network will operate, as well as how the people who are using it should function.

Yet, this issue is one that most would prefer to avoid. Even mentioning security policies during a meeting will virtually ensure that the one raising the issue will have to write or upgrade the policies and procedures. Countless companies have nothing formalized in hard copy or electronically, only in their minds. Other companies have volumes of policies and procedures resembling a law library. Given that wide variance, the key to successful policies and procedures on network security is that the corporate culture must change. Having rules and regulations in writing isn't of much use if personnel do not know where the manual is located and/or the guidelines are not followed or enforced. Furthermore, if these policies and procedures aren't enforced it is a futile effort on the part of the person charged with periodically reviewing and updating the regulations.

For an in-depth examination of network security policies and procedures, many excellent books and consultants address the topic very well. However, a "short course" may be useful, beginning with an overview:

1. Network policies and procedures should be treated as a living document and updated often (ideally not less frequently than quarterly).
2. Clearly define within non-technical jargon, as much as possible, the policies and procedures that the masses must adhere to; in other words, don't scare the non-technical audience.
3. Keep all policies and procedures readily available. Some individuals will need access to the entire document, while others will only need access to various components (an intranet works very well for this distribution purpose).

A sample template is available for download from the NaSPA web site as filename WOOD1100.DOC or by emailing your request to editor@naspa.com. To access this template from the website (www.naspa.com), click on "Technical Support" and then on "Coding Samples from Articles." This template is designed to jump-start the process of determining what should be included in a network policies and procedures manual. This is not intended as a fill-in-the-blanks-and-I'm-done worksheet, but rather it is designed to help those without policies and procedures and/or those with very "loosely" written policies to tighten them up.

Note: When reviewing the template please note that text in red italics indicates where information would be inserted. It may be helpful to refer to that that document while reading this article.

INTRODUCTION

The main charter of a policies and procedures document is to provide the typical user a set of guidelines for performing their daily tasks while connected to the network. Not intended to deliver an in-depth look at every event behind the scenes, the design provides users with an understanding of what is expected of them to remain good citizens of the network as well as shows them where to seek help.

FIGURE 1: CONTACT TABLE

Title	Name	Address or Location	Office Telephone & Ext.	Pager	Email	Home # (Optional)	Cell Phone
Building Maintenance							
Building Premises Security							
Database Administrator							
Desktop Services							
Firewall Administrator							
Fire Department							
Local FBI Computer Fraud Investigation Division							
Local Law Enforcement							
MIS Help Desk							
MIS Manager							
Network Administrator							
Network Security Administrator							
Network Security Director							
Network Services							
Novell Administrator							
NT Administrator							
Unix Administrator							
Other Special Contacts							
(Continue listing any special individuals, departments, vendors, agencies, etc. that may provide special services in the event that they should be notified.)							

Acting as the governing body of the network, the majority of MIS departments decide on which policies (rules) will be adhered to and how to enforce these policies. Too many times, there only lies an expectation between the MIS Department and the network user. Both develop expectations about the other, but neither is very certain about what they expect or how to go about obtaining it.

Consequently, policies and procedures help alleviate some of the empty expectations while providing a path to follow in determining what each one can expect from the other. That is where the introductory part of the document comes into play. It should clearly state its intent and what can be expected throughout the document.

CONTACT INFORMATION

Next, individuals and groups that provide service to the network should be listed with their contact information in an easy-to-read table format. All contacts from A to Z that would provide needed services during network problems should be listed. The table in Figure 1 lists some of the more prominent contacts' titles that would typically be included. Each company's structure will dictate whether more or fewer contacts should be part of this representative table.

USER ACCOUNTS AND PASSWORDS

Different types of user accounts and the party responsible for those accounts should be listed. It is also necessary to include information on how one goes about obtaining an account or how to determine an account's status.

