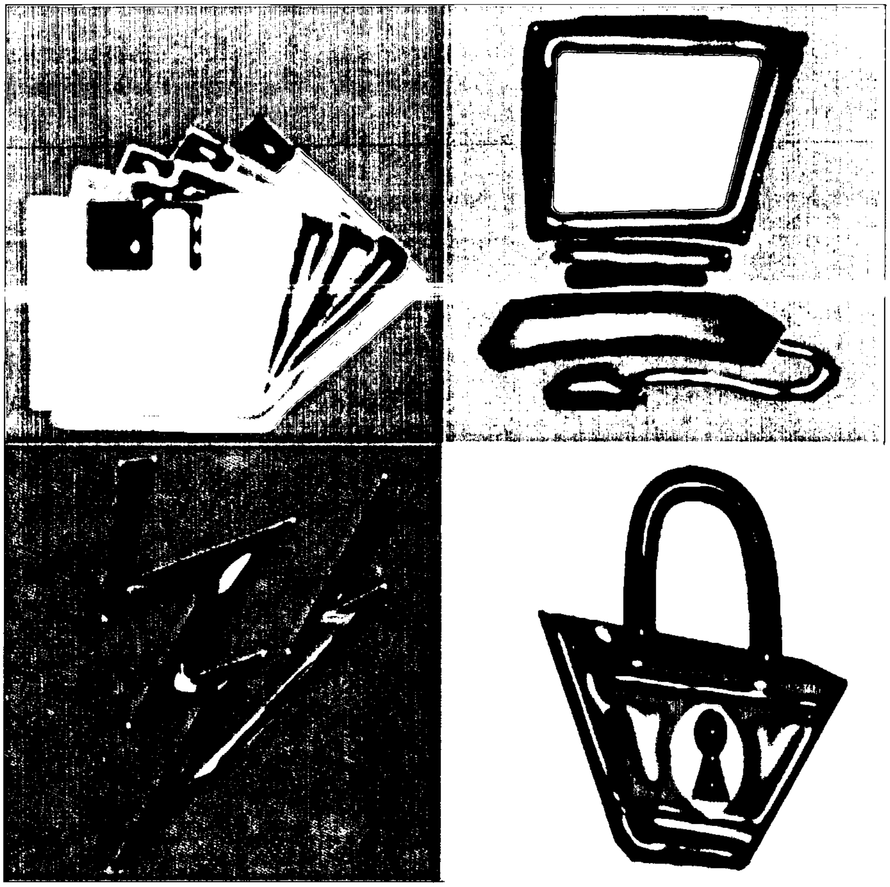
ED 475 309 IR 058 657

AUTHOR	Williams, Robert L.
TITLE	Computer and Network Security in Small Libraries: A Guide for Planning.
INSTITUTION	Texas State Library and Archives Commission, Austin.
PUB DATE	2001-00-00
NOTE	150p.; Published by the Library Development Division.
AVAILABLE FROM	For full text: http://www.tsl.state.tx.us/ld/pubs/compsecurity/.
PUB TYPE	Guides - Non-Classroom (055)
EDRS PRICE	EDRS Price MF01/PC07 Plus Postage.
DESCRIPTORS	*Computer Networks; *Computer Security; Libraries; Library Administration; *Library Equipment; *Library Planning; Library Policy; *Library Technical Processes
IDENTIFIERS	*Library Security; *Small Libraries

ABSTRACT

This manual is intended to provide a free resource on essential network security concepts for non-technical managers of small libraries. Managers of other small nonprofit or community organizations will also benefit from it. An introduction defines network security; outlines three goals of network security; discusses why a library should be concerned with network security; and describes limits of this work. The manual is divided into three main parts. Part One features the management issues related to network security: analyzing risk, developing a security plan and policy, the funding requirements libraries can expect in operating their networks, and implementing adequate security. Part Two describes the areas of computer networks that need to be secured, and provides a description of many of the security measures necessary for adequate security. Part Three presents sample documents that may be help in the library's efforts to secure its network A glossary and bibliography are also provided. (AEF)



Computer and Network Security in Small Libraries

by

Robert L. Williams

Texas State Library and Archives Commission + Library Development Division + 2001

Computer and Network Security in Small Libraries

A Guide for Planning

Robert L. Williams

Published by the
Texas State Library and Archives Commission, Library Development Division
Austin, Texas
2001

**TEXAS STATE LIBRARY AND ARCHIVES COMMISSION
CATALOGING IN PUBLICATION DATA**

Williams, Robert L.
Computer and network security in small libraries : a guide for planning / Robert L. Williams. – Austin, Tex. : Texas State Library and Archives Commission, Library Development Division, 2001.
xii, 151 p. : ill. ; 28 cm.
Includes bibliographical references (p. 145-151).

1.Computer security. 2. Computer networks—Security measures. 3. Internet—Security measures. I. Texas State Library and Archives Commission. Library Development Division. II. Title.

005.8 W675c

Computer and Network Security In Small Libraries

This guide is dedicated to the staff of public libraries everywhere

who have done so much

with so little

for so long —

and yet stay on to keep the fire of imagination

burning inside us all

Table of Contents

Part I. Managing Network Security

Part II. Implementing Network Security

Part III. Auxiliary Documents

A

Acknowledgements

This guide is an outgrowth of an e-mail conversation begun on the Texas Automation Consultants mailing list (tx-autocon) last year. As we discussed content, format, and training styles, we learned there were a lot of different desires for library training related to network security. While I don't think this product fits the entirety of what any one of us had in mind, I do believe it represents something from each of us. I hope it serves everyone well. For working through that discussion, I owe a debt to:

- Bob Gaines, Automation Specialist with the Central Texas Library System;
- Jerry McCulley, Library Technology Consultant with the Northeast Texas Library System;
- Grete Pasch, then the Technology Consultant with the Texas State Library and Archives Commission
- Christine Peterson, Library Liaison Officer with Amigos Library Services;
- Beth Salas, Automation/Technology Consultant with the South Texas Library System

I'd also like to thank Kelley Argenta, TANG Supervisor for the Alamo Area Library System, for her comments on the draft; Belinda Boon, Manager of Continuing Education at TSLAC, both for her comments during the e-mail discussion and for working with me through the paperwork process; Marilyn Johnson for her assistance in editing the manuscript; and the various staff at TSLAC for all the behind-the-scenes work it takes to get a manuscript edited and published.

Also, I'd like to say a big thanks to Nancy, Nic, and Tessa, who give me reason to write. They have to endure the technospeak while I'm writing!

And, finally, a simple thanks to the One who sees beyond my seeing.

Preface

Security.

It's such a cozy, comfy kind of word. One would think that it's something you either have or don't have, but just like the rainbow after a spring shower, it's elusive. Try to find the pot of gold at the end and you will find yourself traveling for ages because there seems to be no end to our search for the end of the rainbow and the treasures it holds. It's the same with computer and network security. As we use the word in this guide, security is non-attainable. Thomas Wadlow writes in his book *The Process of Security*, "Security is a direction you can travel in, but you'll never actually arrive at the destination. What you can do... is [manage] your level of acceptable risk."[1]

"So why spend our time on it?" one might ask. Isn't that the real question? Why spend time on an ideal that can't be achieved?

The possible effects of a security breach are loss of data, loss of services, loss of time, or loss of face and goodwill. In public libraries and other small community organizations, our time is especially precious, where we already have 800 other things we need to be doing. We can't afford the time it takes to recreate data (if it's even possible to be recreated) nor to get our systems cleaned up and operational again. For us security is the process of achieving a balance among our time, the risk associated with loss of our data or service, and the cost of implementing and maintaining adequate security.

Therefore, this is the direction in which we'll go once you turn the next few pages. We must identify the major areas of security, possible threats to resources, and the cost of securing systems.

[1] Thomas Wadlow. *The Process of Network Security*. Addison-Wesley, 2000. p. 4.

Who is This Manual For?

When you wade into the waters of network security, you will not be wading into a tranquil pond to feed the duckies. One step into these waters and you are immersed in a whitewater rush of jargon, alerts, technical descriptions, and long, maybe incomprehensible, documents. The challenge is simply to stay afloat. For someone new to the topic, it's rough water indeed.

This manual is intended to provide a softer entry into the world of network security for non-technical managers of small libraries. Managers of other small non-profit or community organizations will also benefit from it. It's a beginner's introduction.

We hope to teach you some basic principles to help you keep your kayak afloat and get to your campsite somewhere down river, a place where you will be ready to work with a vendor to discuss, plan, and implement your library's specific security strategy.

Need

For the organization that uses network-based access to the Internet, network security is no longer an optional component of its technological infrastructure. Access has become an integral part of the business structure. Doing without Internet access for a long period of time will negatively impact services offered and normal business practice. So securing access against loss is imperative. We hope to show you why in the following pages.

Because few administrators of small libraries have technical support staff available, many are forced to learn at least the major facets of network security so that they can hire an outside entity to implement and maintain security for them. **The goal of this manual is to provide a free resource where a non-technical person can go to learn essential security concepts without adding further to the burden already placed on what training funds the organization may have available.**

For some of you, hiring an outside consultant or vendor will also not be an option. So I couldn't just leave this as a conceptual guide. For those who are interested, a companion online training module is being developed as well. The training module will help tech volunteers—or staff if the library is fortunate to have technically proficient employees—learn many of the primary procedures required in securing a Windows NT network and in working with general perimeter network equipment (routers, firewalls, and proxy servers). For more information about course availability, go to the address below:

http://www.classhost.com/classhost/netsec/training.html

A web-based version of this guide is available on the training site, with appropriate links to step-by-step tutorials, allowing the user to configure her/his organization's network servers, workstations, and other network equipment more safely. A virtual classroom component allows the user to participate in real-time class sessions using chat and whiteboard software, providing a forum to discuss problems, ask questions, and clarify understanding of security topics, just as one would in an in-person seminar.

Disclaimer

The subject of network security is complex. This guide seeks to provide basic information about network security, but the information contained herein is not intended to take the place of consultation with a security professional prior to the implementation of security measures within an organization. There are many variables regarding network connectivity, and proper security configuration is incumbent on many of them.

Therefore, to minimize the risk of breaches, data loss, or other mischief or damage, we caution the reader to use the material to become familiar with concepts related to network security in order to contract with a security practitioner to plan the best security implementation possible.

I hope you find the guide helpful in your quest to understand network security. After you've read or looked through the guide, do feel free to send comments and suggestions by e-mail to *nscomments@rlwconsulting.com*, or go to the following web page to fill out an electronic evaluation: http://www.rlwconsulting.com/netsec/eval.html

1

Introduction

A lone light shines across his right shoulder, lighting the notepad on the right side of the desk. In the penumbra falling across his face the phosphorescence from the monitor before him makes his eyes glow with an almost sea-blue quality. The eyes are intense, small squint lines forming at the corners as he focuses, watching the progress of the download. Upon its completion his fingers flick from mouse to keyboard.

He is filling his toolbox, printing out documentation, learning the trade that will take him on an adventure, hopefully behind the walls of protection the government and corporations are beginning to erect.

With his hacking toolkit downloading, he sits silently, watching.

This scene plays out in many of our minds as a stereotype of today's "hacker." Many of us see the danger as being "out there." Someone on the Internet may break into our network and do something malicious. Large businesses spend a lot of time and energy in protecting their networks from these external threats. Why would a hacker be interested in breaking into a library network?

As we begin to peel away the stereotypical images associated with network security, we are all learning that the total threat to our systems and network resources isn't quite this simple, not so easily defined. First we learn that it's not just external threats that are a problem. Many times the threats are *local*, inside our buildings. Then we learn that it's not the devastating things that are the biggest threats—it's those annoying little things patrons do that consume what little time, and sometimes funds, we have for managing the computers through which we offer services. We're also learning, as we put up web servers on the Internet, that there really could be a threat from Internet-based attackers. It's not rocket science to obtain and use tools that can devastate our servers and our workstations as well.

With the proliferation of funding for computers and Internet access the past two years, it has been terribly easy to walk into a quagmire of issues we didn't know existed. Now we find ourselves having to put on yet another hat, learning the basics of another responsibility we must take on: network security. What is it? How do we get it done? What impact will it have on our daily operations? Over the next hundred pages or so we will address these questions, but let's begin here with the first one: what is it?

What is Network Security?

Network security is the process of configuring network hardware, computers, software, and the physical environment to minimize the risk of attack to these resources. Or, more simply put, network security is protecting your equipment and software so people aren't likely to do bad things with or to them. Or at least reduce the chance that they'll do these things. The key idea here is that network security is a *process*.

(Did this just wash right over you? It's easy to assume that a reader already knows the basics about what a *network* is, but many may not. If you're totally new to this topic, you might find a basic discussion of networking helpful. To learn more, there are lots of tutorials available on the Internet. You can also find a basic discussion in a previous manual the Texas State Library published. See Part Two of the *Wireless Community Networks*[2] beginning in Chapter 6, available online at http://www.tsl.state.tx.us/ld/pubs/wireless/chapter6.html .)

The practices that make up good network security evolve over time as vulnerabilities in network operating systems, network hardware, and software are discovered. *Vulnerabilities* are weaknesses in network configurations that can be exploited (taken advantage of) to gain unauthorized access to network resources. These are most often discovered through experimentation, either by those who want to break into networks or by those charged

[2] Robert Williams. *Wireless Community Networks: A Guide for Library Boards, Educators, and Community Leaders*. Texas State Library and Archives Commission: Austin, Texas, 1999. pp. 63-72.

with securing them. This experimentation normally involves using software in a way it was not designed to be used.

The "bad guys" and security experts push the boundaries of programmers' expectations of use to see if a system responds in ways that are advantageous to malicious users. Such *cracking* attempts may originate just as easily on local workstations as from the Internet. Some patrons may use public workstations in a way you would never dream of (as an anonymous way to break into other Internet-based computers, for example).

Because those on both sides of the security fence keep trying new methods, new vulnerabilities continue to surface. The notion that network security is implemented once and taken care of forever is a misconception. Making a network 100% secure is also a misconception; absolute security simply cannot be achieved. So, the process of network security is about minimizing, rather than eliminating, the risk of misuse of one's network resources.

The Three Goals of Network Security

As you become familiar with network security, you will see three theoretical goals commonly presented: availability, confidentiality, and integrity. These form the foundation for effective use of shared resources.

- *Availability* — the whole purpose of a computer network is to share limited resources in a convenient way. Resources, as we define the term later, may include equipment, software, or data. In small public libraries, the most commonly shared items are an Internet connection and a printer. If something blocks or interferes with a user's access to one of these resources, it renders the resource unavailable and therefore unusable. To justify the expense of creating a network, its resources must remain available.
- *Confidentiality* — shared resources have a theoretical problem, though. If I store my data "on the network," what's to prevent someone else from accessing it? If data packets are transmitted across a shared network medium, what's to keep someone else from seeing what's in them? Few of us would use shared resources if we believed someone else could read or view all the information we transmitted or stored. So keeping data confidential is a foundational requirement of network services.

- *Integrity* — not only is confidentiality important, but we must also be able to trust the data stored on a network. Thinking about a teacher's electronic records, what would be the impact on network use for the project if we believed data stored online could easily be altered? Most of us would find another method of storing data. In order to make network use practical, we must provide a reasonable guarantee that data stored or transmitted on the network will remain in its intended form.

In order to accomplish these goals, a solid program of network security will seek to accomplish the following tasks:

- analyze the risks associated with threats to network resources
- determine which risks are most likely to occur
- apply current practice in protecting against these risks
- review security alerts and bulletins regularly for the emergence of new vulnerabilities and repeat the process

Why Should a Library be Concerned with Network Security?

Securing the library's computer network means the library will spend less time reconfiguring workstation settings, recovering from the mischief patrons may do, and responding to system and server problems resulting from unauthorized use of systems. Network security will also provide a defense against accidental or malicious deletion or alteration of data residing on network servers.

Properly implemented, network security will also reduce the risk of attackers (from both the Internet *and* the internal network) breaking into library systems and either rendering various systems unusable or just creating a nest from which to launch attacks on other systems across the Internet. In other words, implementing adequate network security measures provides the benefit of *minimizing* the following:

- the potential for *loss of data*.
- the *staff time required* to manage local workstations and servers.
- the *funding required* to maintain networked services.

- the *potential for embarrassment* from the effects of break-ins.

Limits of This Work

Network security, because it involves many aspects of both computer and network operation, is an extremely wide subject. In order to pare down the material to be covered, I make the following assumptions about your network:

- Someone other than staff (a vendor, consultant, or volunteer) will be doing the actual installation, configuration, and maintenance of the library network.
- The library uses Microsoft Windows NT/2000 Server for its server operating system.
- The library uses Microsoft Windows NT Workstation/2000 Professional or Windows 9x for its workstation operating system.

Other operating systems may be used in some libraries (e.g., Novell Netware for an automation server, Linux for servers or workstations, MacOS for workstations). However, Windows NT/2000 is currently the most common server and workstation operating system used in small Texas public libraries, due to the influence of Gates Foundation grants and the ease-of-use of the Explorer interface shared with the Windows 9x desktop operating systems. So, for the remainder of the manual, we will focus on Windows NT/2000 Server (for servers) and Windows 9x or Windows NT Workstation/2000 Professional (for workstations).

Content

This manual is divided into three distinct parts:

- *Part One*: features the management issues related to network security: analyzing risk, developing a security plan and policy, the funding requirements libraries can expect in operating their networks, and implementing adequate security

- *Part Two*: describes the areas of computer networks that need to be secured, and provides a description of many of the security measures necessary for adequate security
- *Part Three*: presents sample documents that may be helpful in your library's work in securing its network.

Part

I

Managing Network Security

1

Defining Risk

Mrs. Winkle stared at the e-mail message in disbelief.

"We have traced the source of a denial-of-service attack against our Internet connection to several dozen hosts on the Internet. Two are part of your network. We would appreciate your assistance in removing this source of attack against our resources.

"Please scan the two workstations (IP addresses listed below) for viruses and have the offending software removed. Also, have your firewall configuration updated to minimize the possibility of similar attacks occurring in the future."

It was signed by the Security Manager of a company in Ohio she'd never heard of.

"Oh, my," she murmured. "I'd better call Tony."

She picked up the phone and pressed speed-dial 8 as they had decided in the response plan.

The process of securing your library network begins with realizing what the library stands to lose if security is not pursued. Network security is not just "another thing to do." Its importance lies in protecting the library's network resources.

Network resources? What does *this* conjure up in your mind? Maybe we need to start at the beginning.

In this chapter I hope to accomplish three things:

- define some of the concepts involved in the world of network security
- provide you with an understanding of the "treasure" present in your library's network
- help you see the possible dangers to this treasure

In the next chapter I will suggest a strategy you can use in beginning to defend your library's treasure. For now, let's proceed to some definitions and some basic questions about security. Are you ready?

Definitions

Listed below are eight terms I will use throughout the remainder of the manual. Learn them well, be able to use them in the correct context, and everyone will begin to think you're a security expert!

Network Resources — the equipment, software, and data that make up a networking system, including the user data that is shared over the network. In terms of network communication, this includes the servers, workstations, hubs, switches, routers, firewalls, and telecommunications links that make up a network. In terms of usage, this includes shared printers, database systems, shared software, user accounts, the shared or user-specific files stored on a central server, and the keystrokes and form information that travels across the network.

Backup — a term I use throughout this manual in a general sense to mean any preferred method of making a copy of the software and data installed on a computer's hard drive. Along with traditional backup hardware and software, many entities now use "ghosting" software to make image copies of a hard drive's contents.

Attacker — a person (or inanimate force, such as a fire, torrential rain, or thunderstorm) willfully seeking to access in an unauthorized manner, damage, alter, corrupt, misuse, steal, or otherwise deny access to any network resource. Likewise, an *attack* is an event during which a network resource is accessed for any of these purposes.

Weakness — a characteristic of hardware or software (especially of an operating system) making a network resource susceptible to attack.

Vulnerability — an unprotected weakness by which an attacker can attack a network resource.

Exploit — (use, take advantage of) a process or procedure by which an attack is launched.

Intrusion, Infiltration — a successful break-in, where a user breaks through the security implementation and gains unauthorized access to network resources. Likewise, an *intruder* is someone who has gained unauthorized access to network resources.

Threat — an avenue by which a vulnerability can be exploited to attack a network resource (e.g., a flood or a lightning strike is a physical threat to network resources—a local user or an Internet "hacker" is a personal threat)

Risk — the likelihood that a particular vulnerability will be exploited.

These are all terms commonly used in documents and conversations related to security. But they don't cover the full range of events that might occur in a library, or any other business environment. What do you call it when a patron out of curiosity looks around a workstation's web browser files to see what he can discover about previous users' Internet use, or when someone installs personal software on a public workstation? What is it called when a patron changes the desktop wallpaper to something *he* likes better? Are these really *attackers*?

This sounds a little strong, doesn't it? So I've coined a different term: *mischievous user*. Nevertheless, even though their actions may be mischievous rather than malicious, the effect may be the same: loss of staff time because of the maintenance required to restore the system, or even the loss of a service itself for a period of time.

Why Would Anyone "Attack" a Library?

If we rule out that casual mischief we have all seen to some extent, are there really people who would try to break in to the library network? Maybe not in every community, but many communities will experience such break-ins. Before we discuss users in your local community, though, let's look at the people on the Internet who work in security circles, either as attackers or as defenders. The likelihood of these guys breaking into your system is a lot less than someone messing with your network locally. On the other hand, local attackers may get their knowledge from these.

Black Hats

If you've see "westerns," you already know these guys. They are the bad guys who learn the various ways to steal, mutilate, or view your information resources. They come with all types of personalities and levels of experience:

- the "hacker" (really more appropriately called a "cracker") who searches across the Internet for likely targets and then begins the process of breaking in.

  These guys get the publicity, but they're hardly the most common threat to networked resources. True crackers write software that enables them to take advantage of vulnerabilities in network equipment and operating systems. A less knowledgeable, and generally less capable, group called *script kiddies* may simply obtain software created by crackers and wreak havoc on networks. Either group can be dangerous.

  Some crackers specialize in breaking into web servers and defacing web pages. Unfortunately, this can be done quite easily, and detailed exploits are available on the web. For this reason it is very important to maintain security on your web server. This can be done to a large extent simply by applying security updates to your web server software on a regular basis.

- creators of viruses, Trojan horses, and Bots—while these programmers may never visit your network personally, their work can and very likely may be used against it.

  These are malicious software components, generally designed to attack your network resources, provide information about your network to a cracker, or *use your computers to launch an attack against another organization's network*. While these bad germs are mindless and attack any system they're exposed to, their creators are not. See the section *Bragging Rights* below to learn some of their motivations.

- an inside "predator;" in public libraries this may also be a local cracker or a staff member with a bad attitude.

Public libraries inherently provide more fertile ground for "inside" security violations. Public libraries are one of the few environments where total strangers can walk in and use computer resources. This means workstation security is much more important in public libraries than it might be in another organization.

Strangers and teenagers with too much time on their hands are just two groups representing internal threats in public libraries. Disgruntled employees are another, and they account for a high percentage of security breaches in most organizations. Therefore, some public libraries can expect to see similar activity. If there is sufficient motive, employees can be a serious threat to network security.

- a staff member or volunteer with a big curiosity.

  Maybe I'm stretching things a bit here. Most employees don't want to impair the network or use it to attack other systems. But some may search for information that is none of their business—what other employees or patrons are looking at on the Internet, for example. These are still breaches of security.

- a former employee who was fired and is holding a grudge; also a current employee who feels he has been mistreated and is preparing to move to another job.

  I'm not exaggerating. Someone with a little knowledge of the library network (e.g., the Administrator password) may take that with them and use it, trade it, or give it away. I wouldn't expect this to happen in libraries nearly as much as it happens in the business environment. It's a real threat nonetheless. A good program of security will take this into account and minimize the associated risk.

- other mindless, purposeless causes: natural disasters and simple accidents

  Accidents happen. Someone may spill liquid onto a workstation and short it out. A storm may damage one or more systems. For these events there may be no recourse but replacement. In this case, good security requires a disaster recovery plan and financial planning.

Grey Hats

Normal human beings don't see these guys often. Usually they are very knowledgeable network users. Some are "hackers" in the true sense of the term, curious about the details of operating systems, but with an interest in how they can be made to do what normally cannot be done. They do so "for the good of the networking world."

Their distinguishing characteristic is that when they find a vulnerability, they typically notify the software manufacturer to reveal the security weakness. Sometimes they make their discoveries public, trying to force recalcitrant manufacturers to take measures to fix the problem. While this may seem good, it also has the negative effect that it may lead to exploitation by the black hats.

White Hats

You've probably seen these guys in the westerns as well. The good guys. They lead the fight for truth, justice, and the American way. (Okay, I do get a little carried away, but they do lead the fight to defend the network frontier.) These are security experts and practitioners charged with defending large organizations from attack. They may also help other organizations learn about vulnerabilities and develop measures promoting sound security practice.

These, too, may be hackers in the pure sense. They test the strength of operating systems and network software to see if they can find vulnerabilities before the Black Hats do. When they find vulnerabilities, they may develop procedures, create software patches, and post security alerts so the rest of us can protect ourselves from the insecurities they've discovered.

In many cases, White Hats are available to consult on security matters, perform security audits, speak at conferences, conduct workshops, and generally help the computer and network industry protect itself against attack.

Personality

What this demonstrates is that there are many, many personalities out there. Some are just curious. Some are benevolent. Some are greedy. And some are just downright mean. When a break-in occurs, if the attacker is a curious person, he may just look at your data. A greedy person may steal a copy. A vindictive person may cut off your access to it. One wants it for himself. The other wants to make sure no one else has access to it. The effect may be the same, but the motivation is totally different.

Unfortunately, it's just not possible to forecast which personalities may come into contact with your network today—whether Internet-based or within your library. It's just as impossible to determine whether local attackers will be complete strangers or patrons using your workstations for the fortieth time, but it is possible to guess why they are trying to break in.

Treasure: The Pot of Gold

Obviously, anyone breaking into a network is looking for something. Thieves are treasure hunters. They want the gold.

If an attacker breaks into a bank's network, you can imagine what the treasure might be. Maybe he could take money from one account and put it into his own, or into another account over which he has control. Or maybe he could simply disrupt the network so that no transactions could be processed. Maybe he could try to steal credit card numbers, along with the name and address information used to confirm credit transactions on the web. There is a boatload of treasure waiting in a bank.

If the attacker was a teenage student breaking into a school network, you could just as easily guess what his treasure might be. The ability to change a grade or two—or ten or twenty; this is a lot of skill and power to be sold to other students. Lots of treasure there.

What treasure awaits the thief attacking a library network? (It certainly doesn't have anything to do with the fine money!) The ability to spy on someone's reading habits? Man, that sounds pretty boring! It would be easier just to stand behind a person in line at the checkout desk and look over her shoulder. There is probably not even any driver's license information stored online. So there is no gold in library networks, right?

I'd better give you a moment to think on this one... On second thought, it might be time for a coffee break. So take a break and think on it a moment. Why would anyone want to break into a library network? Or, take the flip side. What is so valuable that it's worth a public library's time and money to secure?

What is the pot of gold we're protecting?

Okay, go get that coffee.

Okay. Break time is over. Here it is, my list of three treasures: *budget, opportunity*, and *real estate*.

Technological Support Costs

Budget. I'll bet you weren't expecting this! Think about it. If an attacker is mean-spirited, he may attack the network out of sheer spite. Just to deprive someone else of the resource, he may choose to deliver mayhem to your network configuration. Maybe he's just trying to install his own stuff. Either way, it usually takes staff time, or a volunteer's time, or a paid tech support person's time to recover from the attack. Two of these result in lost time for doing other, probably more important, library activities. The third results in finding real money in our already strapped budgets to recover. Neither is an acceptable alternative. How many times will the library have to repeat this during the year?

In this case the gold is not what the attacker sees, but what *we* see as a result of the attack. Our time is valuable!

However, causing financial pain and suffering is not the only treasure on the network. The following two sections describe treasure much more likely to be of interest to an attacker.

Bragging Rights

Opportunity. In the scheme of things, small public library networks ought to be the last ever tampered with by attackers and malicious users, but library computers and networks do get tampered with, and on a regular basis! Most attacks are only mischievous, and many of the remainder are simple acts of ignorance. Some are purposeful, malicious acts. Why are library networks hit?

Because they are usually unsecured! Here are a few common reasons why unsecured networks are attractive targets:

- bragging rights; young "script kiddies" can break into a library network and then tell their teenage computer buddies all about it.
- learning opportunities; open networks allow inexperienced hackers to practice tradecraft; in this case, the library may never know it's been attacked because the normal intent of this type of attack is not destructive.

- mischief; some attackers are joyriders who just want to have "fun" and know the library network is one where the repercussions of their joyriding are minimal.
- meanness; what can I say—some people are just mean-spirited; they attack just to break something or to keep others from using it; for this reason, almost any network is at risk.

Strategic Bases

Real Estate. Besides bragging rights, computers on library networks also provide two other benefits to an attacker, sometimes together:

- Anonymity

  Few public libraries assign specific user accounts to patrons accessing network resources. Almost all assign some generic account for public users: Public, Patron, or some other class name.

  While this makes network administration easier, it also makes use of the network totally anonymous. There may not be any way to know who sent the latest death threat to the President of the United States from the public computer. Likewise, there may not be any way to trace the source of harassing e-mail sent to members of the community. It gets worse. There may be no way to know who used a public workstation to chat with a teenage runaway in another city or state, or who used a public workstation to break into computers at the Pentagon, Los Alamos, or the local bank. But all these activities can be traced *to* the library computer used for such activity.

- Nest building

  Some attackers will break into a library network just to build a "nest." If they can succeed in gaining administrator rights on a library computer connected to the Internet, they can store software tools on its hard drive. From this computer they can launch more aggressive attacks against other computers and networks on the Internet. Generally, these attackers also store tools allowing them to cover their tracks. Any subsequent investigation dead-ends at the nest—your library's computer.

Are These Threats Real?

In short, yes—to all of the above. One library suffered an attack resulting in the loss of its bibliographic database, with the system being down for two weeks while the database was rebuilt. Another library reported having a computer impounded because of purchases made online with a stolen credit card. Yet another incident involved a teenager using a library computer and an Internet-based chat room to arrange a face-to-face meeting with a man she had met there. And one librarian reported having e-mail sent from a library computer to a community member with whom she was having a personal conflict—signed as if she had sent it! Bots (software robots) have been developed that, when activated, make the victim computer participate in a distributed denial of service attack against another site on the Internet.

The threats are real.

The question is how likely are they to occur? Below I present a list of threats with particular activities listed below them. Each is rated—on a scale ranging from very rare to very likely—with my best guess of its likelihood to occur in your library. The more likely a threat is to materialize, the greater the risk of problems if the network is left unsecured.

- Lack of Discipline or Knowledge
  - no data backups (common)
  - no Windows registry backups (very likely)
  - no protection or poor protection of passwords for network resources (likely)
  - library staff fails to obtain password information that a vendor has used to secure a network device (common)
- Accidents (including operator error)
  - Fire (rare)
  - Breakage or Damage to Equipment (very rare)
  - Spills (rare)
  - Faulty Wiring or Electrical Equipment (rare)
- Natural Disasters
  - Flood (depends on location; not uncommon)
  - Electrical Storm (not uncommon)
  - Tornado (very rare)
- Human Attackers
  - Theft of equipment (not uncommon)
  - Web server defacement (common)

– Password guessing (common)
– Internet probing (very likely)
– Infiltration and nest building (common; likely in a poorly secured web server)
– Workstation configuration alteration (very likely)
– Installation of personal software (common)
– Illegal activities (not uncommon)
– Destructive activities (reformatting hard drive or deleting files—rare)
– Viruses on unprotected workstations (common)
– Unauthorized access to patron data (rare)

Consequences of Not Securing the Library Network

In many libraries Internet access has been offered for two or three years without any major problems. Installation of basic workstation security measures alleviates many, many headaches and eliminates a lot of wasted staff time. So, what are the consequences of just letting the network configuration roll on as it is?

It is tempting to let things continue as they are when there have been no demonstrable problems. The problem with leaving a network unsecured is that past performance is no predictor of future events. Leave your server poorly secured and one day you may find yourself unable to log in as Administrator to add another user, or change some system setting. Then you will be left with the option of trying to crack the current Administrator password yourself or reinstalling the system from scratch. It's almost totally unpredictable what *may* happen. Here are some possible consequences of doing nothing:

- Nothing bad will happen; the network will continue operating as it always has (consider yourself fortunate)
- A workstation or two will have to be reconfigured occasionally; if we could predict this, we'd just invest our security money in tech support
- The library will suffer the embarrassment of having one of its workstations or servers participate in an Internet attack or of having its web server's pages defaced

- The library will suffer the loss of a workstation or server as evidence due to its being used to conduct illegal cracking attempts over the Internet (the attacks could originate from a user inside the library or across the Internet)
- The library will lose a key component of the network—a switch or the router or firewall—due to storm or theft. The entire network will be down until a replacement is installed and configured.

Just looking at this range of possibilities shows the cost of inadequate security varies from practically nothing to almost catastrophic. If the library has no disaster budget and no means of replacing equipment, it may lose network access completely: no Internet access and no catalog (if the library is automated). If the library is providing access to its library catalog over the Internet, what will be the perceived loss when patrons can no longer access the catalog from home?

What Attacks are Most Commonly Experienced?

Thankfully, the most common attacks experienced in public libraries are more mischievous than damaging. These are workstation configuration messes: adding or removing icons, changing the wallpaper, changing the screensaver, installing personal games and browser plug-ins required to play Web-based games, and others. Occasionally a patron will try to break into the Administrator account on the network, just to see if he can.

Theft always remains a very real possibility. If your library just got a $30,000 grant to expand access to the Internet and provide access to your library catalog over the Internet, it will not be a secret. Everyone in the community will know about it. Even the bad guys. $30,000 worth of computer equipment will still fetch a handsome price on the black market. Not only that, but with 24-hour-a-day access to the Internet, your web server will become more of a target for Internet-based attackers.

These aren't the most significant problems. Libraries aren't like the normal business world where business-critical security simply must be implemented. Libraries exist in a very different economic and political environment and, therefore, have a much broader set of concerns. The list below demonstrates this in item one: money. Because of its cost, *network security may be easily overlooked by policymakers in local communities*. Yet, sustainability of grant projects, including increased funding for maintaining current levels of technology, is of primary importance. In most small communities, the threat of losing service due to inadequate funding cannot be understated or overemphasized.

With that said, Table 1 below presents the top ten threats to network security I see in most small libraries, listed first in order of probable occurrence. In column three I've also listed the order in which I believe most small libraries are able to implement security measures to defend against them, from least expensive (in time and funds required) to the most expensive.

Table 1. Top Ten Network Security Threats

Order by Likelihood	Threat	Order by Expense
1	Inadequate funding to operate, maintain, and replace network equipment	10
2	Local patron tampering with workstation desktop and hardware settings	4
3	Unauthorized access to workstation file systems, including installation of personal software and other activities	5
4	Defacement of library web pages if hosted on library-based web server	8
5	Theft of equipment	9
6	Damage to equipment or data due to electrical anomaly; for example, lightning strike, surges, or inadequate power	2
7	Local users cracking of passwords, especially for the Administrator account	1
8	Internet-based attacks of internal network resources	3
9	Unauthorized access to server file systems	6
10	Tampering with local network infrastructure: network devices, network wiring, etc.	7

Having listed the above threats, one commonly overlooked item when networks are first configured in libraries is obtaining copies of passwords. Some vendors have not provided to their library customers the passwords used to secure switch, router, or firewall configurations. Not having the passwords can cause expensive delays when the devices must be reconfigured in the future. *Be sure you obtain the passwords from your vendor.*

A Self-Assessment

Having noted some threats that are present in every library environment, it's time for a test. How has your library prepared for the common maladies that plague networks? Look at the questions below and check the ones you've already addressed in your library.

- □ Is the back up of your library automation server current (performed within the last week)?
- □ Is the back up of your primary administrative workstation current (performed within the last week or two)?
- □ Do you have workstation security software installed or Windows NT/2000 Workstation securely configured to minimize mischief on your public access workstations?
- □ Are the virus definitions for your anti-virus software up-to-date (new signatures downloaded within the past week)?
- □ Do you have the BIOS supervisor password set on all your public access workstations?
- □ Have you changed the default Administrator password on your Windows NT/2000 Server and your Local Administrator password on your Windows NT/2000 workstations?
- □ Does the library have a simple, written, disaster recovery plan (e.g., do you have procedures in place to help you recover if your server is stolen over the weekend, or if the library roof develops a leak and pours rainwater on top of your server and network equipment)?
- □ If someone breaks into your network, do you have a mechanism in place by which you might discover it (you get bonus points if your network is configured to alert you immediately that certain attacks are happening *right now*)?

Okay, now for the assessment part. If you checked less than five items, you need to do a lot of work, just like most small organizations! If you checked less than seven items, you still have some work to do. If you checked all eight, you have reason to celebrate! Your library has already done a lot of work. You may still have a couple of corners to clean up, but your network is secure from a lot of the bugaboos likely to attack it.

If your library is like most, you've discovered some threats that need to be addressed. To help you get started, I will present some principles to use in assessing and managing risk and security in your library in the following chapter.

Summary

- We defined nine key terms used in discussing network security: network resources, backup, attacker, weakness, vulnerability, exploit, intrusion, and risk.
- We described three types of personalities involved in network security:
  - Black hats: the bad guys who seek to control or misuse others' network resources
  - Grey hats: the in-between guys who work at discovering vulnerabilities and getting vendors to fix them, but who sometimes publish their findings, making it easy for black hats to break into networks.
  - White hats: the good guys who seek to discover vulnerabilities and educate the network community about them.
- We described three aspects of the treasure incorporated into your network:
  - Budget: time and expense incurred in recovering from attacks
  - Opportunity: the bragging rights and learning opportunities represented by weakly secured library networks
  - Real estate: servers or workstations attackers can use to run their own software, typically used to attack other networks
- We categorized the likelihood of particular threats materializing and the consequences of not securing your library's network.
- We listed the top ten threats to network resources in small public libraries.

2

Managing Risk

John uses library workstations frequently for Internet access. The new computers work pretty well for gaming, and the library's policy allows him to play when no one else is waiting to use a station. The library also has a policy against bringing in your own diskettes; patrons are supposed to buy them at the circulation desk. Ms. Smith is so busy she does not notice who sneaks a diskette out of his pocket or backpack.

Games get boring for John. So every once in a while, just for grins, John tries a few new tricks, just to see if he can get to anything that's normally off limits. The new workstations are secured pretty well, so there's not much a user can do to change their configuration, unlike the old ones these replaced. Occasionally he logs off, just so he can see if he can guess the Administrator's password. So far, he hasn't been able to crack it, so it's still an amusement for him.

On the other hand, today John has learned he can execute a program from the main drive's TEMP directory. He'd never tried that before. So he creates a folder named F111 under the TEMP directory. If it's there tomorrow, he'll know it doesn't get cleaned up when the system gets rebooted. Then he'll try to download a root kit to it. It could get really *interesting tomorrow!*

"The uses to which we intend to put the network drive the security requirements for our network, and these strongly influence the security solutions we will choose and our degree of willingness to invest in network security solutions. Some networks require relatively little security; others may require a great deal."[3]

[3] Marcus, J. Scott. Designing Wide Area Networks and Internetworks: A Practical Guide. Addison-Wesley, 1999. p. 253.

You've learned that security is a process. You've learned there are some real threats to your library's network. You've hopefully made a decision to minimize as much risk as possible. All of this can be called *managing security,* or *managing risk.* In this chapter I'll present information to get you started on the road to securing your network: determining which measures to implement and how to carry that through; in other words, how to manage your library's program of network security.

How to Secure Resources

Securing a computer network is the process of mitigating risk—bringing risk down to a manageable level. Another way of saying this is that network security is about balancing the consequential cost of dealing with an attack against the cost of implementing sufficient security measures to prevent, or reduce the likelihood of, an attack. Securing a network is important because there is a very real cost in recovering from an attack.

On the other hand, there is a definite cost in implementing security measures as well. Ideally, in securing network resources, we would like to spend just a little on security in order to keep from having to spend a lot on recovery. The work is a balancing act of cost versus risk.

Once one has a grasp on the necessity for network security—and what may occur if the network is left unsecured—it is a lot easier to begin the process of managing risk to network resources. In the last chapter we dealt with the first step: identifying threats. In this chapter we introduce the other major aspects of risk management:

- Assessing Risk—determining what to secure
  - What are the threats present in your network environment
  - What are the most significant risks in your network environment (review an appropriate checklist)
  - How much latitude local users will have in using public workstations
  - How much latitude staff and volunteers will have in accessing the network
- Developing a Security Policy
- Updating Staff Skills (providing/scheduling training: to recognize threats, enforce security policy)

- Monitoring Security
- Regularly Reviewing Security Resources for other measures to implement
- Repeating the Process

Assessing Risk—Deciding What to Secure

Your security management program begins the moment you assess the threats to your network to determine which are most likely to be realized in the form of an attack. Let's call this step one: securing your network. In fact, let's build a list of steps you will go through in securing your network:

1. Assess the threats to your network.
2. Assess the vulnerabilities open to attack. This requires investigating the possible vulnerabilities using a standard list of items that describe them.
3. Evaluate which vulnerabilities are most likely to be exploited by the threats you've identified. Vulnerabilities that can be exploited create the risk of an attack occurring. Vulnerabilities that are easily or conveniently exploited create *great* risk.
4. Estimate the cost of securing the vulnerabilities you've identified.
5. Determine how much money you have available for implementing security.
6. Prioritize the risks. Use the cost estimate you created in step 4 to decide which vulnerabilities you can reasonably secure. See "Determine Priorities" below for more details.
7. Hire someone (or have staff trained) to implement security measures that eliminate or minimize the vulnerabilities you've decided to secure.
8. If financially possible, have the security implementation audited to verify that your security decisions are implemented as specified.

Determine Priorities

It is step six above that is the most difficult, because there are multiple ways to categorize and prioritize risk. As mentioned, you must determine the cost of security first. If it costs more to secure a vulnerability than to recover from an attack on it, you will likely decide not to secure it. Likewise, if the risk is extremely low (the likelihood of its being exploited is low), then you may also decide not to secure it. On the other hand, even if the risk is very low, if the exploitation of the vulnerability will result in an extremely expensive recovery, then the vulnerability should be secured.

After this raw cost basis, you must prioritize the remaining areas. I've identified four common-sense principles used generally to prioritize actions. Let's see how these work in the context of computer networks.

- ♦ Secure the simplest things first

This principle sounds good up front, but it has a weakness. Many involved in securing networks know the simplest things aren't always the least expensive. Some security measures are simple only when you have sufficient knowledge to implement them. Unfortunately, obtaining someone with the requisite knowledge may not be inexpensive. So, given the limited budget circumstances most libraries find themselves in, simplicity may not be the best criterion to use. A second principle that might be more appropriate in determining priority is:

- ♦ Secure the least expensive things first

Expense—or lack of it—is also a good criterion, but it has limits as well. Someone will point out that the least expensive things don't necessarily represent the most serious things. For these practitioners, it may be more appropriate to prioritize risk by a third principle:

- ♦ Secure the most serious things first

Believe it or not, there may be a fourth camp of security experts. These recognize that the most serious things are not always the things most likely to occur. They advocate this principle:

- ♦ Secure first the things most likely to result in an attack

This is a great deal of categorizing! In fact, there are 24 different ways to arrange just these four categories to determine priority. Thankfully, you get to choose which elements carry the most weight for the purposes of evaluating priority in your library. For right now, let's just say this: if securing a vulnerability includes any three of the four of these principles (e.g., a very serious vulnerability, that is likely to be exploited and is inexpensive to implement), then it should have a very high priority for security.

Once you have determined priorities, it is very important to document the library's decisions, especially when deciding not to secure some areas (some will say it is important to document all the security decisions, describing why security measures are implemented or why they are not). This documentation will be used in future reviews to determine which environmental conditions might have changed and whether the reasoning behind the decision is still valid.

Least Privilege

There is one more common security principle we need to introduce here because it impacts risk, even though it has nothing to do with prioritizing them. Rather, it has to do with the access a user has to network resources. It's called *the least privilege principle*: when creating new network user accounts, grant the user the lowest level of privilege necessary to perform his job functions properly or use the available network resources appropriately.

For example, this means that you may be creating a security risk by granting a staff member the right to execute backup software on the server when the user has no responsibilities for backing up systems. The fact that the staff person has this right may lead to unintended access to other information—a password file, for instance.

This principle comes into play for the person actually performing the initial configuration of your library's network and for the person charged with creating and maintaining user accounts for the library network.

A List of Suggested Priority Areas to Assess

While you could (and should) go through a long list of security measures, such as the *Network Security Checklist* included in Part III, it's usually helpful to have a starting point. Here is a list of areas where attention to network security will provide the most benefit for a small investment in time and money. This can be considered a minimal security configuration suitable for those libraries where there is little risk of patron tampering.

- Theft and electrical protection, including a surge protector or UPS on all workstations, servers, and network equipment; placement of equipment (line-of-sight considerations, etc.) is also a factor
- Workstation security, including proper file system protection, through the use of third-party security software (such as WinSelect Policy+Kiosk, Fortres 101, or FoolProof Security), security hardware

(such as Centurion Guard), or Windows itself if Windows NT Workstation/2000 Professional is used (through policies, profiles, and permissions)

- Proper file system protection on servers, with severe limitations placed on the patron account(s)
- Anti-virus software installed on all workstations
- Strong password selection on all staff and administrator accounts
- Secure configuration of the server Administrator account
- Proper router/firewall configuration. This item is best considered before equipment is purchased. Firewalls, which are generally used to keep the bad guys on the Internet from accessing any computers on your local network, come with different capabilities. It's important that the firewall be configurable to prevent many common Internet-based attacks. It should also provide a network port called a DMZ to offer protection for publicly accessible servers, like a web server. There are several configuration issues to address here.
- Updated operating system software on all workstations and servers, and updated web server software if a web server is used.
- **Do not install a web server in this configuration unless absolutely necessary.** Providing access to web services over the Internet requires a more complicated configuration of the router/firewall and introduces several points of weakness into the network.