The section on passwords includes varied opinions as to how a password should be construed. In this particular reference document is what is generally agreed upon by most network professionals as a common approach to creating passwords. Bear in mind that passwords are one of the key elements in network security and should not be taken lightly. Therefore, it is good practice to force password changes periodically as most users will keep the same password if possible since it is one less piece of information to recall.

It is often helpful to let users change their own passwords and to rotate passwords. Passwords should be rotated at least four to five times before allowing the same password to appear again. Again, some companies may not allow this flexibility if security is of the utmost concern, as in some financial institutions.

USER REQUESTS

Periodically, users may make requests to the MIS Department for a new user account, group membership, or group access to certain files or areas. Providing information on how to fulfill this special request makes it easier for users to proceed through the proper channels in obtaining their request rather than going through the "old buddy" system. Having someone grant requests on the fly, without any record of a request, is not an appropriate procedure.

In contrast, maintaining accountability for everything that takes place in the network

assures the network administrator that all will operate as smoothly as possible.

ACCESS TO NETWORK RESOURCES

This section addresses where the user is allowed to go not only physically, but also electronically. Included are the physical access certain individuals have to certain areas of the network and where those locations are. Also significant are the following points:

- how a user is connected to the network via certain devices, most commonly PC-based workstations
- how that connectivity is made, whether via Internet or remote access

A section that should be added to most network security manuals would focus on discouraging users from adding devices to the network. In a network management environment, when a user takes it upon himself to add a device to the network, the result is usually a disaster waiting to happen.

RIGHTS AND RESPONSIBILITIES

In this section, the use and expectations of the user of software, file storage, printers and email should be listed. Examples shown represent only a small listing of what can actually be grouped under each of these topics, since each network will dictate what will be necessary to convey the message that end users should preferably receive.

ABUSE OF NETWORK RESOURCES

The "Abuse" section should list what potential disasters users can wreak on a network and anticipated consequences. Take special heed to the section listed under "Electronic Mail and Communications." There may be special laws in your state that govern certain nuances of electronic communication. The link http://cyber.findlaw.com/privacy/workplace.html takes users to a site that details the Electronic Communications Privacy Act, which examines what constitutes invasion of privacy concerning electronic communications such as email.

SYSTEM ADMINISTRATOR'S RESPONSIBILITIES

This section lends itself to describing the roles and responsibilities of the personnel or groups of personnel who are in charge of the network. This is useful in that it can help direct a user to a point of contact instead of them aimlessly wandering around lost and frustrated. Any individual or groups that are listed here should definitely be listed in the contact table.

The main charter of a policies and procedures document is to provide the typical user a set of guidelines for performing their daily tasks while connected to the network.

ENFORCEMENT

This section describes what happens to users when they have not abided by the policies and procedures that were stated in the previous sections. Therefore, it may be especially helpful to include information specific to your company on how it will work with law enforcement when an individual has allegedly committed certain crimes.

"Law enforcement" is not included in this section because a considerable number of companies prefer to keep legal problems/matters in-house until being reasonably certain they must seek official law enforcement involvement. "Think lawsuit" if an employee is wrongfully accused before the company conducts a full investigation.

REPORTING PROBLEMS

Ideally, this section would not be necessary. However, networks, computers and users can be a volatile combination. So why not list all the avenues that a user can call upon in a time of need? By effectively using this section, companies can considerably reduce end-user aggravation and negative use of the help desk as a complaint department.

APPENDICES

The Appendices section should include any specialized request forms employed in conducting a smooth network operation. Note also that by using an intranet for this document, links can be added to these forms and stored in one location. When updates are complete, companies have the assurance that users of the forms have filled out the latest request version.

CONCLUSION

Most would readily agree that creating a network policies and procedures manual is not the most exciting aspect of one's job, but it plays a critical role in helping to ensure that the network operates as efficiently and securely as possible.

Everett Woodard works for Kent Datacomm, which develops total "end-to-end solutions" for integrated voice, video and data networks as a division of Houston-based Kent Electronics Corporation. Everett can be contacted via email at ewoodard@kentelec.com.