Of these items the first four will potentially be most expensive. If library computers are not covered by city/county or building insurance policies, such a policy might be investigated. Insurance policies should provide *replacement* costs and should cover theft of the equipment, accidental breakage, and damage due to lightning or other electrical anomaly. Workstation security software must be purchased, or a technician must be hired to configure tight security through Windows NT Workstation (2000 Professional).

However, the other items can be implemented with little or no additional cost to the library. The router/firewall configuration cost should be included with its purchase. Password selection can be taught to staff, as can proper procedures for updating, or "patching," server and workstation operating systems. The Administrator account configuration should have been included in the initial server and workstation configuration. If it was not, then, with a little staff training, the cost for reconfiguring it is minimal.

The Need for a Security Policy

In order to secure all the areas of your network adequately, it is necessary to determine how the resources will be used. To which resources will your staff, volunteers, and patrons need direct access? Which patron activities will be permitted and which will be restricted? What are the responsibilities of each of the constituent groups (staff, volunteers, patrons, contract technicians, city staff)? These questions point to the need for a written guide describing intended/appropriate access to and use of network resources.

A document created for this purpose is generally called a *network security policy* (referred to hereafter simply as a security policy). Security policies are still uncommon in local government agencies, but they are becoming quite common in the business sector. In libraries, the security policy will have some areas of overlap with the acceptable use policy. Whereas an acceptable use policy is generally aimed at patron use of the network, a security policy is much more comprehensive, including rules and guidelines for all access to and use of the network.

Just like an acceptable use policy, the security policy will only be useful if it is developed as an administrative guide rather than treated as just another task to be completed. There is a great need in small public libraries for such policies because they provide continuity, consistency, and a basis for enforcing staff and patron conduct on the network. Developing a security policy also makes an administration really *think* about the use of the network. The security policy encapsulates the decisions made by library administration regarding proper use of the network; therefore, future library directors don't have to wonder why certain aspects of the network are implemented the way they are.

Libraries will benefit from doing a security policy "right," but this means taking more of the library director's time. In some small public libraries there may be no desire to take time to do another paperwork project. If you simply can't take the time, it will be better simply to review the library's current acceptable use policy to be certain all of the proper "right and responsibilities" are included, as are all of the warnings regarding improper use. Be sure to note the reasons security decisions have been made and leave the notes for future administrative needs.

A sample security policy is provided in Part III for those libraries wanting to start with an existing document and refinish it to fit their own environment. This sample is a heavily edited version of one provided in the Federal Information Processing Standards (FIPS) documentation for federal agencies,[4] including wording and provisions more commonly used in small public libraries. Permission to use the security policy in its current or edited form is granted to all entities.

The Process of Implementation

Once a risk assessment is completed and a security policy is developed, an implementation of these security decisions must be performed.

The following list provides a rough outline of the process of implementing a network security project. The first two items represent the risk assessment process presented earlier, but are repeated here for continuity.

1. Meet with a vendor or consultant educated in network security issues to discuss the costs of implementing various security measures (such as those in the *Network Security Checklist*) and the likely consequences of not implementing each measure.
2. Review costs and determine which security measures are required for your library and which risks the library is willing to accept (areas where security is not specifically implemented).
3. Develop a list of specific security measures to be implemented and a request for proposals (RFP) to be submitted to prospective vendors.
4. Review the RFP with the library board and with regional library system staff familiar with security in public libraries.
5. After the RFP is approved and formally produced, submit it to three or more suitable vendors and advertise it.
6. Award the project to the most appropriate responding vendor (for a discussion of appropriate vendor characteristics, see the discussion of vendor selection under audits on page 62).
7. If possible, have interested staff shadow the vendor during implementation to see what aspects of security in-house staff can learn.
8. Begin a similar process for a security audit to determine how well the vendor implementation matches the library's stated goals for its security implementation.

[4] Computer Security Resource Center (CSRC). *FIPS 191: Guideline for The Analysis of Local Area Network Security*. National Institute of Standards and Technology, November 1994. pp. 40-47.

Maintaining Security

Implementing network security is not the end of the project. Remember that security is a process. There is an ongoing aspect of security that requires regular maintenance.

Managing risk includes two associated topics as well: detecting intrusions and responding to attacks. These areas are formally called *intrusion detection* and *incident response*. Each of these is an important part of an organization's network security program, and there are entire books available about them. They deserve discussion in separate chapters, but their complexity and cost will impair most small public libraries' abilities to formally adopt them into the security project. Therefore, I present them briefly below, leaving a fuller discussion for another time.

In addition to these two areas, I also present below the other ongoing aspect of network security: keeping the library's implementation current.

Intrusion Detection

As defined at the beginning of chapter one, an *intrusion*, or infiltration as it's called in some sources, is a successful break-in, where a user exploits a vulnerability or breaks through the security implementation and gains unauthorized access to network resources. *Intrusion detection* is the art of using software tools and configuration techniques to monitor network activity so that any break-ins—or even break-in attempts—are reported to security staff. The report can take the form of a log entry (notation in a text file), an e-mail message, or an alert sent across the network to a manager's console. In large businesses, the vast majority of a security manager's time may be consumed with intrusion detection. After all, if someone breaks into your network, you want to know about it before they make off with all the treasure!

For our purposes, however, I need to reduce the topic to practices that are appropriate in a small public library. First, let's refine our terminology. Public libraries probably won't have a great number of intruders from the Internet. They may, however, have several local users over a period of time that "test the locks" on the doors of the library network. For example, you should expect over time to see someone to try to guess the Administrator password on a Windows NT/2000 workstation or server. You can also expect users to try to load their own software onto the local hard drive. While these may seem innocuous, especially if you've implemented security measures to prevent success in these attempts, they are still attempts at intrusion.

Let's consider all the security mechanisms your library has put into place to be a bubble of security surrounding the network resources. Any attempt to test the network for vulnerabilities, implement known exploits, or just use the network in ways that are restricted by policy will be considered poking the bubble. Any successful attempts will be considered popping the bubble. Neither one is good. As a manager, you need to know when any of these events occurs.

Unless you stand over a user's shoulder, the only way to know that such attempts are occurring is to monitor activity on the network. One can do this without having to know the content of a user's searching on the Internet. Monitoring is accomplished primarily by configuring the Auditing feature within Windows NT/2000 user and group accounts. One can also monitor Internet activity by noting restricted router, firewall, and web server activity in a log file. A *log* is a standard text file (one that is editable in Notepad, for instance). Specified activities cause a new entry to be recorded in the log. All of the following devices are, or should be, capable of creating an activity/audit log:

- Windows NT/2000 Server (audit logs)
- Windows NT Workstation/2000 Professional (audit logs)
- Router
- Firewall/security appliance
- Web server

A network administrator can set the parameters controlling when a log entry is created. The log might record the type of activity that triggered the entry, the date and time, and the workstation and user id that were being used. Depending on the type of device, more information can be recorded in the log. The administrator can also configure many of these devices to send an alert when restricted actions are attempted.

In order to be effective, the logs must be reviewed on a regular basis (every day, two days, or once a week; any period longer than a week may be too long to be helpful, except to know *someone* is messing with your network). Staff or volunteers can be trained to examine the logs and assess the danger in intrusion attempts. [*Note:* It is possible to contract with a vendor to monitor logs for the library, but the service is usually financially impractical in small public libraries.] Reviewing logs is an important aspect of the library's network security program, so someone must be assigned the responsibility. The library director must encourage regular review by seeking status checks occasionally.

Other options. For larger libraries, separate intrusion detection hardware/software can be purchased to perform more advanced duties. In businesses where a security breach can be catastrophic this equipment is common. However, the cost of equipment and maintenance is too great to be practical for small libraries.

Monitoring a server's file system for changes is another option for some libraries. This security technique can provide information about an intrusion even if the audit log has been tampered with. This, too, may require maintenance from an outside vendor. If existing staff has the technical acumen to be trained in this procedure, the training is highly recommended.

The Cost of Intrusion

Is all this work worth it? Just remember what the consequences may be if, indeed, intrusions occur. In some cases the intrusion will be kids just playing. In others it may be serious hackers looking for a home. The following list of consequences is provided as a reminder, and a bit of a warning:

- Data loss or corruption
- Cracking an Administrator account and controlling the server or workstation
- Attacking the Web server and gaining Administrator privileges (defacing the web pages is one effect, controlling the server is another)
- Nest building in order to launch attacks on other targets
- System corruption/disablement
- Impounding of one or more computers as evidence due to illegal activities

Responding to an Incident

If you've had a chance to get coffee, you may have already thought of the next question. What happens when, despite the great lengths you've gone to secure your network, someone discovers a new vulnerability before you have an opportunity to close it and breaks into your network? What if the person you've put in charge of reviewing server logs discovers an intrusion? What if, like the library director in the opening scene to chapter one, you get an e-mail message indicating that one of your workstations participated in a coordinated attack of some other network across the Internet? What happens then?

Most libraries have no plan for such an event. The typical response tends to be haphazard. The problem with an ad hoc response is that the moments after the discovery can be important. It *may* not matter if you do anything, or what you do, for the next week or two. However, what you do the next few minutes may be *very* important. If the intrusion is ongoing, what you do may make the difference between "catching" an attacker and letting him get away. It may make the difference between being able to prosecute an attacker who's caught and being unable to prosecute.

Do you have an incident response plan for your library? If not, here are some basic suggestions to get the planning process started:

- Find out if the city/county is interested in any attacks that may occur on the library network. If the library network is connected to the city/county network, there *should* be a great deal of interest. Otherwise, there may not be. Likewise, if the library receives its Internet connectivity through the school district, find out if the school district is interested in any attacks you discover on your network (there should be).

  Assuming the external agency is interested, clarify which security breaches need to trigger a phone call and to whom.

- Determine the proper chain of command. As a result of the step above, you may be required to contact a member of the city/county/school staff immediately. If you've contracted with a vendor to assist with network maintenance and security, you have a contact to call there as well. Determine who needs to be called first. Establish contingencies for your contacts as well. If one contact is on vacation, whom do you call in her place?

- Determine the proper course of action for legal inquiries. For example, if a law enforcement representative shows up with a court order to search records or impound equipment, do you call someone (either before or after some item gets whisked away as evidence)? If so, whom? If a local patron is discovered conducting illegal activities, what steps need to be followed?

- If insured equipment is damaged or stolen, what is the procedure for filing a claim? What is the contact person's name and phone number?
- What procedures need to be set in motion as a result of your intrusion discovery? These may vary greatly based on the nature of the intrusion. This is especially important if the intrusion is active at the moment. In some cases, a staff member may be glued to the telephone and in front of a workstation for a while, acting as a remote security contractor's eyes and fingers.
- There are also questions related to recovery. For example, if an attack results in an Internet-based attacker having control of a server, how will the server be restored to its "pre-hack" state? Who will be responsible for working on the server? How long will it be out of service? Will a loaner be available for the library's use? Is there money in the budget to cover a vendor's time in conducting the recovery?

As mentioned earlier, this is a topic that deserves much better coverage than we can devote to it here. I hope these suggestions are enough to get you started, at least in considering the ramifications of a break-in and how your library can recover.

Staying Current

With new vulnerabilities being announced weekly and new products and services being announced almost as often, how are you as a small library manager to keep up? One easy suggestion is for you to team up with other library directors in your area to split duties by assigning each a different security topic. Here are four areas to start with:

- Security updates to the Windows NT/2000 operating system
- Security updates to the Internet Explorer browser
- New workstation security techniques using Windows NT/2000
- Security updates to the Microsoft Office applications

There could be other areas as well, such as updates to network equipment.

While trained technical personnel should be hired to update network equipment, library staff must be aware that such updates exist. (In fact, if no technically proficient staff are available, even routine patch installation may require the services of an outside vendor.)

Besides security updates, what other activities are involved in keeping your network security implementation current?

- Review the backup program—check periodically with the person responsible for backups to be sure they are performed on schedule.
- Update anti-virus signatures—even though these are now downloadable automatically, it never hurts to check occasionally to be sure the signatures are indeed updated.
- Upgrade software—at some point, security patches are no longer sufficient. Keep track of optimal times for upgrading or replacing outdated software.
- Review and maintain the budget—the most important of all

Developing a Security Plan

No work on managing a service would be complete without a section on planning. In this case I present just a skeleton, which you can alter to fit your library's needs.

- Assign Responsibilities
  - For maintaining backups
  - For assessing risk
  - For implementing the security program
  - For developing policies, plans, and procedures associated with security
  - For monitoring log files
- Assess Risks
- Implement Specified Security Measures
- Develop Policies, Plans, and Procedures
  - Network Security Policy
  - Acceptable Use Policy
  - Password Policy
  - Backup Plan
  - Disaster Recovery Plan
  - Incident Response Plan

- Monitor Logs
- Report Anomalies and Incidents
- Perform Regular Maintenance
  - Backing up data
  - Reviewing network security sites for new vulnerabilities/software updates
  - Patching operating systems
  - Upgrading software
  - Raising funds

Summary

In this chapter we covered a lot of ground. Here are the main points of managing security:

- First, assess risk; this includes evaluating the threats and vulnerabilities present in your network, as well as evaluating which are most likely to be exploited in your library environment.
- Next you would estimate the cost of securing the vulnerabilities and compare that to money available to secure them.
- Finally, prioritize risks by determining which of the vulnerabilities are most serious, are likely to be exploited, and are inexpensive to secure.
- Develop a formal process to hire a vendor to implement the desired security measures.
- Develop a security policy to describe the rights and responsibilities of users of the network and of management.
- Implement a procedure for monitoring access to the network to detect any illegal or unauthorized use of network resources.
- Determine proper procedure for use in responding to any security breaches.
- Develop an outlined plan for implementing security in your library.
- Determine how your library will keep its security implementation updated.

3

Securing Financial Resources

"Four years," the young woman had said, "maybe five. But you'll need to begin searching for replacement funding before then."

Mr. Johnson looked at the figures on the budget sheet before him and sighed. Every year it was the same thing, asking people for more money. There was always something that needed to be done, something that came along to steal his time and sap his strength. He had always intended to get it done – tomorrow.

No one provided grants for operating costs.

He looked over the top of the sheet and gazed out in the public area. Of his ten workstations, three had "Out of Order" signs taped to the front of the monitors. One hard drive failure, one he didn't-know-what failure, and one complete trashing. None would run the latest version of the library's public access catalog software, so he hadn't upgraded.

Where was he going to find $10,000 to replace them?

As mentioned in the Chapter One, probably the most common—and potentially most dangerous—threat to network security in small libraries is the lack of funding required to properly maintain the network. Many libraries have received the bulk of the technology equipment, software, and cabling (collectively called *infrastructure*) through grants. The problem is most library budgets are not sufficient to support the cost of maintaining this infrastructure. In this chapter I focus on the monetary resources required, including the costs to secure certain network components.

The Cost of Operating a Small Library Network

Costs associated with developing and operating a small library network vary from one library to another based on the purchase decisions management makes. Some entities purchase from local vendors, some from national vendors. Some purchase "business" model computers (which have features like manageability that regular workstations do not), and others purchase the least expensive equipment they can. Nevertheless, some general guidelines can be established for average costs in a small library.

Equipment Used

The following table details the major components used in creating a small library network. Workstations and servers are assumed to have a network card included in the base installation. The costs for computers shown below include shipping costs if ordered online. Computer prices may be reduced by $100 each for local purchases. The last column indicates the allocation I recommend including in the library budget for annual maintenance of the equipment, with the minimum budget allocation included in parentheses.

Table 2. Network Equipment Costs

Quantity	Description	Cost	Maintenance
6	Public Internet Workstations	$ 8,400	$ 600 (300)
2	Staff Workstations	2,800	200 (100)
1 staff 2 public	Circulation/Catalog Workstations	4,200	300 (150)
1	Automation Server	5,000	150 (150)
1	24-port Switch	1,200	100 (0)
1	Router	700-2,000	100 (50)
1	Network Laser Printer	2,100	100 (50)
	Total:	$ 24,500	$ 1,600 (800)

One might argue that maintenance costs increase with the age of the equipment, and that the costs shown above may not be appropriate till the third or fourth year the equipment is in service. However, an opposing argument suggests using the standard industry average for an annual maintenance contract, which is 10% of original cost ($2,450 for this example). Another argument is that the annual maintenance cost shown here ($1,600) only represents between 27 hours (at $60 per hour) and 53 hours (at $30 per hour) of a technician's time—and just 13 to 26 hours if the budget is $800. Depending on the severity of the network or computer problem, this represents only 4-6 incidents during the year. This, indeed, is minimal for the normal operation of a small network.

If a security breach results in the need to call in a paid technician to resolve resulting problems, the maintenance budget gets squeezed even further. How many such breaches can the library pay to resolve?

Libraries in Texas using a regional library system TANG technician (a system staff member hired through a state Technical Assistance Negotiated Grant) for network maintenance will be able to stretch their budgets, because the TANG technician's assistance is "free" to the library. I highly recommend that libraries with access to a TANG technician use her services as often as possible. Unfortunately, this is a resource with diminishing returns. As more libraries use the TANG technician, the less available she will become—especially in emergencies. So budget funding still needs to be available to hire paid technicians.

Software Maintenance Costs

Equipment maintenance costs are not the only maintenance costs involved in operating a network. Library automation software requires a software maintenance/support contract to be renewed each year in order to receive technical support. One can also expect a software upgrade (for the operating system and also for those workstations providing MS Office to patrons or staff) to be needed during each computer's service life. Table 3 indicates common software costs a library can expect to incur during the normal lifespan of a computer.

Table 3. Software Maintenance Costs

Software Description	Update Cycle	Cost
Library Automation System (support)	Annual	$395
Automation System Web Server Module (support)	Annual	$195
Security Software Upgrade (if used)	Approx. Two Years	$30 per workstation
MS Office upgrade	Approx. Three Years	$90 per workstation

MS Windows upgrade:	Approx. Three Years	
NT Workstation -> 2000 Professional		$48 ($101)
NT Server 4.0 -> 2000 Server		$92 ($145)
2000 Server Client Access Licenses, each		$5.10

MS Windows and Office upgrade pricing is for the Academic Versions (no technical support provided). The pricing shown is available through the Texas Department of Information Resources as of July 1, 2001, and is subject to change. Prices in parentheses include the license, manual, and media, whereas the lower prices include the license only. In most cases only one copy with new media and manuals is required. The remaining computers require a license, but can be upgraded physically from the same master CD. Some libraries may require multiple copies of media and manuals.

Services

Various services, from cable installation and workstation configuration during the initial creation of the network to Internet access costs incurred during its use, contribute to the annual cost of offering Internet access and automated library systems. Table 4 shows approximate costs of these services (cabling and configuration costs will apply to any future workstations added to the network as well). The estimates shown are "average" costs, with high-end costs displayed in parentheses.

Table 4. Service Costs

Software Description	Cost	Cost after 70% E-Rate Discount	Ongoing Annual Cost
Cabling and Configuration, Per "drop"	$150 ($250)	—	—
ISDN Line	$60 ($120) / month	$18 ($36)	$216 ($432)
128K Internet Access (ISP)	$50 ($300) / month	$15 ($90)	$180 ($1,080)
		Total:	$396 ($1,512)

Equipment Replacement

The most difficult cost to deal with, however, is the cost for equipment replacement. This cost is deceptive because replacement is not an immediate need. It's easy to put off, but replacement must be planned if your network services are to continue. The sooner you prepare your replacement plan, the better.

Future costs represented by equipment replacement are easily figured. All equipment has to be replaced after a number of years of service for three common reasons:

- it will fail through normal use
- it will become obsolete, unable to perform the functions we need
- the manufacturer will declare it beyond useful life and cease to support it

In most cases, the useful life for equipment in public libraries is longer than it would be in the business environment because of the need to stretch funds. Productivity and competitive advantage will be of lesser strategic advantage in libraries than in businesses. Nevertheless, even given a longer lifecycle, costs associated with equipment replacement are large.

For public libraries, I recommend a four-to-five-year replacement cycle (current business practice sets obsolescence at about three years). Patrons may begin to see the equipment as "old" and outdated after four years, especially if office software is provided but hasn't been upgraded.

Four years of ownership represents a critical time period because technology may have evolved enough to make an upgrade undesirable. The processor package may have changed enough that updating the processor means replacing the motherboard as well. More RAM, or a different type of RAM, may be needed with a new motherboard. The video card may also need to be replaced. The combined cost of the parts, plus the cost of installing them, usually ends up being just a little less than the cost of buying a new unit. Considering a new system has a complete, three-year warranty, buying new looks much more attractive than upgrading. So the fifth year may be one when the library limps along, knowing that waiting a year and purchasing a new system is more feasible than upgrading this year.

Table 5 illustrates the estimated replacement period for various components of a small library network. It includes the number of years you may expect a particular component to serve before needing to be replaced.

Table 5. Equipment Replacement Costs

Equipment	Replacement Period	Expected Replacement Cost	Annualized Replacement Cost
Public Internet Workstations (6)	4-5	$ 6,000	$ 1,500 ($1,200)
Staff Workstations (2)	4-6	2,000	500 (333)
Circulation/Catalog Workstations (3)	5-6	3,000	600 (500)
Automation Server (1)	6-8	4,800	800 (600)
24-port Switch (1)	7-9	1,000	144 (111)
Router (1)	7-9	500-1,500	71 (46)
Network Laser Printer (1)	5-7	1,800	360 (257)
	Total:	**$19,600**	**$4,046 ($3,093)**

Obviously, it's impossible to forecast hardware failures, so these periods are just estimates. The annualized replacement cost includes dollar estimates for both the optimal and a maximum (protracted) replacement period.

The Cost of Securing a Small Library Network

In terms of dollars, the purpose of security is to spend a little up front in order to keep from possibly having to spend a great deal later on. So it's important to quantify the potential cost of not securing the network. Some costs are easily estimated and quantified:

- staff time required to handle problems related to altered workstation desktops
- staff time required to reconfigure such desktops, and deal with vendors supplying technical support
- the cost of having a vendor reconfigure or repair a workstation configuration

However, there are other factors for which cost is not so easily quantified:

- patron disappointment and upset feelings when a workstation is not available or working properly
- the library's loss of use of its automation system for a period of time if catalog stations or the server is tampered with
- the negative publicity generated by an attack or someone using the workstations for an illegal purpose

Given these limitations, we are left with vague guesses about the cost of security breaches. But the dollar cost of implementing network security, on the other hand, is much easier to estimate. There are several variables that affect the cost:

- the number of workstations and servers to be configured and tested
- the number of security measures to be implemented on each workstation and server (determined in consultation with the library director)
- whether a public server (such as a web, DNS, or mail server) is to be secured
- the complexity of the router and firewall used
- how much of the work can be performed by local staff or volunteers (such as configuring backup software to perform scheduled backups of important data, including the library's bibliographic database and director's documents directory, and making sure physical security is addressed)
- the experience of the vendor representative (in working in a public environment) contracted to secure the network

Table 6 provides a sample cost summary, with estimates of the time required to perform the various activities. To arrive at the cost range for security configuration, I make two assumptions:

- a technician with little experience configuring workstations and servers for security will take considerably longer to complete the task, but charge less for the time spent

- router/firewall configuration will be performed by a network technician experienced in such configurations, at a higher hourly rate

Table 6. Security Implementation Costs

Security Service	Est. Hours	Cost
Securing workstation configuration (per workstation; 6 total)	0.5 - 2 3 - 12	$38 - $100 $225 - $600
Securing LAN server (1)	2 - 4	$150 - $200
Securing Internet server (web, ftp, mail—if used)	4 - 8	$300 - $400
Securing low-end router/firewall	0.5 - 4	$50 - $200
Testing configurations and resolving problems	2 - 3	$150 - $150
Installation of lockable equipment cabinet	1 - 1.5	$38 - $75

Total (without Internet server):	8.5 - 24.5	$613 - $1,225
Total (including Internet server):	12.5 - 32.5	$913 - $1,625

In keeping with these, the time to configure a workstation or server is represented in two increments: less time for an experienced technician and more time for one who is inexperienced. Likewise, two hourly rates are used: $75 per hour for an experienced technician ($100 for router/firewall configuration) and $50 for a less experienced technician. The cost range is determined by multiplying the inexperienced technician's rate times the estimated completion time to arrive at one cost, then multiplying the experienced technician's time and hourly rate.

Take these figures as vague estimates only. Actual costs can vary greatly from this sample, depending on the factors listed above.

If all the major components are contracted to a vendor, the cost could easily range from $500 for a tiny library network to $5,000 for a "moderately sized" small library. The good news is that much of this configuration, if not all of it, can be paid for through grant funds.

Before we quit, let's return to the notion I mentioned earlier of paying up front to keep a service functional and save time, frustration, and money down the road. Let's assume the six-workstation, one-server configuration above costs $1,000 to secure. Is security worth the price?

Leaving the network unsecured might result in various attacks that could compromise the network server, leaving it unusable until someone can reconfigure it. That will take time and money. How many days will the automation server be down? Zero? Ten? Is it worth $1,000 to provide a reasonable level of assurance that it will remain operational? There are also other types of "attacks" involving illegal activities through a public workstation. This may result in the workstation being impounded as evidence in a criminal investigation. How long will it be unavailable? A week? A month? A year? Will the library be able to replace it?

When we look at the possible results of security breaches, the $1,000 cost of a security project appears well worth the money.

The Cost of Maintaining Security

Unfortunately, the cost of original implementation is not the only cost associated with securing a network. At the very least, operating systems installed on workstations and servers need to be updated periodically. So a good security program budgets ongoing costs for security administration and staff time for managing backups, monitoring anti-virus updates, monitoring server logs, and resolving small workstation issues as they arise.

Here is a partial list of "costs" the library may expect as part of its security program:

- Costs for training staff/volunteers in basic procedures for securing workstations or servers
- Staff time used in resolving minor workstation problems or arranging for outside technical support
- Staff time in reviewing security logs; alternatively, funds for contracting for outside monitoring of security logs
- Staff time in reviewing backup reports and automatic anti-virus updates
- Staff time in downloading and applying workstation and server operating system patches on a regular basis; alternatively, funds for contracting for operating system updates (costs may be $35-70 per hour, including travel time if required)
- Restricted services; patrons may be restricted from certain activities, such as using chat or e-mail facilities, or writing to a hard drive, floppy drive, or CD-RW drive

The Cost of Auditing Security

As we've discussed in previous pages, network security is a process. It also has scope. Some libraries will decide to implement security measures that other libraries have declined to implement. Each library is encouraged to examine its community, operating environment, budget, and other local funding constraints to determine the best course for securing its network. In many tiny libraries this may comprise just basic physical and server security and significant workstation security measures.

Regardless of the scope of its security project, the process needs an element of accountability. A *security audit* will provide this accountability. The library should consult with a network technician either before or during its deliberations to review the library's options and opinions regarding security. Once final decisions have been made specifying which measures to implement, and the implementation is performed, then an outside agency should be hired to audit the security implementation, based on decisions made by the library.

An audit will provide the library three benefits:

- The auditor can comment on the state of security without bias, providing an independent review of a contractor's work.
- The auditor serves as a failsafe; if a specific security vulnerability has been missed, the auditor provides a secondary resource to catch the omission and suggest implementation.
- The auditor will also serve as an independent party to voice concerns with the current implementation and make suggestions for future iterations of security implementation.

Unfortunately, like security implementation, the benefits are not gained inexpensively. There are four primary cost factors involved in security audits:

- the scope of and methodology used to conduct the audit
- number of servers, workstations, and network devices to audit, if included
- the vendor's experience level, which relates to hourly/daily fee
- and, the scope of methodology used to produce the audit report

Audits reports vary widely in their content and presentation. More information about reports and how security audits are conducted is presented in Chapter 4. For the purposes of this section we'll just say the more extensive the documentation, the higher the full audit cost will be.

Most tiny libraries with limited infrastructure can expect audit costs to range from $500 to $1,500 plus travel time and expenses, if any. Small libraries with larger numbers of workstations, and web-based access to the library catalog can expect costs to range from $1,000 to $3,000 plus travel time and expenses, depending on the extent and complexity of the network. These ranges are vague estimates only. Table 7 details some of the costs you can expect to incur for an audit of your library.

Add $200-$400 more if you would like to receive an extensive report.

From this table you should be able to determine the approximate cost of an audit for your library. You can get a better estimate of the audit cost for your particular library, but you'll need to develop a request for quote (RFQ) for the audit. We'll cover this and other audit topics in Chapter 4.

Table 7. Security Audit Costs

Audit Service	Rate/Cost
Experienced network/system administrator with little to no knowledge of public access or security issues	$300-$600 per day
Network/system administrator with experience in public access and security issues	$600 - $1,000 per day
Certified, experienced security administrator/ auditor	$1,000 - $1,500 per day
Basic audit of four to eight workstations, one to two servers, and physical (access) security	5 - 8 hours (one day)
Intermediate audit, including six to twelve workstations, one or two LAN servers, an Internet server, and network devices	12 - 16 hours (1.5 or 2 days)
Internet-based audit/probe of perimeter security	3 - 6 hours (0.5 or 1 day)
Detailed written report	2-4 hours (0.5 day)

Sample Budgets

In this chapter we've looked at the various costs related to building your library network, keeping it going month after month, implementing a security project and maintaining it, and having a security audit performed. We've looked at them in a disjointed fashion, however. I've included all the costs in two different sample budgets in Part III. One shows the costs as they may apply to a library having more infrastructure and having to contract out its maintenance services.

The second shows the minimum costs a tiny library can expect if the director locates a volunteer or other free source (such as the TANG technician from the regional library system office) for technical support and maintenance. This second budget also assumes that equipment replacement will be provided either through future grants or continual replacement through donated equipment approximately three years old (replacing each computer every two to three years). While maintaining a program of donations is time-consuming, it is nevertheless a valid means of sustaining services for a tiny library with very little operating budget.

For those who may want to use them, these budgets will be available in electronic form on the web site for the PDF version of this manual (see the reverse of the title page for the web address). The budget forms, provided in Word 97 format, may be edited in any way you like.

Summary

In this chapter we looked at the various costs related to developing and operating a computer network in a public library. We looked at costs in the following areas:

- Cost of Network Equipment
- Cost of Software Maintenance
- Cost of Network Services
- Cost of Equipment Replacement
- Cost of Securing the Network
- Cost of Maintaining Security
- Cost of Auditing Security

We also pointed out two sample network technology budgets for small public libraries. These are presented in Part III.

4

Auditing Security

The auditor's report was favorable. All except the last section. Internal LAN security had been tightened fairly well. As well as the library could afford, anyway. The web server was open to attack, however. The auditor had been able to access the Administrator account on the server. That was very bad.

The director wondered if the $300 he had left in the grant would be enough to cover the re-configuration.

Once your library embarks upon a program of network security, how do you know your resources are secured as well as they should be, or can be? Once your staff, or a contractor you've hired, has configured your network components for secure operation, how can you confirm that the job is done well? To what standard do you compare your security implementation?

If any of these questions have occurred to you, then you get bonus points for thinking ahead. These are pertinent questions that every manager should ask at some point in the process of installing, configuring, or securing her network. Taking the word of staff or a contractor when you can't verify the work yourself is risky. The best course is to hire an independent contractor, one who is knowledgeable in the basics of securing network resources, especially in networks providing public access.

A *security audit* is the process of assessing the various components and the operating environment of a computer network for vulnerabilities. The audit may be either casual or formal, superficial or detailed, onsite or conducted entirely over the Internet. An in-house self-audit can be conducted when the library employs technically trained personnel, but this is unusual. These audits work well in a security project where the library is assessing what security measures may need to be implemented. As a final audit, however, a self-audit loses the benefit of an independent, objective view.

In this chapter I present some of the issues surrounding security audits and contracting with an auditor to test the security implementation of your organization's network. I also propose three levels of auditing for small public libraries, by which the security of your network can be assessed. If you are able to contract for an audit, then these are many of the items your auditor will be reviewing. If not, then these points should provide you or your network administrator with a guide to use in conducting a self-audit.

Purpose of an Audit

In order to assure library staff and interested funding authorities that the library network's implementation meets some definition of "best practice," it is necessary to perform an audit of the configuration. *Best practice* does not mean perfect. As mentioned in previous chapters, it is impossible to create a perfectly secure network. That ideal would provide access to no users at all. Any walls that are built technologically can, in theory, be "vaulted" technologically. In public libraries and other small community organizations where funding for technology is extremely limited, best practice is amended to provide a configuration that is *reasonably secure* given the organization's determination of its acceptable level of risk.

In small public libraries, acceptable risk may be much greater than it would be, say, in a small non-profit community organization, where the loss of proprietary information or of personal information associated with community businesses or organization members is critical. So the determination of what is an appropriate level of security may differ from one organization to another. The audit provides feedback to the library director indicating whether the library configured security meets its determination of appropriate security.

Benefits of an Audit

Having created security goals for the library in response to developing its security policy, library staff and board members will have engaged in a reasonable discussion of the risks associated with offering public network services. The library will also have determined a base level of security it wishes to implement.

After hiring someone to configure the network to meet this level of security, the security audit will determine how well the security implementation meets the library's goals. The following list shows the potential results of a network security audit:

- It will point out problems or weaknesses in a network's configuration so that the library may address them.
- It will verify the work of a vendor or staff implementing measures to secure the network;
- It provides assurance to funding agencies that resources are protected as well as reasonably possible;
- It provides an independent evaluation of a library's compliance with a set of network security standards, lending both credibility to future requests for funding and justification for current spending.

Is an Audit Essential?

In short, no. At this time, there is no granting agency I am aware of that requires a network security audit as part of its technology grant. A few local funding authorities are just now beginning to implement security policies, and many have no security policy, so they are not yet concerned with audits.

However, without an audit it is impossible for the library to know how open to attack its network is. Therefore, the library cannot know how likely it is to lose the service of a workstation, a server, or other network device. Where no audit is performed, a range of scenarios may be present, but be unknown. Here is a list of extreme scenarios and their consequences:

- The network may be relatively secure and experience no attacks
- The network may be very insecure and experience no attacks
- The network may be very insecure, experience attacks, and lose all services

When the library has no knowledge of its network's degree of insecurity, it is much more likely that one of the following consequences will be realized:

- minor attacks, where library staff occasionally have to reconfigure equipment and/or software
- frequent or significant attacks, resulting in the library having to pay a vendor to reconfigure equipment and/or software
- more significant attacks, where the library loses access to a workstation or server until it is reconfigured; this may also include illegal activities where a workstation or server is impounded as evidence, in which the loss may be limited or permanent
- a major attack, where the library will lose all access to the Internet or to its catalog

Hopefully, these illustrate that without an audit the library will not have a proper idea of its network security risk. Therefore, the library director will have no means to budget adequately for annual network support and maintenance. If the library significantly under-budgets its need for network maintenance, it may be unable to have network equipment repaired or reconfigured. In most libraries, this is an unacceptable risk.

On the other hand, some libraries simply do not have the financial resources for an independent audit (grant resources are becoming available for audits, however). In this case, a self-audit is highly recommended.

A self-audit requires someone on staff or a volunteer to be familiar with securing the network in the basic ways mentioned in the *Network Security Checklist* included in Part III of this guide. The implementation chapters in Part II will help you learn what each measure means, but staff will need additional training to implement/audit these measures. One portion of the online component of this training series will provide this basic instruction. There are other network security training resources as well.

The Audit Project

Content

Security practitioners may each recommend different security measures to be implemented, depending on their background experience and knowledge of the library environment. Here are seven major areas I use to classify specific security measures:

- General Security
- Physical Security
- Password Security
- Hardware Security
- Server Security (operating system and server software)
- Workstation Security (operating system and security utilities)
- Perimeter Security

All of these may be evaluated in a network security audit. Not all of them, and not all of the measures described within each area, are appropriate in every environment. In addition, as mentioned previously, the library must decide what its acceptable level of risk is. By doing so, the library can determine the scope of its own audit.

One aspect of deciding which measures will be audited is whether the cost of securing a specific measure is greater than the cost of recovering from an attack resulting from leaving it unsecured. Where a specific security measure is not implemented, the library should provide written justification of its exclusion to the auditor. This informs the auditor of the parameters of the audit. While the auditor may suggest reasons for implementing such a measure, the library is the ultimate arbiter of what risks it is willing to accept.

Standard Security Measures

To our knowledge, there is no standard list of network security measures that can or should be implemented or assessed to ensure maximum security of a library's computer network. The only documents close to this ideal that I have discovered are the consensus documents from the SANS Institute (listed in the bibliography). To fill the gap and assist libraries with security implementations and audits, I have developed the *Network Security Checklist*. The measures listed in the *Checklist* are divided into three separate levels of network security in public libraries. These are presented in *Elements of a Security Audit* at the end of this chapter.

As more practicing library network administrators and analysts review the *Checklist*, it should become more of a standard, reflecting the best practice in public libraries. A copy will be maintained online with the electronic version of this manual. (See the reverse of the title page for the Web address.)

What an Auditor Might Examine and Test

There are a number of established methods for conducting security audits. Some assess the security of *all* aspects of the network. Some assess the security of particular components, such as just the security of the perimeter equipment (router/firewall, web server) connecting the network to the Internet. In the business world, managing staff accounts and Internet-based attacks draw the most attention, but these are usually not the primary concern of most libraries.

There are three common types of audits. Each uses very different techniques.

- The *automated* audit. This type of audit involves the use of commonly available network scanning and assessment tools, usually onsite, to check a network for known vulnerabilities in operating systems (such as Windows NT Server, Linux, etc.) and in the network configuration itself. If no other techniques are used, this type of audit has limited usefulness for libraries. The audit report may consist mainly of printouts from the scanning utilities.
- The *black box* audit; also called a *penetration study*. It gets its name from the bad guys who may be trying to break into your network. In this scenario an auditor will be located outside the library and do his testing of the library's firewall and/or router configuration over the Internet. The auditor may or may not have any information regarding the library's internal network, but any information he has will be basic, such as a range of IP numbers representing the workstations or servers on the network. Because everything is hidden from the auditor, he must discover details about the network independently, just as a cracker would. Only minimal information is provided in the auditor's report through this type of audit.

  A problem with this approach is that it may not provide an accurate evaluation of the organization's actual perimeter security. It depends to a large degree on the auditor's skill in breaking into private networks. If the auditor is unable to breach the perimeter security, it tells you only that his skill is not sufficient to break into the network, not that the network is secure. On the other hand, a breach of the perimeter—especially if the auditor is able to become Administrator, or "root" (gain the privileges of the all-powerful super-user on the system)—indicates a major vulnerability. Such a breach is usually demonstrated by planting an innocuous file or program on a server or adding a new user account with administrator privileges.

Another problem with this approach in libraries is that it ignores a much more prevalent threat: the local user who accesses the network daily via a local workstation. Having great perimeter security may not preclude very bad things from happening from within the library.

- The *white box* audit; sometimes referred to as a *manual* audit. This audit requires an onsite visit and includes an examination of many more aspects of network security, resulting in a more thorough determination of the library's actual security implementation. It may make use of automated scans, but will also feature manual analysis of the physical and logical network configuration, the building, the configuration parameters of equipment, servers, and workstations, and the documentation that serves as a foundation for the site's security, comparing the implementation against "best practice." Therefore, the auditor must be given access to most, if not all, of the library's network configuration information, including staff account and administrator passwords.

  The purpose of this audit is to learn as much as possible about the level of vulnerability in the network configuration. The report provided through a white box audit usually describes the auditor's tests and findings in detail, and, therefore, it is the most helpful of the report generated through an audit. Expect the audit cost to include time to produce the report.

Specific items that could be included in a manual audit are listed in *Elements of a Security Audit in Public Libraries* later in this chapter.

Information an Auditor Needs

The scope of the audit, as described above, will require the auditor to have access to differing levels of information. The information may be public or very sensitive information. I recommend asking the auditor what he or she requires soon after a contract is signed. The library may need some time locating and packaging the materials requested. The auditor may need some time to review the materials after receiving them prior to an onsite visit.

Here is a list of the items most likely to be requested by the auditor for reference prior to or during the security audit:

- Network diagram (installer should have supplied one)

- Network addressing documentation (installer should have supplied one)
- List of hardware and software passwords
- Documentation for the servers/workstations/network equipment used in the library's network
- Various policies and plans, if available (and just having a document formally drafted may be one item of the security audit):
  - Security Policy
  - Acceptable Use Policy
  - Password policy
  - Backup plan
  - Budget plan, or technology plan with budgetary information
- Training documentation:
  - Network equipment and software configuration procedures (staff use)
  - Strong password selection (staff and possibly patrons)
  - Basic use of workstations (patrons and staff)
  - Basic security of sensitive information, such as passwords (staff)

Responsibilities

When the library hires a security consultant to perform an audit, especially an onsite, manual audit, there is some risk inherent in providing access to confidential and sensitive network information. The auditor will have access to an administrator account and passwords, as well as access to sensitive documents, such as personnel records or patron information. Therefore, it is a good idea to have a non-disclosure agreement (actually, a disclosure agreement, limiting what will and what will not be disclosed) indicating the responsibilities of the auditor and organization in detail.

First, the library must agree to disclose all of the information required by the auditor to access system and network resources during the audit. This information will provide the auditor with a basis from which to perform a thorough inspection and audit of the network. Lacking information such as an administrator's password may prevent the auditor from accessing portions of the network which need to be evaluated.

On the other hand, the auditor must agree not to disclose to any other party any of the information she is provided for purposes of the audit, or any information she accesses/discovers during the course of the audit. Any such disclosure can be considered a breach of security. The auditor, however, may need to disclose some information in specific instances to another person in her organization, so her firm—and not just the specific auditor—should be bound under this area of non-disclosure.

Sound security practice (some may call it paranoia) suggests that an agency undergoing an audit should change all significant passwords (for administrator accounts) immediately after the auditor concludes the final onsite visit. When changed, the new passwords should be created with strong password guidelines currently practiced or suggested for practice by the auditor.

In addition to the disclosure agreement signed by the auditing firm, it is also a good idea for the library to have a similar written agreement with the firm it uses for installation and/or maintenance of the library's network equipment. [**Note:** *The vendor responsible for installation and configuration must agree to provide to the library the specific passwords used to configure or administer each piece of equipment (hub, switch, router, firewall, etc.).* In several cases in the past, vendors have withheld these passwords from library staff, causing the library difficulty in trying to change vendors for maintenance and expense in trying to solve configuration problems.] The signed agreement should also include a statement that the vendor will not disclose such information to any third party.

Likewise, the library has responsibilities in this regard as well. The library must agree not to disclose the nature of passwords and other configuration information used by a vendor, because the vendor may use similar devices in the creation of passwords for other agencies. This is not recommended from a security standpoint, but may indeed occur. By disclosing the library's password to some other agency or library (third party), the library may inadvertently give someone a "head start" in breaking into another agency's network.

A final responsibility of the auditor will be to schedule the time at which an onsite visit will be made. In some cases, the audit may interrupt ordinary operation of the network, and the audited agency needs time in advance to prepare for the possibility of an outage. For example, especially in public libraries, public access workstations may need to be reserved for the auditor's inspection, leading to "downtime" for the library's public access service.

Project Deliverables

The primary product of a network security audit will be the auditor's report. In businesses there may be a formal presentation of findings as well, providing business representatives an opportunity to ask the auditor questions. Such presentations require time to develop, time to travel back to the business, and time to make the presentation. All this increases the final cost of the audit. Most libraries would be better served to receive copies of the report and have an opportunity through e-mail or a phone call to resolve questions arising from the report.

Be aware that some audit reports are mainly printouts from automated network scanning utilities. While these may be extensive, their content may be unhelpful. At the other extreme are complete custom documents detailing the state of security on each system, including areas of weakness in each system, with a list of recommendations for further implementation. Such documentation is very helpful, but is expensive to produce.

Selecting an Auditor

Qualifications

Network security auditing in small organizations is still in its infancy. There are very few practitioners who are certified security professionals. Therefore, determining a vendor's qualification to conduct the audit is based on several evaluative factors:

- Does the consultant or vendor possess a knowledge of general security principles ("best practice") commonly used in the library's network operating system?
- Does the vendor possess a certification for the operating system used in the library's network (e.g., MSCE for *Windows NT/2000*, RHCE for *Red Hat Linux*) or for the network devices installed (e.g., CCNA for Cisco switches and routers)? For operating systems, it is important to realize certification measures basic of knowledge of an operating system at one point in time—it does not guarantee (and, in fact, indicates very little about) knowledge of common security practices used with the operating system. Microsoft now requires students to pass a security unit for its Windows 2000 MSCE certification.
- How trustworthy is the consultant or vendor? Whoever performs the audit will have complete access to your systems, so trust in the vendor is crucial!

- Does the consultant or vendor have experience with network security in a public access environment, especially in small public libraries?

There may be other vendor qualifications or characteristics that are important to your library. For example, the hourly/daily fee a vendor charges is a primary consideration for most small public libraries. If you develop a Request for Proposals (RFP) or Request for Quotes (RFQ) for the project, be sure to ask responding vendors for references of other clients, particularly any public library clients. Ask the RFP/RFQ respondent to describe her experience with security in a public access environment. Also ask her for a generic copy (with all client references and any sensitive information removed) of a report or two from a similar audit she performed previously. Evaluate each vendor responding to the library RFP or RFQ based on these characteristics and documents.

Formal Process

The security audit is really the last step in implementing a network security project. So a number of preliminary steps is assumed:

- Research the various aspects of security in a public library setting.
- Meet with a system administrator or a network vendor representative to discuss the possible costs of implementing various security measures and the risks incumbent in not implementing each.
- Review the costs and risks to determine which items of network security are required in your library and which risks the library is willing to accept.
- Contract for the security implementation.

Given the security implementation, there is a separate process required to conduct a network security audit. Here are the major steps:

- Create a list of the security measures implemented, which then becomes a list of items to be audited; include written documentation of the library's decisions not to implement specific measures.
- Develop a Request for Proposals (RFP) or a Request for Quotes (RFQ) for the security audit, including the measures to be audited.
- Review the draft RFP or RFQ with the library board and with regional library system staff familiar with network security in public libraries.

- After the final RFP or RFQ draft is approved and formally produced, submit it to three or more likely/suitable vendors and advertise it.
- Evaluate responses to the request, with an eye toward the characteristics presented in the previous section.
- Follow up by contacting the references provided by the respondents.
- Award the audit project to the appropriate vendor and arrange an onsite visit.
- Gather all relevant network documentation (especially passwords, plans, and policies) requested by the auditor and deliver as agreed.
- Conduct any onsite and Internet-based assessments.
- Once the auditor has completed his or her assessment, *change all administrator-level passwords* (see the *Sample Password Policy* in Part III for help in creating strong—not easily hacked—passwords. This may seem paranoid, but this is very sensitive information about your network. Believe it or not, some hackers even have day jobs as network consultants! (Okay, maybe I got a little enthusiastic again, but do change those passwords!)
- Review the audit report to see if any specified areas of network security require more implementation work; review any additional comments or recommendations the auditor may include in the report and determine their appropriateness to your library's needs.

Elements of a Security Audit

In the following tables I present three levels of security a small public library may choose to implement and have audited. The lists are creatively labeled *Basic, Intermediate,* and *Advanced.* They are cumulative. To secure a network at Level Two, everything in Level One must be implemented as well. The items listed in each level are taken from the *Network Security Checklist* and categorized according to the top ten threats identified in Chapter One. They are listed in order of expected cost, from the least to secure to the most expensive.

The lists may not completely represent your library's needs, but are intended to be a starting point. Feel free to delete or add specific security measures from other levels as library administration deems appropriate.

Table 8. Level One. Basic Audit. Foundational Items

Threat, Expense Order	Related Checklist Items
Local users cracking passwords	3-3, 3-4, 5-6, 6-10, 6-11, 6-13, 6-14, 6-15, 6-16, 6-17, 6-18, 6-19, 6-24, 6-25, 7-1 If web server used, add: 9-10, 9-11, 9-16, 9-17
Electrical damage to equipment	2-9, 2-10, 4-13, 4-14, 4-15
Internet-based attacks of internal network resources	Viruses: 5-15, 5-16, 5-17 8-1, 8-4, 8-5, 8-6, 8-8
Local patron tampering with workstation desktop and hardware settings	4-1, 4-2, 4-3, 4-4, 4-5, 5-7, 5-8, 5-10, 5-18,
Unauthorized access to workstation file systems	5-1, 5-2, 5-4, 5-9, 5-12, 5-20
Unauthorized access to server file systems	4-8, 6-1, 6-6, 6-7, 6-20, 6-21, 6-22, 6-23, 6-36
Tampering with local network infrastructure	2-2
Defacement of web pages hosted on library-based web server	if web server used: 9-1, 9-2, 9-3, 9-4, 9-5, 9-6, 9-7, 9-8, 9-10, 9-11, 9-13, 9-14, 9-16, 9-17
Other	Privacy: 5-5; Monitoring access: 6-12, 6-29, 6-30, 7-3, 7-4; Update equipment firmware: 7-5; Data safety: 6-31; Store equipment passwords: 7-2

Table 9. Level Two. Intermediate Audit. Greater Security

Threat, Expense Order	Related Checklist Items
Local users cracking passwords	1-7, 1-9, 3-1, 3-2
Electrical damage to equipment	2-8, 2-11
Internet-based attacks of internal network resources	5-3, 6-4, 6-5, 8-2, 8-3, 9-9, 9-15
Unauthorized access to workstation file systems	1-4, 1-5, 1-6, 5-11, 5-14, 5-22
Unauthorized access to server file systems	6-2, 6-27, 6-33, 6-38

Tampering with local network infrastructure	1-8
Theft of equipment	1-3, 2-1, 2-5, 2-12, 2-13, 6-32, 6-34, 6-35
Inadequate funding	1-1, 1-2
Other	Minimize tech expenses: 2-6, 5-19, 5-21, 5-23, 6-28, 6-39, 7-6, 7-7, 8-7, 8-9, 9-12, 9-18; Minimize expense: 6-37; Boot up settings: 4-9

Table 10. Level Three. Advanced Audit. Best Security

Threat, Expense Order	Related Checklist Items
Internet-based attacks of internal network resources	10-1
Unauthorized access to server file systems	2-3, 2-4, 5-13, 6-8
Tampering with local network infrastructure	2-7
Theft of equipment	4-11, 4-12
Other	Minimize tech expense: 4-10, 10-2, 10-3; Maximize uptime: 6-3; secure against dial-in attack, if applicable: 6-26

Summary

In this chapter we looked at various aspects of network security audits. These include:

- Purpose
- Benefits
  - Knowledge of unsecured vulnerabilities
  - Verification of a vendor's security implementation
  - Assurance that a library is doing all it can to secure its network infrastructure
- Is an Audit Essential
- What Security Measures Should be Included in an Audit
- What an Auditor Might Examine in the Network

- Just the publicly available computers (router, web server, and possibly public workstations)
- Tests for known vulnerabilities
- Comprehensive review of security practice including access control on workstation and servers
- Review of administrative process, including policies, plans, and procedures

- ♦ Information an Auditor Needs
  - Network documentation and passwords
  - Equipment documentation
  - Copies of policies, plans, and procedures
  - Copies of training documentation
- ♦ Responsibilities of the Library and Vendors
- ♦ How to Select an Auditor
  - Qualifications
  - Formal Process
- ♦ Elements of a Security Audit
  - Three levels: basic, intermediate, and advanced

5

Training Users

"Mary, are you telling me you didn't know chatting is against the rules?"

"Yes, ma'am," Mary replied, sounding very contrite.

"But you read the acceptable use policy?"

"Yes, ma'am."

In exasperation, the library director pulled a copy of the AUP out of the acrylic stand of training brochures sitting just to the right of the monitor. She opened it and spread it out on the desk in front of Mary, putting her index finger below the bold-faced letters.

"You didn't see these statements in bold-faced type?"

"No, ma'am."

"How do you explain that, Mary?"

"Maybe it got updated sometime after I read it?" the girl offered hopefully.

You've taken the time to learn about dangers lurking around your network if you don't secure it. You've done some planning and created a security policy, working it in with your Acceptable Use Policy where applicable. You've identified the security measures most likely needing implementation on your network. You've hired someone to come onsite and implement those measures. You've arranged for a security audit. Seems like you're close to being able to go home and get a good night's sleep.

What's left?

Just a little training.

Content

Security training isn't like learning a software application. It's not like learning to sew or ride a bike. It's not a step-by-step thing, and it's not skill gained by repetition or judgment. Security training is more a process of familiarization. After determining security goals in your security policy and listing the rules of use, it's time to impart these to your staff and your patrons.

Staff Rules & Guidelines

Be sure that everyone on staff is familiar with the rules and procedures that apply to their positions. For example, make sure the person in charge of system backups understands:

- how to operate the backup software
- the procedure related to rotating backup media (e.g., which Friday tape is to be used next, or when to take a tape offsite)
- how to review the backup log the morning after each backup and remove the tape
- report any problems
- schedule and conduct a test restore 2-4 times per year

In these cases, training the person also means checking their work occasionally to make sure it is done as specified.

The remainder of the training relates to the sensible guidelines of making sure sensitive information isn't inadvertently compromised. Here are common guidelines taught to staff members.

- Always log out from the server when finished performing administrative tasks. Lock the console if necessary.
- Those staff members who know the Administrator password should log onto their workstations using their personal accounts unless the task they are performing specifically requires Administrator privileges. (Always assign each staff member and volunteer a personal account with appropriate privileges for routine use.) They should log off immediately after completing the task(s) requiring Administrator privileges. Further work can be done after logging back in under their personal accounts.

- Do not log onto the Administrator account from a public workstation.
- When logging on as Administrator, be sure no unauthorized persons are observing.
- Keep passwords secret. Since everyone is assigned a personal account, there is no need to reveal personal or system passwords to anyone. This especially includes technicians or competent-sounding phone callers. Staff must obtain approval from the library director or his/her designee before revealing passwords or other network-related information to a representative of a computer company arriving at the library to do tech work.
- Keep network configuration information (IP addresses, for example) confidential. Obtain approval from library administration before revealing such information to any third party.
- Create strong passwords, as specified in the Library's password policy (see Part III for an example), when creating or changing passwords.
- Memorize your password. If it's a password you may forget, write it down on a sheet of regular paper (with no reference to the account it corresponds to) and store the sheet in an innocuously labeled manila folder and file it.
- Do not use credit cards to purchase products online with any library computer.

Public User Rules & Guidelines

Rules and guidelines are generally different for public users of your network. If your library offers individual accounts to patrons (not many do at this writing), the first two items below should be included; otherwise they can be deleted. Most of the other items are warnings about using the Internet safely in a public environment.

- Keep your account password secret. Since everyone is assigned a personal account, there is no need to reveal your password to anyone.
- When changing your password, create a strong password as described in the Library's password policy.
- Be cautious about submitting personal information to sites on the Internet; personal information submitted as part of a web-based form

may be stored on computer's hard drive in the form of a "cookie" and the privacy of such information cannot be guaranteed. Never use a credit card to purchase products online from a library computer.

- The following services are not available through the Library's Internet connection (include a list of these services, such as chat and e-mail use)
- Read the following documents (list preferred web sites or library materials here), which describe safe practice in the use of Internet resources.
- When you complete your Internet session, exit the web browser to clear the browser's cache, history, and URL lists.

Monitored Use

In order to maintain a secure network, it is important to monitor specific user actions on the network. Monitoring specific patron use of resources is not often done in libraries. It has been important in our work to assure patron's privacy in regard to their use of materials. In the case of computer networks, however, it is necessary to strike a balance between the patron's right to privacy and the library's right to protect its resources for the use of all patrons.

Part of the library's security program is to determine what specific actions or activities should and will be monitored. The program must also determine the procedures used to monitor these activities and how violations of policy will be reported and resolved. When these decisions are made, it is then imperative to inform staff and public users how their usage will be monitored.

The library is encouraged to include a disclaimer providing details related to the monitoring of network activity on all training materials, acceptable use policies, and other public documents. (A sample statement is included on the next page; it is provided for illustrative purposes only. Be sure to have the library's legal counsel review and approve all such statements before adopting them for use.) The disclaimer works in tandem with the custom logon banner recommended in the *Network Security Checklist* (a sample is provided in Chapter 8 on pages 98-99) to notify patrons that not all uses of the network are anonymous or welcomed.

> ***Use of the Library network is a privilege, not a right.*** *All network activity is monitored for illegal and unauthorized use. While the Library keeps no permanent records of particular materials viewed by patrons, any attempts to access restricted services are noted. The Library reserves the right to refuse service to anyone engaged in illegal or unauthorized activity as specified in its Security Policy and its Acceptable Use Policy.*
>
> *Specifically, the following actions are monitored:*
>
> - *all attempts to access the Administrator account*
> - *attempts to access restricted areas of the network server or local workstations*
> - *attempts to copy unauthorized software or utilities onto a server or local workstation*
> - *attempts to run unauthorized software or utilities stored on a server, a local workstation, or on a personal diskette*
> - *public workstations are configured to operate without providing access to a "command line" (also called a DOS session). Patrons observed running a DOS session will be considered to be running unauthorized software.*
> - *Other actions (as they are identified) harmful to the provision of network services to all patrons.*
>
> *When confirmed by library staff, unauthorized attempts to access restricted resources, whether successful or unsuccessful, shall result in loss of privilege as indicated by policy.*

There may be other activities that need to be monitored. However, given the library's need to protect its patrons' privacy in their use of resources, such activities are anywhere from difficult to impossible to monitor. These activities include, but are not limited to:

- sending threatening or harassing e-mail to others,
  - to the President of the United States (possible)
  - to any prominent person (very difficult)
  - or any other Internet user (next to impossible)
- using chat or other multi-person communication resources in an illegal way (almost impossible)
- breaking into government or banking networks (difficult)

If these activities are an extreme concern, the only common, practical method for most libraries to use in restricting them is filtering software, although it is also possible to limit access through the router, firewall, or ISP's connection. For many libraries this is an untenable solution.

Timing

Like most training, staff and patrons need to be taught these guidelines and rules of conduct as soon as the network is functional. This means planning an orientation session and software training. Optimally, the training plan needs to be developed well before the network implementation.

If the network is already operational when security topics are addressed, an orientation and "re-certification" of user access is recommended.

My recommendation is to conduct a short staff and volunteer orientation session first, explaining the terms of use of library computers and the network, allowing questions to be asked and issues to be raised. Basic training in the use of any new software can be conducted separately.

For public users, the orientation session and software training can be combined and be presented in small groups at scheduled times.

Part II

Implementing Network Security

6

Overview of Implementation

In this portion of the manual, we turn our focus from the management aspects of network security to actual security measures to be implemented. As a manager, your interest will be in understanding how these impact your library's network security rather than in how to implement them. So, in the following chapters, I describe the various security measures specified in the *Network Security Checklist*.

Need for a Standard

This *Checklist* is submitted as a candidate for a *standard* list of items public libraries need to evaluate in securing their networks. I have asked other librarians familiar with both the limitations of staff and financial resources in small public libraries and with the technical requirements of computer networks to review the *Checklist*. Although it is not a definitive guide to best practice for network security in the small public library, as more and more systems librarians (and others) review it, it will become more of a standard of practice.

It is important to realize that not every item on the list will apply to every library. Each item on the list has a specified level of implementation, either Mandatory, Recommended, Optional or Not Applicable. This last classification indicates that each library needs the freedom to review an item—even one considered by some to be mandatory—and determine that the cost of implementing it is greater than the consequences of leaving it unsecured.

Therefore, I encourage the library to seek the help of a knowledgeable professional to discuss and evaluate each of these items for appropriateness in the local library's environment. This will help ensure the library's funding for security is spent to reduce the threats that are most likely to materialize in each particular library environment.

Division of Security Issues

I divide the realm of network security in libraries into seven main categories: physical security, password security, hardware security, server security, workstation security, perimeter security, and financial security (this area is most important in small community organizations where the operating budget is severely constrained). These areas are expanded in the *Checklist* by separating out specific configuration issues related to web servers and general administrative issues related to budgeting, planning, and policy development. In addition, the perimeter security area is expanded into separate router/firewall and virtual private network sections.

Therefore, there are ten sections in the security checklist:

1. General security
2. Physical security of computers and network equipment
3. Password security
4. Hardware security
5. Workstation security
6. Network server security
7. Network equipment security
8. Router/firewall security
9. Web server security
10. Virtual Private Network Security

Chapter 7, *General and Physical Security*, includes the description and the need to secure the items in Sections 1 and 2.

Chapter 8, *Local Area Network Security*, describes the items in Sections 3 through 7.

Chapter 9, *Perimeter Security*, covers Sections 8 through 10.

7

General and Physical Security

Alec Strauss (no kin to Levi, unfortunately) looked around the room. He felt a sick emptiness spread through his stomach, matching the bare desktops all around the lab. Every workstation was gone. The thieves had even taken the power cords and surge suppressors. They were thorough. He'd give them that.

Wondering where it would all lead, he went back to his office and dialed the city manager's office, according to the city's policy. He wondered how many training classes he'd have to cancel before any new equipment arrived.

This section recommends the development of various planning documents that help a library understand the fiscal and service requirements of maintaining network infrastructure and network-based services. For tiny libraries, the cost of maintaining and eventually replacing system components is very high. Having a written plan indicates the library is aware of the financial challenges that threaten to wreck its network-based services. The planning documents also include backing up data and making staff and patrons aware of their responsibilities in using network resources.

This section also suggests areas of staff training to prevent a process formally called *social engineering*. This phrase describes a ploy where an unauthorized person contacts a library staff member (usually over the phone) and pretends to be someone official: a technician with a company that provides technical support of the network, someone from the phone company, or a representative of another vendor. The attacker tries to gain sensitive information, such as usernames or passwords, to be used later to break into the network.

General Security

Budget plan and budget line items for equipment replacement

Computer equipment (servers, workstations, network devices) must be replaced or upgraded within reasonable timeframes to keep the network functional. So the library must address the issue of equipment replacement. In many cases, upgrading memory or adding a hard drive can prolong a computer's life. However, once a workstation gets to be four to five years old, its processing power diminishes in relation to the requirements of newer software. At some point upgrades are no longer practical. In a tiny library with four to six public access workstations and a staff workstation or two, replacing workstations even just every five years may place a severe burden on resources. To illustrate the costs involved, I have included sample budgets in Part III.

Proper forecasting of future equipment costs is imperative. A budget plan is a document in which the library director and board have made an effort to identify (through a three-to-five-year budget) all of the cost factors associated with computer and network technology in the library. The budget plans will take into consideration these costs:

- Annual maintenance and repair of computer equipment
- Annual maintenance of network configuration, administration, and maintenance and repair of network devices
- Annual operational costs for the network
- Periodic replacement of computer equipment

The budget plan may also include specific levels of funding from various potential sources of funding, such as the local budget, local and regional fundraising, grants, donations, and others. A well-developed budget plan will help the library forecast current fiscal year costs and prepare budgets for future grant applications.

Data Backup Plan

To properly protect the data created, used, and transmitted over a computer network, a backup plan is needed. (*Note:* I use the word backup here in a general sense, so it can include the process of creating a disk image and copying it to an alternative location—also known as "ghosting"— as well as the traditional procedure using a tape drive.) A *backup plan* is simply a document describing how data created and used in the library will be protected. The plan describes these concepts:

- How often each workstation hard drive (staff and/or public) needs to be backed up
- How often each server hard drive needs to be backed up
- The backup process: medium used (tape, CD-RW, network hard drive), schedule, and person responsible for management
- Rotation of backup media
- Security of backup media
- Response process in the event of equipment failure, damage, data loss—how data will be restored

Securing Use of Network Services

There are three main aspects of network services that need to be secured in a public environment:

- Data (integrity and availability)
- Privacy (patron transactions and use)
- Equipment (physical availability)

In order to review and analyze the library's need to implement specific measures to protect these aspects of network services, additional administrative documents need to be developed. The *Network Security Checklist* specifies the following required documents as part of securing network-based services in our libraries:

- Security Policy; as described in Chapter 2, an overarching document describing the various rights and responsibilities of all users of the network: staff, patrons, and contracted vendor reps.
- Acceptable Use Policy (AUP); developed for patrons and staff; includes consequences of misuse of equipment or services
- Security Plan; describing the decisions made by administrative staff related to security configurations of all network equipment and software. The security plan should document the decisions made in determining which security measures are appropriate for implementation in the library.

Securing Sensitive Information

One of the most important components of network security is having staff that is knowledgeable in proper procedure. Staff should be told when maintenance personnel or contract technicians will be onsite to work on the network. Staff should be trained in the proper formation and use of passwords. Staff should be trained to be suspicious of callers requesting information over the phone about the network. Here are several training items necessary for good network security:

- Train staff not to reveal system passwords to anyone other than specified contracted technicians having prior authorization
- Train staff not to allow anyone access to systems and network equipment without prior authorization
- Require companies performing maintenance/configuration to sign a disclosure agreement: *to disclose all configuration parameters (especially passwords) to designated library staff* and *not* to disclose library network configuration information to any third-party without prior authorization.

Any written or verbal contract with a network services vendor must include a requirement that all passwords created for network resources be provided to the library director. Documentation, especially of router and firewall configurations, must also be provided in electronic or print form. Additionally, the contract should also restrict the vendor's disclosure of that information to any third party without prior approval of the library.

Physical Security

In businesses, most of the physical components of a network are housed in a separate room, which may be called a computer room, telecom closet, data center, or other descriptive term. The room is locked and accessible only by authorized personnel. This physical isolation protects much of the equipment from unintended access and from electrical anomaly. However, libraries seldom have the luxury of such accommodations. Therefore, special attention must be paid to the following areas of physical security.

Isolating access to equipment

Momentary access by an unauthorized person may result in lost data, altered data, altered equipment configurations (having a wide variety of negative results), physical damage or theft of equipment, or even the disclosure of private information. Here are some recommended physical security measures for public libraries:

- Dead bolt locks installed on all building entrances/exits
- All servers and network equipment housed in a staff-only area, preferably locked (alternatively, in a locked equipment cabinet)
- Data cables/data jacks (public areas) secured from patron access, if possible

Installing dead bolt locks on all entrances/exits is essential in providing simple protection of expensive equipment. It creates one more small fence a thief has to climb. Putting the network equipment in a room locked during business hours will prevent casual access to the equipment by the public. In the event that network equipment must be housed in a publicly-accessible area of the library, putting the equipment in a locked equipment cabinet provides the same protection, along with protection against minor mischief (like unplugging network cables) and small component theft.

Isolating access to disks and tapes

Whereas items in the previous section protect access to equipment, these items are required to secure access to critical system data files.

- Locked storage for backup media, system recovery disks/CDs, and Emergency Repair Disks
- Rotate one backup set offsite regularly and store in a secure location
- Store backup of router, firewall configuration file, if applicable, in a secure location
- Keys used in securing equipment or media are stored in a controlled location

Backup tapes or other media need to be stored in locked cabinets or boxes. The same is true for any system recovery disks/CDs supplied by the manufacturer, Emergency Repair Disks created after a Windows NT/2000 system is installed or re-configured, and any configuration files for router and firewall equipment.

Both backup media and recovery disks usually contain data that, if accessed by a malicious person, could result in the compromise of your network. For example, backup tapes and recovery disks may contain a copy of a network server's password file, and if an attacker obtains a copy of this file, he may be able to crack the Administrator's password and break into the network at will. All he needs is to "borrow" the media overnight.

Access to the keys for the locked storage containers or cabinets obviously must be controlled as well. The library director and one assistant (usually the person specifically assigned to maintain network security) should know the location of the keys so that only authorized users have access to the media.

Protection from Electrical Problems

Besides theft and unauthorized physical access, damage or corruption of data due to electrical problems may be the second greatest danger to a library's computer and network equipment. The following checklist items provide a minimum level of protection against electrical surges, and even lightning strikes. The following items are required:

- Electrical system inspection for adequate building power capacity, breaker box, and independently grounded electrical circuits (dedicated circuits suggested for PCs; ground suggested for equipment racks)
- All workstation power cords connected to surge protectors meeting UL1449 330V standard
- All server and network equipment power cords connected to UPS(es), with surge suppression meeting UL1449 330V standard
- All modems physically connected to phone lines are surge protected
- Outlets on dedicated circuits are colored fluorescent orange

Before adding more computer equipment to your library, it is important to have an electrical inspection performed. In the inspection, the electrician will ensure that the building's power infrastructure is adequate and appropriate for computer use. Installing different colored plugs for dedicated outlets provides an easy means of identification so library staff can be trained not to plug other electrical devices (copiers, vacuum cleaners, and others) into outlets designated for computers.

Miscellaneous Items

- Serial numbers and physical asset numbers (if applicable) are recorded for all workstations, servers, and network equipment
- Insurance coverage against damage or theft

These items just make good sense. Be sure to record the serial numbers for all computer and network equipment. Serial numbers may be needed when repairing equipment or to identify equipment in the unhappy event of a theft. Asset numbers are used by many governmental and business organizations as tracking numbers and ownership stamps. Make sure these are recorded as well.

If possible, protect your equipment against theft or damage, either electrical or physical, by insuring it. Any insurance policy for computer or network equipment should specify replacement value—rather than fair market value—in its terms and provide coverage for electrical or accidental damage. It is also a good idea for insurance purposes to make a digital photograph or video recording of the equipment, including the area where the serial number and asset tag are located.

8

Local Area Network Security

He had never really thought about it, but now that he was seeing it, he couldn't believe it. Jonesy (it wasn't his real name, but the persona he assumed when he was on the Net) looked at the data jack, mounted in the wall above the desktop. What a blessing from the Muse of things electronic!

Shielded from direct view, he quickly disconnected the cable from the workstation, connected the cable from his laptop, and went to work. He wouldn't even have to reconfigure his network settings. The DHCP server would automatically connect him. Maybe next time he'd choose another host name in case they were auditing logons. In under a minute he was in.

What he had was an untraceable connection. The Internet stretched out in front of him like the wide-open spaces before a Porsche. He figured he had thirty minutes before he had to start looking to disconnect and get out gracefully.

Password Security

Undoubtedly, the least expensive and most important aspect of network security is the use of appropriate passwords. Password protection is inherent in various aspects of the network:

- Administrative access to server functions
- Workstation access to various files and services (such as the Internet)
- Administrative access to network hubs, switches, routers, and firewalls

- Access to administrative files, such as confidential personnel files or reports

Yet, given its importance as a foundational aspect of network security, ironically it is often the least emphasized. Password security includes the following facets: selection, documentation, and enforcement. Creating and implementing a password policy is the first step in developing password security (a sample password policy is included in Part III). The policy will outline the rules about creating good passwords, called *strong* passwords in most security documents: the minimum number of characters to be used, what types of characters, how often the password needs to be changed, and others aspects of password usage. Here are the checklist items related to password security:

- Develop written password policy and provide to all staff and patrons using specific user logons
- Develop written instructions in creating strong passwords and provide to all staff and patrons using specific user logons
- Document passwords for all network equipment, servers, and workstations
- Store password documentation in secure location known only by library director and one other person

In addition to developing the policy, it is important to develop training materials for your staff. If your library provides user-specific accounts for your patrons, the training materials should also be distributed to your patrons. Make sure all administrative passwords are written down (yes, write them down, but not on post-it notes stuck to your monitor!). Just like the keys to locked storage, the passwords need to be stored in a secure location known only by the library director and one other staff member.

Hardware Security

Hardware security is a convenient category used to classify miscellaneous items related to your computer and network hardware. The first set of items relate to the BIOS (the Basic Input/Output System) of your servers and workstations. The BIOS is a well-known feature on all Intel/AMD PC-compatible servers and workstations. It performs basic tests of internal components to be sure they are working satisfactorily. It also stores and manages the configuration of many of the parts inside the CPU case.

- BIOS: *workstation*: boot order, set primary hard drive first
- BIOS: *server* (locked staff only access): boot order, set floppy drive first
- BIOS: *server* (when locked staff-only access is not possible): boot order, set primary hard drive first
- BIOS: *workstations*: supervisor password set
- BIOS: *servers*: if servers can restart automatically with supervisor password set, set one (otherwise, leave with no password)
- BIOS: *all*: anti-virus protection enabled
- BIOS: *public workstations*: floppy drive(s) disabled if AUP specifies no patron access to floppy disks
- BIOS: *servers*: (when locked staff-only access is not possible): disable floppy drive
- BIOS: *public workstations*: setup message hidden/disabled, if option available
- BIOS: *all*: record setup configuration parameters

When a computer is working satisfactorily in a controlled environment—such as that locked computer room mentioned earlier—there is little need to worry about protecting BIOS settings. However, anywhere patrons have access to computers, even momentary access to them, there *is* a need to secure the BIOS settings. Obviously on public workstations BIOS security is a necessity. There is also a need to secure the settings on a server if it's located in a place where there is a possibility that a patron may gain access to it. Secured BIOS settings can easily be accessed by an administrator when needed for maintenance or reconfiguration.

The previous settings prevent the computer from being booted to a floppy disk that a patron might bring in—preventing the patron from having complete control of the system. They also prevent most of the mischief patrons may cause by making changes to the proper BIOS settings, such as removing the hard drive configuration.

- Servers and workstations: use small padlocks to secure case covers

- Public workstations (or all computers in a very insecure environment): secure CPU, monitor, keyboard, and mouse to table/desk with hardware security cables/devices

The danger of theft is a security risk with one of the highest negative impacts on network services in a public library (a lightning strike is another). A small investment in time and money greatly reduces the risk of many types of theft. A small padlock or other device will prevent patrons from removing case covers from computers and taking RAM modules or other internal components. (Some libraries enclose the CPU case in a lockable cabinet, eliminating the need for locks.) Vendors are available that supply steel cable systems to protect CPUs, monitors, keyboards, and mice from theft.

- All servers: protect with UPS (400va or higher), preferably having auto shutdown software
- Network equipment (hubs or switches) with UPS (250va or higher)
- Router/firewall: protect with UPS (250va or higher)

Data integrity is a concern when a server loses power. In addition to data corruption, there are other power concerns for networks. If the power goes off, circulation cannot be conducted and home-based users cannot use a web-based library catalog. [*Note*: if multiple servers are connected to one UPS, it should be rated at no less than 700va, and probably higher.] This configuration ensures small power interruptions will not disable critical services. For servers, be sure to load software enabling communication between Windows NT/2000 and the UPS. The software automatically shuts down the server in the event of a power failure, protecting data integrity.

Workstation Security

Although sometimes treated as a separate topic, properly securing workstations is a very important part of the overall network security in a library. There are a large number of configuration issues to address when securing workstations. Using the Windows NT Workstation/2000 Professional operating system provides a better security foundation than does Windows 98. Those libraries using Windows 98 on public workstations are highly encouraged to install special software to secure many of the workstation functions.

- Configure NT Workstation/2000 Professional partitions with NTFS file systems

Windows NT/2000, unlike Windows 98, includes a feature known as file system security. (An operating system's *file system* is the structure it uses to store data and program files, and includes two types of objects: *files* and *folders*—folders are also called *directories*.) A secure file system is one in which an administrator can configure any file or folder so only specified users can view or use those files and programs. The administrator controls access by associating specific user accounts with individual files and folders and assigning *permissions* to each account. The general permissions include the ability to read, write to, or execute a file or folder. A user with no read, write, or execute permission cannot access a file or folder.

In order to take advantage of this built-in security, the library must be sure the workstations are configured with the native NT file system (called NTFS) rather than the alternative, the older Windows 95/98 file system (called FAT or VFAT). Previous conventional wisdom indicated that the boot partition (known as drive C to most of us), ought to be formatted as FAT, but this is no longer true.

- Disable boot keys on Windows 95/98 workstations

Boot keys are only available in Windows 3.1/95/98. They are not available in Windows Me or Windows NT/2000. They allow the user to interrupt, or escape from, the normal Windows start-up sequence. Since they allow unrestricted access to the command prompt (the old "DOS prompt," C:\>), they provide too much opportunity for patrons to tinker with the system—perhaps even to reformat the hard drive. Utilities and manual instructions are available to disable these keys.

- Configure workstations with private IP addresses (LAN-wide recommendation), either static or dynamic (through DHCP)

An IP address is a numeric address used for each computer connected to the Internet. IP addresses have the form 210.130.74.190. Each number in the four-number set can range from 0 to 255. However, not all such addresses may be used on the Internet (e.g., 192.168.1.200). Certain ranges of

IP addresses have been reserved as private IP addresses and may be used only on local area networks.

Computers configured with private IP addresses must use a "translator". This device would convert the private IP addresses into data packets that could travel from the local area network to the Internet. Because private IP addresses cannot be used on the Internet, using them locally provides a small measure of protection against attackers trying to break into computers from the Internet.

Many routers, firewalls, and proxy servers provide this translation service, called *network address translation* (or *NAT*). Unless there is a reason not to, using private IP addresses for all workstations and servers on the local area network is recommended in the security checklist.

- ♦ Require logon at each workstation
- ♦ Disable display of previous user name on logon screen
- ♦ If individual patron accounts are implemented, develop a written password policy with training documentation for patrons to follow

As mentioned earlier, one of the foundational elements of network security is a password-protected user logon. In libraries, public access is usually controlled by a generic user account, such as "patron". In this case, the password is practically irrelevant and may be empty. These accounts are created to control access but make network resources easily available. All other users should have accounts secured by strong passwords, as defined in the library's password policy.

To maximize the security of the network in a public environment, system policies (part of a Windows NT/2000 and Windows 98 utility called the *Windows System Policy Editor*) should be used to force a logon. In Windows 98, if this option is not configured, users can get past a logon screen by pressing the Escape key. It's also possible to configure a system policy setting hiding the previous user's name when the logon window is displayed. This should be the default for all public workstations.

If the library uses separate accounts for each patron (rwilliams might be mine, for instance), all patrons should be trained to adhere to the library's password policy. A training brochure will help.

- ♦ Install Windows System Policy Editor or third-party software to restrict access and secure desktop/shell
- ♦ Restrict command line/shell access

- Restrict access to hard drive (consistent with terms for downloading/saving files specified in AUP)

In most libraries, the System Policy Editor, in combination with the built-in file system security provided by Windows NT/2000, provides enough strength to adequately secure public workstations (the Gates Library Foundation computers are configured this way). Windows 98 does not provide the same level of security. Libraries using Windows 98 for public workstations are encouraged to purchase public access computer security software (also called workstation security software). In some cases, the library may find this software more beneficial than the System Policy Editor. These two options provide a means of restricting user access to desktop features such as wallpaper, desktop icons, Start menu items, the screensaver, and more.

These utilities can also be used to restrict access to other system features. In particular, users should never have access to a command line (C:\>). The library's AUP will determine whether public users may save files on a workstation hard drive. According to this policy, the Windows NT/2000 file system or public access security software should be configured to *deny* write access (saving) to *all* folders or *permit* write access only to designated folders on the hard drive.

- Secure web browser against mischief and privacy violations
- Install software to restrict access to system functions within Windows applications

Several options, including workstation security software and an alternate browser called *Public Web Browser* (a specially designed version of Internet Explorer 5.5), allow the library to secure the web browser used on public workstations so that certain features cannot be accessed. Restricting access keeps users from seeing sites viewed by previous users and from changing other settings, like the default home page. Some public access security software (WinSelect *Kiosk* and Fortres Grand's *Cooler*) also makes it possible to limit access to menu items and buttons in some Windows applications and to protect access to system files allowed by "back doors" programmed into some applications. If the library is using Netscape Navigator as its public access web browser, this type of software is highly recommended to protect browser settings.

- Remove unnecessary/unused files/programs from hard drive

- Remove the Network Monitor Agent from public workstations, if installed
- Schedule procedure to periodically remove all user files if file downloading/saving is permitted in the acceptable use policy; also remove unneeded "cookies"

Removing files that are not appropriate for use on a public workstation is another foundational aspect of security. In particular there are several system files that should be removed, such as `format.com`. The Network Monitor Agent (a packet analysis program that, if used by the public, may allow users to see private information of other users as it is transmitted across the network) should also be removed from a public access workstation if it has been installed inadvertently. Limiting a patron's access to just those programs she needs to use the workstation as intended will also limit security flaws introduced through other programs or utilities.

Related to this issue, if patrons may save files on the hard drive, regular maintenance should be scheduled to erase all stored files. Also scan the web browser cookies that may be saved with patron use, and remove any that are unneeded for information sites. This reduces the risk of disclosing of personal information.

- Install and maintain anti-virus software on all workstations
- Update virus signatures on regular schedule (at least once every two weeks)
- Upgrade anti-virus software to support scanning of floppy diskette, e-mail, and Internet file downloads, if necessary

Anti-virus software should be installed on all (or licensed for access from a server by all) workstations, staff and public. The software needs to be regularly updated, as well. There are two components to anti-virus software, the "signatures" (programming code strings) that identify a virus, and the main software, which uses the signatures in examining files on a hard drive for the possible presence of a virus. The virus signatures should be updated on a regular basis—once a week or twice a month at the least. The anti-virus software should be upgraded as new versions (with more features) are released. Some libraries may choose to skip a version and upgrade with every other major version release.

- Implement secure registry settings to secure desktop/operating system settings

- Document software and security settings for future use in configuring new workstations

In addition to the settings available through the System Policy Editor, it is also possible to edit a database of operating system settings called the *registry* to further enhance security. In future versions of this document I will provide a specific list of registry keys and values that should be set on your public and staff workstations.

Once your workstations are secure, all of the selected settings (in the System Policy Editor and in the registry itself) should be documented. In the event of a hardware failure where the operating system must be reinstalled, having all the settings documented will make restoration of the security a simpler process. Store the documentation in a secure (controlled) place, such as the library director's file cabinet.

- Schedule periodic download and installation of operating system patches
- Create and maintain current Emergency Repair Disks, and store in a controlled location
- Implement paper log to record maintenance problems and patron misuse of workstation
- File all workstation component documentation (papers/manuals/disks) for use by service technicians

Windows NT/2000 and Windows 98, including their updates, are tremendously complex programs. Bugs and settings that threaten security are discovered regularly. Microsoft releases small file "fixes" as quickly as possible when such problems are reported. These releases are called *patches* to the operating system. Therefore, it is imperative that all workstations have appropriate patches applied on a regular basis. Also, an Emergency Repair Disk may be invaluable if a computer's registry is corrupted or some other system problem occurs. Whenever settings are altered or new software is installed, it is important to create a new Emergency Repair Disk. As mentioned previously, these need to be stored in a locked case in a staff-only area.

The last two items are not as much security-related items as timesaving measures. Keeping a paper log of problems on a computer may help a paid technician diagnose future problems and minimize the repair bill. Having all current documentation for the components of a particular workstation may also minimize the time required for a tech to diagnose and resolve a problem.

LAN/Domain Server Security

This document assumes the use of Windows NT/2000 as the library's server operating system. Obviously, in larger environments the automation system may require the use of another operating system. Some of the items below will not apply at all in those cases, and some may need to be "translated" into terminology used in the alternative system.

In most small library local area networks, there will be one or two servers: a main server, usually a *domain controller* under Windows NT/2000, which verifies the logins of all users, and a file server used with the library automation system. In some libraries, these two services are combined on one server. It is possible to operate in a very small environment with just Windows NT Workstation/2000 Professional-based computers and no server at all, but it is more difficult to maintain security in this environment. So this base level of security assumes the presence of at least one server. The following items are needed to secure the local area network servers in the library (with the exception of a web server, which has its own configuration settings presented in Chapter 9).

- Configure all NT Server partitions with NTFS file systems
- Configure separate operating system and data partitions (both NTFS)
- Mirror server drives (or implement RAID), if funding allows, for redundancy

These two items are similar to the settings for workstations. Best practice now dictates that all partitions (that show up as distinct drives in the Explorer window) be formatted with the NTFS file system. On a server, that idea is expanded to include a separation of the operating system files and all other programs and user data installed on the server. Separating these so they are located on different "drives" (drives C and D, for example) makes it a bit faster to perform backups, easier to secure sensitive operating system files, and less likely that applying patches and Service Packs (updates to the operating system) will affect other files on the system.

Mirroring hard drives provides an exact duplicate of everything on a server's hard drive. This can be an important feature if the server hard drive fails. Mirrored systems automatically switch to use of the secondary drive while the first is being replaced. This redundancy provides a way to keep a service operational even when there is a hard drive failure. One might call this *service* security. While they are advantageous, mirrored systems do add significant cost to a server. (RAID is a more sophisticated approach that offers similar functionality.)

- Configure servers with private IP addresses (LAN-wide recommendation)

This item is repeated from workstation configuration. If private IP addresses are used on the workstations, they need to be used on local servers as well to keep the network configuration simple (this does not necessarily apply to web servers used to provide web pages to Internet users).

- Remove unnecessary services
- Remove unnecessary files/programs

Many security holes in server operating systems are discovered as users attempt to do things they "shouldn't do." Current security wisdom indicates services not used on a server should be removed from the server. This limits a user's opportunity to do what he shouldn't do. For example, on a typical library file server, if no web documents are available on the server to share across the local network, then the Internet Information Server (IIS) service should be removed (*turned off*). Leaving it running presents an unnecessary opportunity for someone to break through the server's normal security and have complete access to the server.

By the same logic, system files that allow reformatting the hard drive (and other such utilities) should be removed from the server hard drive. They can be copied onto a floppy drive for use by administrators when needed. In the event that an attacker does break through your security, there will be no utility available to help him reformat your drive! Also, if a program is no longer being used on the server, go ahead and uninstall it so that it presents no unintended threats later on.

- Configure file system with proper file/folder access permissions

As mentioned under workstation security, all the files and folders on the server hard drive can be assigned permissions so that only specified users can read or write to files, or open folders or execute programs. On the server it is especially important to limit what users can access.

- Restrict access to the Network Monitor Agent

This agent is a packet analysis tool, which potentially allows a user to view the contents of all the data flowing across the network. It can be a valuable tool for a network administrator. However, extra care should be taken to secure the file so unauthorized users do not gain access to it.

- Disable anonymous user logons
- Disable caching of user logons
- Configure account policy to restrict unauthorized logon attempts
- Create logon warning message (a warning against unauthorized logon or access and use of restricted resources)

As mentioned earlier, the primary means of restricting access to sensitive files on a network is through user logons (requiring a user to supply a user name and password). The password becomes the key to securing the entire system. In addition to using strong passwords, and requiring users on each workstation to log on, the items above add more security on the server side of the connection. First, disable the "anonymous" user, where someone leaves the username and password fields blank and clicks "Logon". Logon information, like most other network data, can be stored temporarily in a place called a cache. In most library environments, workstations and the server should be configured to disable this process.

Also, make sure there is a limit placed on the number of logon attempts made before the account is locked out for some specified time. Three is a good limit. This keeps attackers from using unrestricted blocks of time trying to guess passwords.

Last, due to court cases involving unauthorized access to networks, many security consultants now advise the use of a posted warning against unauthorized use of the network. Windows NT/2000 provides a generic logon warning that can be edited for use in your library. One example of such a banner is the warning notice defined by the Department of Energy's classified order 5639.6A-1:

> *WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.*

- Create alternative Administrators group and restrict membership
- Restrict privileges of default Administrators group
- Create alternative Administrator account (with new name) with full privileges
- Disable default Administrator account
- Configure auditing of Administrator account logon attempts (to track hacking attempts)
- Set a strong password for current administrator account
- Use different passwords for domain/server accounts than for local workstation accounts, or use different account names
- Restrict access permissions for the Everyone group
- Disable Guest account if enabled
- Create appropriate user and group accounts (minimum of three groups: Patrons, Staff, and Administrators)
- Set appropriate group access permissions
- Set appropriate user account passwords (password for PatronX account(s) may be simple or empty)
- Encrypt the SAM password database

This lengthy list applies to the main concepts of user control in any operating system: user accounts, group accounts, and the password file. Your library may assign a user account to each staff member, temporary accounts to contracted technical workers, and individual accounts to patrons. (Most libraries have chosen to allow patron access only through a generic patron account, one account used by all patrons.) These form natural groups of users. So the operating system allows the formation of group accounts as well. Individual users can then be assigned to one or more group accounts. Then it's easy to manage access to all files and folders by controlling just the access that each group has. It keeps the administrator from having to assign permissions to the file system for each individual account. It also ensures a uniform application of permissions.

One note here is that creating a new administrator account and keeping the default "Administrator" account allows easy monitoring of logon attempts to the default account. Since many people know this account exists, it is often the target of attacks. If an attacker can successfully logon as the Administrator, he will have complete control of the server. By keeping the account, but disabling it, it's possible to monitor all logon attempts and deal with potential attacks in their early stages.

- Configure Remote Access Service security, if applicable

Most libraries won't provide any type of dial-in access to the network through the server, so we don't cover security of the Remote Access Service in this document. Libraries that do allow dial-in access, to staff or patrons, need to review other security documents to be sure their network is as secure as possible. This, too, is a popular point of attack if it's available.

- Set/Create registry entries/values for proper security
- Document software and security settings for future use in reconfiguring servers

As mentioned in the workstation security section, the registry holds many different configuration settings for programs installed on the computer. There are many settings which should be set: disabling the Netware DLL Trojan horse capability (assuming Novell Netware is not used on your network), restricting remote access to the registry, restricting access to "named pipes" and to the Scheduler, blocking the 8.3 DOS naming convention attack. There are others. It is imperative that you document for future reference any decisions your library makes regarding specific registry settings.

- Configure audit logs to track unauthorized access to files/folders/accounts; restrict access to log files
- Develop and implement procedure for monitoring audit logs

With Windows NT/2000 it's possible to track, or *audit*, all types of access to system resources, even to track all access attempts on a certain file, folder, or account. Server usage that you've chosen to audit is recorded in an *audit log*. Auditing needs to be configured (especially for sensitive areas like accessing the Administrator account or attempts to run restricted programs) for many areas, but *creating* the logs is useless unless staff reviews them. Develop the discipline of regularly reviewing server logs. This responsibility should be assigned to a specific person to be conducted at specific intervals (e.g., daily or weekly).

- ♦ Install software for the server's UPS that automatically shuts down the server

Be sure to install software that allows the UPS (to which the server is connected) to communicate with the server when a power problem occurs. The communication may include a command to shut the server down if battery power is low. This protects the integrity of data being written to the server's hard drive.

- ♦ Implement procedures for file backups according to backup plan
- ♦ Restrict access to backup program
- ♦ Maintain backup log and auditing
- ♦ Rotate one backup set offsite regularly

Backing up, while not a normal network security issue, does goes to the heart of network security: protecting data from loss or corruption. Only a specified individual or two should have access to the backup software, so unauthorized persons cannot restore sensitive data from a previous backup. Good discipline requires backups to be performed regularly and that one person be responsible for the backup procedures and maintenance of backup logs. To protect data stored on a server against theft, rotate one set of backup media offsite (out of the library) regularly. (What could be worse than going through the rigors of backing up regularly only to have both server and backup media stolen?) Be sure all backup media, the offsite set as well, is secured properly. This may include putting the media in a lockable container and securing the key in a controlled location.

- ♦ Schedule periodic download and installation of operating system patches
- ♦ Create and maintain current Emergency Repair Disks, and store in a controlled location
- ♦ Implement paper log to record maintenance problems, attempts at unauthorized access, and other server problems

- File all server component documentation (papers/ manuals/disks) for use by service technicians

Even more than with workstations, it is vitally important to update the server operating system on a regular basis by installing patches and Service Packs as Microsoft makes them available. Doing so will greatly reduce your risk of attack. Use the same paper log for servers as for workstations to document problems and repairs, attacks, and other anomalies related to servers. And keep the server's documentation available for any service technician that may need it.

Network Equipment Security

Network equipment refers to all the devices required to get data signals from one computer to another. Generally, these include hubs, switches, routers, and firewalls. Bridges may be included in older designs. The following items apply to all these devices. A separate section is devoted to other issues related to routers and firewalls.

Libraries should be purchasing network equipment that provides management capabilities. This provides the possibility of remote management of the network even if the library does not contract for that service initially.

- Set appropriate network management protocol (SNMP) passwords/community strings
- Record and secure any password settings created by staff or contractors

These two items minimize the risk of network equipment configurations being altered by unauthorized personnel. *When the library hires a vendor to install and configure network equipment, be sure to document all passwords used to secure the equipment.* More than one installation has been performed where the vendor did not disclose equipment passwords. When the library chose to change vendors for maintenance of the network, the passwords were unknown, and the time required to reconfigure the equipment multiplied. The disclosure of passwords used in the installation or configuration should be included in the terms of any contract for any paid installation and configuration services. The library must have the right to change vendors without incurring great expense to do so.

On the other hand, it is the library's responsibility to secure these passwords by documenting them and storing the documentation in a secure (preferably locked) location.

- Configure audit logs properly, if available
- Implement procedure for monitoring audit logs

If the equipment provides logs of activity, make sure the logs are configured securely—accessible only by authorized personnel. If the library will be doing its own network maintenance, make it part of the installation contract for the vendor to train staff, or at least provide a demonstration to staff, in monitoring and maintaining the logs provided through the equipment.

- Schedule periodic installation of firmware updates

Just like operating systems on a server or workstation, the firmware[5] that provides the functionality of "intelligent hubs," switches, and bridges may get updated, especially when bugs are discovered. A regular routine to check for firmware updates needs to be implemented to maintain the proper operation and security of the equipment.

- Document equipment settings for future use in reconfiguring equipment

Be sure to document all settings in the installed configuration of the equipment once the installation is complete. Make an electronic copy of the configuration file, if possible. Also, update the documentation whenever a change is made to the configuration. Record any decisions or justification used in making the change. Two years later it may be difficult or impossible to remember why something was done a certain way!

[5] *Firmware*: the term is used to describe programming code providing much of the functionality of a hardware device. It derives from the use of code permanently printed on a Read Only Memory (ROM) chip—firmware rather than software. The term is not used with high-end equipment like routers, being replaced by a BIOS and an operating system. Many low-end equipment manufacturers still use this term.

- File all network equipment documentation (papers/ manuals/ disks) for use by service technicians

The same here as in servers and workstations. Storing documentation in an organized fashion cannot be overemphasized, because it can result in great reduction of the time and frustration required maintaining equipment.

9

Perimeter Security

He looked at the screen in disappointment. He had seen others do it, but he wouldn't be doing it to this network. The library staff had done their homework. The popular ports were closed on the firewall or router. The web server was secured as tight as a drum. He had even sent an e-mail message with a bot attached to see if he could open a hole in the firewall. Either the e-mail address was dead, the library staff was wise to the exploit, or the firewall was configured to block outbound traffic addressed to the port he needed.

Maybe he would visit personally sometime, he thought.

Maybe not.

With a sigh he began scanning another site. This one wasn't worth the time.

Router/Firewall Security

Routers are network devices that "join" (or separate, depending on your view) two distinct networks. Routers allow data from one network to be transmitted to the other while keeping data intended for its own network from crossing over. Routers can be configured to allow or deny individual data packets access to the other network based on a number of parameters. Depending on need and expense, routers can be relatively simple to configure or very complex. The router's level of "protection" of an internal network from an external attack varies widely as a result.

A firewall is a device that usually assists a router in protecting the internal network. Normally it offers features in addition to those supplied by the router. One feature found on firewalls we've discussed previously, in our discussion of IP addresses. When private IP addresses are used on internal workstations that also need to access the Internet, the private IP addresses must be "translated" to public IP addresses. A firewall (but sometimes a router) usually supplies this service, called *network address translation* (or NAT).

Firewalls included with ISDN and DSL routers usually provide little protection beyond network address translation. These may suffice in very small library environments where no public servers (such as a web server) are used. If the library provides only Internet access, then the router/firewall can be configured to deny virtually all inbound requests, minimizing the risk of attack.

On the other hand, if the library will be providing web-based access to its library catalog, or will be contracting with a vendor for remote management of its network, then we recommend the use of a separate firewall device, now often called an *Internet security appliance*. These devices offer *stateful packet inspection*, additional functionality providing much more security against Internet-based attacks (such as denial-of-service attacks). Wherever possible, we advocate the use of standalone firewalls.

- Use a three-port firewall; public services (web/ftp/e-mail) are provided on a separate network segment, the DMZ

One of the other features of many standalone firewalls or security appliances is a third network port (the first two ports connect to the library's internal network and the Internet connection). This port is normally referred to as a DMZ (demilitarized zone) port, to which the library would connect its public servers (web server, mail server, or others). This port provides controlled access to the public servers without putting them on the library's internal network, enhancing security of the internal network.

- Implement network address translation (NAT), if possible
- Use private IP addresses LAN-wide, if possible

As mentioned, the router or firewall must supply network address translation if the internal network is configured with private IP addresses.

- Configure router to *deny* inbound access to unused ports (unless specific library services require them); for example, FTP on port 21, Telnet on port 23, and others

There are many Internet-based services besides the World Wide Web, which provides access to web pages. Older services include e-mail, file transfer protocol (ftp), and telnet (terminal emulation). Much of the router/firewall configuration will have to do with denying access to many of these services. In fact, if no public services are provided by the library (meaning, basically, the library does not maintain its own web server, or Internet-based access to its library catalog), then all inbound service requests can be denied.

Many outbound service requests may need to be blocked as well. For example, if your library policy states that patrons are not allowed to download files, one step in automatically implementing the policy would be to deny outbound connections to ftp servers. This will block some Internet downloads, but not all. Nevertheless, it's an attempt to make configuration consistent with policy. Outbound blocking will also help protect sites on the Internet should a library workstation become infected with a Bot, a software robot. (Bots can lead to Internet-connected computers participating in a coordinated attack on other sites and connections.)

- ♦ Configure firewall so no packets with source addresses outside the LAN are allowed into the LAN, but only to DMZ
- ♦ Firewall uses stateful packet inspection, providing protection against denial-of-service attacks and IP spoofing
- ♦ Document settings for future use in reconfiguring router/firewall; make backup copy of router configuration file, if possible, and store in secure location

These items concern two common attack types that need to be blocked, if possible. This comprises a very basic level of security. The individual responsible for implementing your library's network security may choose more settings to protect against other potential threats. As you discuss firewall security with the vendor, document the decisions made, their justifications, and the firewall settings changed when they are implemented. Just like server setup, document all settings for use should the router/firewall ever have to be reconfigured from scratch (such as when defective equipment is replaced). If possible create an electronic copy of the router and firewall configuration files. This can make restoration of the settings much simpler if equipment must be replaced. Store the documentation in a secure location.

- ♦ Schedule periodic installation of firmware updates

- File all router/firewall documentation (papers/manuals/disks) for use by service technicians

Repeating earlier items, be sure the router and firewall firmware is upgraded as specified by the manufacturer. Some firewalls may have the capability to update themselves across the Internet during idle moments. (If your firewall has this feature, see if the update can be scheduled for non-peak times so that service disruption is minimized.) For a device that requires human implementation, *I highly recommend having the update performed by a qualified network technician*. This, of course, requires maintenance funding in the library budget.

Web Server Security

This section is included for any library providing web pages on its own web server. Libraries providing public access to their library catalog over the Web generally fall into this category. [*Note*: If a library is interested only in maintaining a general web site with no catalog access, I encourage contracting with a Web hosting provider. The Web hosting provider will take care of all the configuration, security, and maintenance of the server.]

Web server security actually involves two phases. The first is to secure the server itself. The second is to configure the web server software (Internet Information Server on most Windows NT/2000-based servers). Because the web server is accessible to Internet users, it is a common target of Internet-based attacks. One of the most common attacks involves defacing one or more web pages stored on the web server. This normally doesn't disrupt service so much as cause embarrassment. On the other hand, there are many tricks that allow an attacker to break into a web server, gain Administrator privileges, and potentially access other resources on the library's network. This is a much more substantial threat.

- Implement normal server security steps as listed in Section 6 of the *Checklist* (with exceptions noted)

Many of the same steps required to secure a Windows NT/2000 file or logon server apply to securing the server upon which the web server software is built. Repeat the server security as indicated. The configuration of the web server software adds a surprising number of additional items.

- Configure web server as standalone server (especially not a domain server)

The web server should be a completely separate computer made available on a separate network segment attached to the firewall. In particular, the web server should not be the library's main file server, with IIS running in addition to everything else and Internet users allowed to pass through the library's firewall to access web pages. Such a configuration is courting disaster! When installing Windows NT/2000, the server should be installed as a "standalone server," not a domain controller or a member server.

- Configure web server to run as separate user (not with root or admin privileges)

No web server software should have administrator privileges. Should an attacker break in, he would have the same privileges.

- Secure the anonymous IIS account

It is possible to authenticate users (requiring logon names and passwords) to a web site. You may have accessed a web page that popped up a logon box. These require specific user accounts on the server. Most web pages are not protected this way and operate under an account called the anonymous user. IIS uses one account (IUSR_*computer name*) for this service. In order to keep attackers from accessing the server through this account, security experts recommend renaming the account on your server and then creating a new account with the IUSR name. The new IUSR account can be disabled, and access attempts logged to track any break-in attempts.

- Disable directory browsing

In IIS and other web servers, it is possible to turn off directory browsing. Directory browsing means listing the contents of a directory contained in the main web documents folder. It can be dangerous to allow Internet users to see directories where scripts and other sensitive information are stored. Turn off directory browsing for all web folders or at minimum for any script folders.

- Set proper file system access permissions

In the folder containing all documents shared through the web server, make sure that the Write permission is never assigned to a file also having Script/Execute permission through IIS. This could potentially allow an attacker to upload a script file, which he could then execute on the server. Make sure that scripts only have Script permission (and not Execute). Finally, place the script-interpreter (such as Perl or PHP) into a different folder than the folder where its scripts are stored.

- ♦ Remove unnecessary services
- ♦ Remove unnecessary files/programs

These two echo similar items for server security. It is especially important to turn off any unneeded services. It is also a good idea to remove any unneeded files or programs from the web server, since a limited configuration gives an attacker less bullets to use in shooting at your network.

- ♦ Unless absolutely required, remove FrontPage extensions if installed

If your web site was constructed using Microsoft FrontPage, some additional files called *FrontPage Extensions* are required on the web server for users to properly view your web pages. The Extensions (especially for older versions of FrontPage) can open security holes in your server configuration. If your web site was designed with some other program, but these extensions are installed, they should be removed.

- ♦ Restrict scope of indexing if Index Server is used

Index Server is a utility that comes with IIS. It can be very helpful in making textual documents stored on your web server searchable. It can also be dangerous if it indexes script and other sensitive files stored on your site. If the utility is used, restrict the folders it indexes just to those storing non-sensitive files.

- ♦ Configure registry settings for proper IIS security
- ♦ Document settings for future use in reconfiguring web server, and store in secure location

There are other registry settings that may be configured to enhance IIS security. A list of these is available in other resources. As with all servers, be sure to document all the decisions made in configuring the web server, and store them in a controlled location.

- Configure web server auditing and audit logs properly
- Implement procedure for creating/monitoring audit logs

Just like any server, it is important to audit system activities and review the logs created. By doing so regularly, one may discover the probes of an attacker before any lasting damage is done.

- Have a trusted source review for security flaws any CGI-type scripts (downloaded from Web or developed locally) used in web pages

Many web sites make use of a variety of forms and server-based scripts to process the data supplied in them. There are a number of ways to create security holes inadvertently by using insecure coding practices. If you've downloaded scripts from the web and use them on your web pages, or if someone whose experience you are unsure of has assisted in designing your web pages, have the scripts reviewed by a trustworthy third party.

- Update IIS web server software with patches as soon as they are released by Microsoft; repeating 4-42, update the web server's underlying NT/2000 operating system as patches are released by Microsoft (several recent break-ins are directly attributable to the lack of applying patches to protect against well-known vulnerabilities)
- Subscribe to Microsoft's Product Security Notification service

The requirement to update IIS with current patches is probably the most important of all the items. Many commercial web servers have been broken into, resulting in stolen credit card databases and other sensitive data disclosure. Most of the break-ins came as a result of a lack in diligence in applying patches to Windows NT/2000 and IIS. *The need for this one item cannot be overemphasized!* It is also important to remember to patch the underlying Windows NT/2000 Server operating system regularly, too. Be sure to subscribe to Microsoft's Product Security Notification service (see page 146 in the bibliography for the contact site), which provides e-mail notification of security problems as they arise with Microsoft products. It's the best way to know when patches are available.

- File web server documentation (papers/manuals/ disks) for use by service technicians

As with all servers, file the documentation for the server and for IIS so that it can be accessed easily by service technicians when maintenance or repair needs to be performed on the server.

Virtual Private Network (VPN) Security

Virtual private networks are "simulated" private connections over the Internet between an individual computer (or other network) and an organizational network—the library network in this case. These types of Internet-based connections use encryption technology to encapsulate all of the information between the endpoint and the library network and protect it from spying eyes.

Virtual private networks require special server configuration and firewall configuration to implement, and not many local vendors have experience in setting them up. Therefore, the time, frustration, and expense factors present a deterrent in small libraries. Nevertheless, the concept is attractive because it presents a way to allow remote maintenance and administration of library networks.

This is an area of security that will be expanded here in the future. For now, the following features are recommended for any VPN solution implemented in libraries.

- Supports Microsoft's point-to-point tunneling protocol (PPTP) or IPSec
- Document all server changes required to support the VPN
- Document firewall configuration changes required to support the VPN

Part III

Auxiliary Documents

Network Security Checklist

III A

Network Security Checklist for Libraries Using Microsoft Windows Operating Systems

Version 0.60

Item	Stan.	Standard Description	Comply	Comments
LEGEND		Implementation Standard: N = not applicable (Stan.) O = optional R = recommended M = mandatory Level of Compliance: X = no protection/not implemented (Comply) W = needs work A = adequate; meets or exceeds standard		
1. General				
1-1	R	Budget plan produced and budget line items include cost of annual maintenance (maintenance contract or line item for time/materials)	X W A	
1-2	R	Budget plan produced and budget line items include cost of equipment replacement.	X W A	
1-3	M / R	Backup plan developed for servers (M) and staff workstations (R)	X W A	
1-4	R	Security policy developed detailing rights and responsibilities of staff, patron, and contract users of the network	X W A	
1-5	M	Acceptable Use Policy (AUP) developed for patrons and staff; includes consequences of misuse of equipment or services	X W A	
1-6	R	Workstation security plan developed	X W A	

1-7	M	Train staff not to reveal system passwords to anyone other than specified contracted technicians having prior authorization	X W A	
1-8	M	Train staff not to allow anyone access to systems and network equipment without prior authorization	X W A	
1-9	M	Require companies performing maintenance/ configuration to sign a disclosure agreement: to disclose configuration parameters (especially passwords) to designated library staff and *not* to disclose library network configuration information to any third-party without prior authorization.	X W A	
2. Physical & Data Security				
2-1	M	Dead bolt locks on all building entrances/exits	X W A	
2-2	M	All servers and network equipment in staff-only area, preferably locked (alternatively, in locked equipment cabinet)	X W A	
2-3	R	Data cables/data jacks (public areas) are secured from patron access, if possible	X W A	
2-4	R	Locked storage is used for backup media and emergency recovery disks/CDs	X W A	
2-5	R	Rotate one backup set offsite regularly and store in a secure location	X W A	
2-6	R	Store backup of router, firewall configuration file, if applicable, in a secure location	X W A	
2-7	R	Keys used in securing equipment or media are stored in a controlled location	X W A	
2-8	M	Electrical system inspection for adequate building power capacity, breaker box, and independently grounded electrical circuits (dedicated circuits suggested for PCs; ground suggested for equipment racks)	X W A	
2-9	M	All workstation power cords connected to surge protectors meeting UL1449 330V standard	X W A	
2-10	M	All modems physically connected to phone lines are surge protected	X W A	
2-11	O	Outlets on dedicated circuits are colored fluorescent orange	X W A	
2-12	R	Serial numbers and physical asset numbers (if applicable) are recorded for all workstations, servers, and network equipment	X W A	
2-13	O	Insurance coverage against damage or theft	X W A	

3. Password Security				
3-1	M	Develop written password policy and provide to all staff and patrons using specific user logons	X W A	
3-2	M	Develop written instructions in creating strong passwords and provide to all staff and patrons using specific user logons	X W A	
3-3	M	Document passwords for all network equipment, servers, and workstations	X W A	
3-4	M	Store password documentation in secure location known only by library director and one other person	X W A	
4. Hardware Security				
4-1	M	BIOS: public workstation: boot order, set primary hard drive first	X W A	
4-2	M	BIOS: server (locked staff-only access): boot order, either setting	X W A	
4-3	M	BIOS: server (when locked staff-only access is not possible): boot order, set primary hard drive first	X W A	
4-4	M	BIOS: workstations: supervisor password set	X W A	
4-5	M	BIOS: servers: if servers can restart automatically with password set, set one	X W A	
4-6	M	BIOS: anti-virus protection enabled	X W A	
4-7	O	BIOS: public workstations: floppy drive(s) disabled if AUP specifies no patron access to floppy disks	X W A	
4-8	M	BIOS: servers (when locked staff-only access is not possible): disable floppy drive	X W A	
4-9	M	BIOS: public workstations: setup message hidden/ disabled, if available	X W A	
4-10	M	BIOS: all computers: record setup configuration parameters	X W A	
4-11	R	Servers and workstations: use small padlocks to secure case covers	X W A	
4-12	O	Public workstations (or all computers in a very insecure environment): secure CPU, monitor, keyboard, and mouse to table/desk with hardware security cables/devices.	X W A	
4-13	M	All servers: protect with UPS (400va or higher), preferably having auto shutdown software	X W A	
4-14	M	Network equipment (hubs or switches): protect with UPS (250va or higher)	X W A	
4-15	M	Router/firewall: protect with UPS (250va or higher)	X W A	
5. Workstation Security				
5-1	M	Configure NT Workstation partitions with NTFS file systems	X W A	
5-2	M	Disable boot keys on Windows 95/98 workstations	X W A	

5-3	R	Configure workstations with private IP addresses (LAN-wide recommendation), either static or dynamic (through DHCP)	X W A	
5-4	M	Require logon at each workstation	X W A	
5-5	R	Disable display of previous user name on logon screen	X W A	
5-6	M	If individual patron accounts are implemented, develop a written password policy with training documentation for patrons to follow	X W A	
5-7	M	Install Windows System Policy Editor or third-party software to restrict access and secure desktop/shell	X W A	
5-8	M	Restrict command line/shell access	X W A	
5-9	M	Restrict access to hard drive (consistent with terms for downloading/saving files specified in AUP)	X W A	
5-10	M	Configure web browser to enhance privacy, and restrict access to web browser settings	X W A	
5-11	R	Install software to restrict access to system functions within Windows applications	X W A	
5-12	M	Remove unnecessary/unused files/programs from hard drive	X W A	
5-13	M	Remove Network Monitor Agent from public workstations, if installed	X W A	
5-14	M	Schedule procedure to periodically remove all user files if file downloading/saving is permitted in AUP; also remove unneeded "cookies"	X W A	
5-15	M	Install and maintain anti-virus software on all workstations	X W A	
5-16	M	Update virus signatures on regular schedule (at least once every two weeks)	X W A	
5-17	M	Upgrade anti-virus software to support scanning of floppy diskette, e-mail, and Internet file downloads, if necessary	X W A	
5-18	R	Implement secure registry settings to secure desktop/operating system settings	X W A	
5-19	M	Document software and security settings for future use in configuring new workstations	X W A	
5-20	M	Schedule periodic download and installation of operating system patches	X W A	
5-21	M	Create and maintain current Emergency Repair Disks, and store in a controlled location	X W A	
5-22	R	Implement paper log to record maintenance problems and patron misuse of workstation	X W A	
5-23	M	File all workstation component documentation (papers/manuals/disks) for use by service technicians	X W A	

6. LAN/Domain Server Security				
6-1	M	Configure all NT Server partitions with NTFS file systems	X W A	
6-2	R	Configure separate operating system and data partitions (both NTFS)	X W A	
6-3	O	Mirror server drives (or implement RAID), if funding allows, for redundancy	X W A	
6-4	R	Configure servers with private IP addresses (LAN-wide recommendation)	X W A	
6-5	M	Remove unnecessary services	X W A	
6-6	M	Remove unnecessary files/programs	X W A	
6-7	M	Configure file system with proper file/folder access permissions (Specifically, restrict access to system files and executables)	X W A	
6-8	R	Restrict access to the Network Monitor Agent	X W A	
6-9	M	Disable anonymous user logons	X W A	
6-10	M	Disable caching of user logons	X W A	
6-11	M	Configure account policy to restrict unauthorized logon attempts	X W A	
6-12	M	Create logon warning message (a warning against unauthorized logon or access and use of restricted resources)	X W A	
6-13	R	Create alternative Administrators group and restrict membership	X W A	
6-14	R	Restrict privileges of default Administrators group	X W A	
6-15	R	Create alternative Administrator account (with new name) with full privileges	X W A	
6-16	R	Disable default Administrator account	X W A	
6-17	R	Configure auditing of Administrator account logon attempts (to track hacking attempts)	X W A	
6-18	M	Set a strong password for current administrator/root account	X W A	
6-19	M	Use different passwords for domain/server accounts than for local workstation accounts, or use different account names	X W A	
6-20	M	Restrict access permissions for the Everyone group	X W A	
6-21	M	Disable Guest account if enabled	X W A	
6-22	M	Create appropriate user and group accounts (minimum of three groups: Patrons, Staff, and Administrators)	X W A	
6-23	M	Set appropriate group access permissions	X W A	
6-24	M	Set appropriate user account passwords (password for PatronX account(s) may be simple or empty)	X W A	
6-25	M	Encrypt the SAM password database	X W A	
6-26	M	Configure Remote Access Service security. if applicable	X W A	

6-27	M	Set/Create registry entries/values for proper security (disable Netware DLL Trojan horse capability, if applicable; restrict remote access to registry; restrict access to named pipes and the scheduler; block 8.3 attack; etc.)	X W A	
6-28	R	Document software and security settings for future use in reconfiguring servers	X W A	
6-29	M	Configure audit logs to track unauthorized access to files/folders/accounts; restrict access to log files	X W A	
6-30	M	Develop and implement procedure for monitoring audit logs	X W A	
6-31	R	Install software for the server's UPS that automatically shuts down the server	X W A	
6-32	R	Implement procedures for file backups according to backup plan	X W A	
6-33	R	Restrict access to backup program	X W A	
6-34	R	Maintain backup log and auditing	X W A	
6-35	R	Rotate one backup set offsite regularly	X W A	
6-36	M	Schedule periodic download and installation of operating system patches	X W A	
6-37	M	Create and maintain current Emergency Repair Disks, and store in a controlled location	X W A	
6-38	R	Implement paper log to record maintenance problems, attempts at unauthorized access, and other server problems	X W A	
6-39	M	File all server component documentation (papers/ manuals/disks) for use by service technicians	X W A	
7. Network Equipment Security				
7-1	M	Set appropriate network management protocol (SNMP) passwords/community strings	X W A	
7-2	M	Record and secure any password settings created by staff or contractors		
7-3	M	Configure audit logs properly, if available	X W A	
7-4	M	Implement procedure for monitoring audit logs	X W A	
7-5	M	Schedule periodic installation of firmware updates	X W A	
7-6	M	Document equipment settings for future use in reconfiguring equipment; make backup copy of router configuration file, if possible, and store in secure location	X W A	
7-7	M	File all network equipment documentation (papers/ manuals/disks) for use by service technicians	X W A	

8. Router/Firewall Security				
8-1	R	Use three-port firewall; public services (web/ftp/e-mail) are provided on separate network segment, the DMZ	X W A	
8-2	R	Implement network address translation (NAT), if possible	X W A	
8-3	R	Use private IP addresses LAN-wide, if possible	X W A	
8-4	R	Configure router to deny inbound access to unused ports (unless specific library services require them); for example, FTP on port 21, Telnet on port 23, etc.	X W A	
8-5	M	Configure firewall so no packets with source addresses outside the LAN are allowed into the LAN, but only to DMZ	X W A	
8-6	R	Firewall uses stateful packet inspection, providing protection against denial-of-service attacks and IP spoofing	X W A	
8-7	M	Document settings for future use in reconfiguring router/firewall; make backup copy of router configuration file, if possible, and store in secure location	X W A	
8-8	M	Schedule periodic installation of firmware updates	X W A	
8-9	M	File all router/firewall documentation (papers/ manuals/disks) for use by service technicians	X W A	
9. Web Server Security				
9-1	As speci-fied	Implement normal server security steps as listed in section 4, with the exception of 4-9, 4-18 (just remove agent), 4-39 (remove service), and 4-40 and 4-41 (see 7-9 through 7-11)	X W A	
9-2	M	Configure web server as standalone server (especially not a domain server)	X W A	
9-3	M	Configure web server to run as separate user (not with root or admin privileges)	X W A	
9-4	M	Secure the anonymous IIS account	X W A	
9-5	M	Disable directory browsing	X W A	
9-6	M	Set proper file system access permissions (especially that both Write and Script/Execute permissions [IIS] are never set on same folder; etc.)	X W A	
9-7	M	Remove unnecessary services	X W A	
9-8	M	Remove unnecessary files/programs	X W A	
9-9	R	Unless absolutely required, remove FrontPage extensions if installed	X W A	
9-10	R	Restrict scope of indexing if Index Server is used	X W A	
9-11	M	Configure registry settings for proper IIS security	X W A	

9-12	M	Document settings for future use in reconfiguring web server, and store in secure location	X W A	
9-13	M	Configure web server auditing and audit logs properly	X W A	
9-14	M	Implement procedure for creating/monitoring audit logs	X W A	
9-15	R	Have a trusted source review for security flaws any CGI-type scripts (downloaded from Web or developed locally) used in web pages	X W A	
9-16	M	Imperative: Update IIS web server with patches as soon as they are released by Microsoft; repeating 4-42, update the web server's underlying NT operating system as patches are released by Microsoft	X W A	
9-17	M	Subscribe to Microsoft's Product Security Notification service	X W A	
9-18	M	File web server documentation (papers/manuals/ disks) for use by service technicians	X W A	
10. Virtual Private Network (VPN) Security				
10-1	M	Supports Microsoft's point-to-point tunneling protocol (PPTP) or IPSec	X W A	
10-2	R	Document all server changes required to support the VPN	X W A	
10-3	R	Document firewall configuration changes required to support the VPN	X W A	

III B

A Sample Security Policy

Somewhere Public Library Security Policy

Purpose

The Somewhere Public Library local area network (herein referred to as "the SPL network" or "the network") is critical to the provision of information services to SPL staff and patrons. The SPL library automation system processes sensitive and valuable information. The addition of public access to the Internet within the library has increased the size, complexity, and management concerns related to the operation of the network. Specific security measures and procedures must be implemented to protect the confidentiality of information transactions being processed on the network and to keep critical systems operational. Because all citizens of Somewhere are encouraged to use the network for informational and educational needs, security risks have increased and more stringent practice in safeguarding resources is necessary than was required when simple standalone PCs were used. These expanding security requirements are addressed in the following network security policy.

This policy has two purposes. First, the policy will emphasize to all Somewhere Public Library employees and patrons the importance of network security in the library and their roles in maintaining that security. Second, the policy will assign specific responsibilities needed to secure networked information resources.

Scope

The SPL network security policy covers all electronic information resources in the library. It applies equally to network servers, workstations, both staff and public access, network equipment, telecommunications equipment, and peripherals, such as printers, within the library. The policy applies to all library users, managers, and administrators, including Library staff, patrons, contractors, and City staff utilizing the Library's network resources.

Goals

The SPL security program is designed to ensure the availability of networked resources and the integrity and confidentiality of data transmitted over and stored on the network. Specifically the goals of the program include:

- Ensuring the library network has sufficient security measures applied to protect the integrity of its data, the privacy of information transactions, and the availability of its resources;
- Ensuring the cost of the security measures implemented is commensurate with the risks present on the network;
- Ensuring appropriate budgetary and technical support is available and maintained;
- Training all users to be responsible for the security of data, information, and other computing resources to which they have access, and training staff to maintain accountability practices;
- Enforcing policies and technical mechanisms which contribute to the auditability of network resources;
- Providing sufficient guidance to library staff in the discharge of their responsibilities in network and information security;
- Ensuring that all applicable organizational and departmental policies and procedures are applied and practiced;
- Developing appropriate contingency or disaster recovery plans to provide continuity of operation for all critical functions of the network.

Responsibilities

Responsibility for implementing and maintaining the Library's network security goals is divided among four specific groups. [The library may choose to create an optional, very detailed list of tasks and responsibilities; a procedures manual should also be developed as a result of this delineation of responsibilities. If so, add the following line here: Detailed responsibilities are presented separately in *Network Security Responsibilities for the Somewhere Public Library.*]

1. Library Management (LM; in most environments called Functional Management) - the library director, library board, and other library administration, if applicable, who have functional responsibility for the library. Library Management is responsible for informing staff about this policy, assuring that each person has a copy, and interacting with staff and volunteers on security issues.

2. Network Management (NM) - contract technical support persons or library staff involved in the technical support, management, and operation of the SPL network. Network Management must ensure the continued operation of the network and is responsible for implementing appropriate network security measures as indicated in this security policy.

3. Local Administrators (LA) - library staff responsible for ensuring that end users have access to needed network resources available through the library's servers or Internet access. Local administrators provide day-to-day maintenance of network security in accordance with this security policy. Local administrators are responsible for reporting observed breaches of security policy to network and library management.

4. End Users (U) - library staff, volunteers, and public users who have access to the SPL network. End users are responsible for using the network resources in accordance with the provisions of this security policy and the Library's acceptable use policy. All users of data and network services (such as the Internet) are responsible for complying with security policy established by library and network management and for reporting to management any actual or suspected breach of security.

Enforcement

When end users fail to comply with this policy, SPL information—while stored, processed or transmitted on the Somewhere Public Library network—may be exposed to the unacceptable risk of loss of confidentiality, integrity or availability. Violations of security guidelines and procedures established to support this policy will be brought to the attention of management for action and could result in disciplinary action up to and including termination of employment or termination of rights to use the network.

GENERAL POLICIES OF THE LAN

GP1. Every workstation and server shall have a designated local administrator who is responsible for maintaining the security of the computer. All end users of the system are responsible for following all policies and procedures in this policy and the acceptable use policy. SPL staff who manage workstations or servers shall be trained so they can follow all policies and procedures effectively.

GP2. Server security shall be exclusively controlled by one local administrator and network management. Access to server security mechanisms by all other staff, volunteers, or public users shall be considered unauthorized access.

GP3. The local administrator responsible for each workstation or server must ensure that all software installed on the system is approved for use and is licensed properly.

GP4. All software installation and updates shall be the responsibility of network management or the designated local administrator.

GP5. One local administrator shall be designated to oversee the backup of server and workstation hard drives.

GP6. Each staff member, volunteer, and contract worker will be assigned a unique USERID and initial password according to established procedure. Public users will use a generic USERID and password [*note:* or unique USERID and password if the policy is adjusted to allow it] to gain access to network resources. Users must not share or disclose unique USERIDs/passwords.

GP7. All users must be authenticated to the network before accessing network resources.

GP8. Use of network hardware or software such as traffic monitors/recorders and routers shall be restricted to network management or a designated local administrator.

GP9. Security training shall be integrated into existing library training programs such as orientation programs for new employees, volunteers, or patrons in the use of computers, software, and network information resources.

GP10. Incident logs and subsequent security reports must be generated and reviewed on a regular basis.

SPECIFIC RESPONSIBILITIES FOR ENSURING Somewhere Public Library LAN SECURITY

1. Users (Staff and Public)

Users are expected to be knowledgeable about and adhere to the Library's security and acceptable use policies. Users are ultimately responsible for their own behavior. User responsibilities include:

U1. Understanding and respecting relevant Federal and State laws, Somewhere Public Library policies and procedures, and other applicable security procedures and practices established for the Somewhere Public Library network.

U2. Using network resources in accordance with terms specified in the Library's acceptable use policy, and being aware of activities disallowed and the consequences of engaging in such unauthorized use.

U3. Being aware of privacy issues related to their use of network resources and protecting the confidentiality and integrity of their own information.

U4. Selecting and maintaining strong passwords as outlined in the Library's password policy. Specifically, users must not disclose unique USERIDs or passwords to others.

U5. Notifying a local administrator when security procedures are not followed—for example, when a previous user leaves a workstation without logging off or when passwords are written and left in open view.

U6. Notifying a local administrator or network management if a security violation or breach is observed or detected.

U7. Being familiar with how malicious or virus-infected software is distributed and observing practice that minimizes the risk of damage due to the introduction of such software.

U8. Reporting any signs of abnormal or suspicious activity to the local administrator.

U9. (Staff only) Ensuring that his/her workstation is left on as scheduled so the hard drive may be backed, according to the Library's backup policy.

2. Library Managers

Library managers, with guidance or direction from the parent agency, are responsible for developing and implementing effective security policy. They are ultimately responsible for ensuring that the objectives of library policy and individual responsibilities are clearly communicated to staff and end users and adequately followed. Specific responsibilities of library managers include:

FM1. Effectively analyzing potential security risks in order to formulate an appropriate security policy. This risk management requires:

- identifying the assets to be protected
- assessing potential vulnerabilities
- analyzing the risk of exploitation
- implementing cost-effective safeguards

FM2. Providing training, or at least written training materials, to all staff, volunteers, and patrons in the appropriate use of the network, awareness of the possible effects of misuse or unauthorized use of network resources, and the consequences of any unauthorized use.

FM3. Ensuring staff and patrons understand the danger of malicious software, how it is generally spread, and the technical controls used protect against it.

FM4. Informing local administrators and network management of the change in status of staff, volunteers, or contract workers [*note*: and any patrons who have unique USERIDs] who utilize the Somewhere Public Library network. This could include a position change (providing greater or more restricted access privileges) or termination of library employment.

3. Network Managers

Network management may include local staff or contracted support and is expected to implement and maintain security measures enforcing local security policies, to archive critical programs and data, and to control access and protect physical network facilities. Specifically, network management is responsible for:

NM1. Rigorously applying available security measures enforcing local security policies.

NM2. Advising library management on the effectiveness of the existing policies and technical considerations that may lead to improved practices.

NM3. Responsible for securing the local network and its borders with outside networks (e.g., city hall, the school district, or the Internet).

NM4. Responsible for responding to security breaches or violations in a timely and effective manner.

NM4.1. Notify local administrators if a break-in is in progress and assist other local administrators in responding to security violations.

NM4.2. Cooperate with local administrators in tracking/monitoring violators and assist in enforcement efforts.

NM5. Configuring audit logs and using network monitoring tools to aid in the detection of security violations.

NM6. Conducting timely audits of network server logs.

NM7. Remaining informed on outside policies and recommended practices and, when appropriate, informing library management of new developments.

NM8. Exercising the powers and privileges inherent in network administration with caution and discretion.

NM9. Identifying, recommending, installing, and configuring software providing:

- intrusion detection
- monitoring of unauthorized activity
- removal of malicious software

NM10. Developing procedures that allow users and local administrators to report security violations, and notifying library management and possibly outside agencies of any threats.

NM11. Promptly notifying designated personnel of all computer security incidents.

NM12. Providing assistance in tracking the source of malicious software or computer viruses and determining the extent of contamination.

NM13. Removing malicious software or viruses.

NM14. Conducting periodic audits to ensure proper security practices are followed.

NM15. Maintaining user privacy.

4. Local Administrators

Local administrators are local staff or volunteers who assist in the daily maintenance of security services and who support and enforce applicable security policies and procedures. Specifically, local administrators are responsible for:

LA1. Managing all users' access privileges to data and programs.

LA2. Monitoring security-related events and following up on any actual or suspected violations, where appropriate; notifying network management of reported security incidents and assisting in investigating them.

LA3. Maintaining and protecting server software, relevant files, and media using specified security mechanisms and procedures.

LA4. Overseeing the update of anti-virus signatures on all local workstations and servers and for scanning server hard drives regularly.

LA5. Assigning a unique USERID and initial password to new users according to established procedures.

LA6. Promptly notifying network management and library management of all computer security incidents;

LA6.1. Notify the network management if a break-in is in progress; assist other local administrators in responding to security violations.

LA6.2. Cooperate with network management in tracking violators and assisting in enforcement efforts.

LA7. Backing up all data on network servers and workstations according to established procedure.

A Sample Password Policy

III C

Somewhere Public Library Password Policy

Purpose

All specific users of the Somewhere Public Library network are assigned user accounts administered by a central server. User accounts are composed of three elements: a user name, a password, and a configuration record on the server. A network user must submit his user name as a means of identifying his specific configuration record. The password is used to *authenticate* – to verify – that the user is who he claims to be.

This password policy is issued to specify the characteristics passwords must possess in order to maintain network security. Users are responsible for understanding and adhering to the following principles when creating or renewing passwords for their library account. Failure to observe these principles, or providing your password to other users, will be addressed according to library disciplinary policy.

Scope

This policy applies to all library staff, city personnel, contracted technical workers, and patrons assigned individual accounts.

Password Composition

Passwords that can be guessed by unauthorized personnel create the opportunity for breaches of security. To ensure maximum security, passwords must be hard to guess—not just by other human users but by extremely fast computers armed with multi-lingual dictionaries. You will create *strong* (hard-to-guess) passwords by following these instructions:

Must Nots:

- Your password must not contain your user name, your real name (first, middle, or last), your e-mail name, or any derivative of these.
- Your password must not be any single word in any language (password cracking software has access to language dictionaries for many, many languages).
- Your password must not be any fact associated with you: a pet's name, your birthdate, phone number, social security number, driver's license number, car license number, et cetera. Likewise, your password should not be a fact associated with your spouse or children.

Musts:

- Your password must be at least six characters long. Passwords 8-14 characters long provide optimal security.
- Your password must be a combination of uppercase and lowercase letters, numerals, punctuation marks, and other special characters. To a computer, the uppercase letters are different than lowercase letters. Three examples are shown below:

  `TriqsL6L`— this password has a mix of three of these categories, making it strong. But it also has a rhyming quality, making it easier to remember.

  `shorT#ducK`— this password also has a mix of three of the categories mentioned. Notice there are two unrelated words joined together, but with mixed case and with a special character between them. Joining two words this way also helps you remember your password.

  `Tqbfjotld`— this password has only two categories represented, but offers a seemingly random mix of letters. In this example, the memory aid is using an acronym of the well-known phrase, "The quick brown fox jumped over the lazy dog." Take a favorite quotation (probably not a famous one, though) and create an acronym by using a particular character from each word. Insert a special character for additional security.

III D

Sample Budgets

Budget Parameters

In Chapter 3 we looked at the costs related to installing and maintaining a computer network in libraries. Looking at the costs separately does not provide a real picture of what the collective costs mean to the library budget. In this document I present two budget configurations to show how significant the problem of sustainability is. Looking at these scenarios illustrates why I've listed lack of funding as the number one threat to the library's network resources.

Some possible equipment and operational costs associated with using technology (fax machines, telephones, additional air conditioning needed to dissipate heat created by the computers, and others) are not included in these budgets. Those included are listed to provide a realistic sense of what the library's actual costs may be. Here are some thoughts to keep in mind as you review the budgets:

1. The maintenance costs included assume the library must contract with commercial vendors for normal computer and network support. Maintenance costs are estimated at $100 per workstation per year. Server maintenance is estimated at $150 per year. Network equipment and printer maintenance is estimated at $100 per item per year.
2. When pooling maintenance funds, it may be possible to reduce the total of the pool by 10-30% (not every item will be worked on every year – unless equipment is unreliable or configured poorly). The

more equipment you add to the pool, the lower the actual maintenance fees per item tend to be.

3. The maximum number of years a piece of equipment is likely to be serviceable is presented in parentheses under the Annualized Replacement Cost column. Replacement cost is simply the original cost of the equipment divided by the expected number of years it will be serviceable.
4. While the budget figures may be shocking, they are reasonably accurate. However, in most libraries these costs will be mitigated, and Sample 3 shows the budget for a tiny library with adjustments for discounts wherever they can be acquired. Here are the mitigating factors I've included in Sample 3:
    - The cost for consumables under Supply Costs should be paid on a cost-recovery basis, so these costs have been zeroed out. Do be sure your library is recovering the full cost of wasted pages as well as those actually printed.
    - The ongoing costs for Internet connectivity are current average Texas rates. The costs do not include federal E-Rate discounts, which most libraries can expect to receive in the near term. Most libraries will qualify for a 50-90% E-Rate discount. I use 70% as an average.
    - Texas regional library system members in some areas of Texas have access to TANG technicians as a resource for maintenance. Others will find local volunteers. These will be able to provide routine maintenance of workstations and patch installations on workstations and servers, so I have zeroed out the cost for obtaining commercial technical support for these items.
    - Some libraries will seek donated computers (three years old) to replace five-year-old equipment. I've reduced the replacement cost of workstations by half. If the total for equipment replacement is still untenable, the library must seek additional grant sources or other local funding to sustain its network.

If you would like to play with the numbers for your library, the budget samples and a blank template are available in Word 97 format with the electronic version of this guide. See the reverse of the title page for the web address.

Sample 1. Tiny Library Network Configuration.

Item Description	Original Cost	Mainte-nance	Electri-city	Annualized Replace-ment Cost	Total Annual Cost
Equipment					
Public Workstations (6)	$ 8,400	$ 600	$ 90	$ 1680 (5)	$ 2,370
Staff Workstations (2)	2,800	200	30	560 (5)	790
Circ Workstation (1 staff; 1 public)	2,800	200	30	560 (5)	790
Automation Server	5,000	150	20	715 (7)	885
Internet Server	3,500	150	20	500 (7)	670
12-port Switch	1,400	100	5	175 (8)	280
ISDN Router	700	100	5	88 (8)	193
Network Laser Printer	2,100	100	25	525 (4)	650
Total Equipment Costs:	$26,700	$1,600	$ 225	$ 4,803	$ 6,628
Security					
Security Implementation	$ 1,250				
Security Audit	750				
Automation Server Patch Application (one hour bi-monthly/$60 per hour)		$ 360			$ 360
Internet Server Patch Application (one hour per month/$60 per hour)		720			720
Workstations (10; one hour each per six months/$50 per hour)		1,000			1,000
Other Recurring Costs					
Internet Service Provision (Access, DNS service, e-mail boxes)		1,200			1,200
Data Circuit (ISDN line)		720			720
Supply Costs					
Printer Paper		1,000			1,000
Toner/Ink cartridges		4,580			4,580
Media (tape cartridges, diskettes)		150			150
Total Annual Cost	$28,700	$11,330	$ 225	$ 4,803	$16,358

Sample 2. Small Library Network Configuration.

Item Description	Original Cost	Mainte-nance	Electri-city	Annualized Replace-ment Cost	Total Annual Cost
Equipment					
Public Workstations (20)	$28,000	$ 600	$ 300	$ 5,600 (5)	$ 6,500
Staff Workstations (4)	5,600	400	60	1,120 (5)	1,580
Circ Workstation (2 staff; 4 public)	8,400	600	90	1,680 (5)	2,370
Automation Server	5,000	150	20	715 (7)	885
Internet Server	3,500	150	20	500 (7)	670
DNS Server	3,500	150	20	500 (7)	670
24-port Switch	1,200	100	5	150 (8)	255
12-port Switch	600	100	5	75 (8)	180
T-1 Router	2,000	150	5	250 (8)	405
Network Laser Printer (2)	4,200	200	50	1,050 (4)	1,300
Total Equipment Costs:	$62,000	$ 2,600	$ 575	$ 11,640	$14,815
Security					
Security Implementation	$ 3,000				
Security Audit	2,000				
Automation Server Patch Application (one hour bi-monthly/$60 per hour)		$ 360			$ 360
Internet Server Patch Application (one hour per month/$60 per hour)		720			720
DNS Server Patch Application (one hour bi- monthly/$60 per hour)		360			360
Workstations (30; one hour each per six months/$50 per hour)		3,000			3,000
Other Recurring Costs					
Internet Service Provision (Access, e-mail boxes)		3,600			3,600
Data Circuit (ISDN line)		3,120			3,120
Supply Costs					

Printer Paper		3,000			3,000
Toner/Ink cartridges		13,740			13,740
Media (tape cartridges, diskettes)		300			300
Total Annual Cost	$67,000	$30,800	$ 575	$ 11,640	$43,015

Sample 3. Tiny Library Network Configuration, with Discounts.

Item Description	Original Cost	Mainte-nance	Electri-city	Annualized Replace-ment Cost	Total Annual Cost
Equipment					
Public Workstations (6)	$ 8,400	$ 0	$ 90	$ 840 (5)	$ 930
Staff Workstations (2)	2,800	0	30	280 (5)	310
Circ Workstation (1 staff; 1 public)	2,800	0	30	280 (5)	310
Automation Server	5,000	150	20	715 (7)	885
Internet Server	3,500	150	20	500 (7)	670
12-port Switch	1,400	100	5	175 (8)	280
ISDN Router	700	100	5	88 (8)	193
Network Laser Printer	2,100	100	25	525 (4)	650
Total Equipment Costs:	$26,700	$ 600	$ 225	$ 3,403	$ 4,228
Security					
Security Implementation	$ 1,250				
Security Audit	750				
Automation Server Patch Application (one hour bi-monthly/$60 per hour)		$ 0			$ 0
Internet Server Patch Application (one hour per month/$60 per hour)		0			0
Workstations (10; one hour each per six months/$50 per hour)		0			0
Other Recurring Costs					
Internet Service Provision (Access, DNS service, e-mail boxes)		with 70% discount: 360			with 70% discount: 360
Data Circuit (ISDN line)		216			216
Supply Costs					
Printer Paper		0			0
Toner/Ink cartridges		0			0
Media (tape cartridges, diskettes)		150			150
Total Annual Cost	$28,700	$ 1,326	$ 225	$ 3,403	$ 4,954

G

Glossary

A glossary of network security terms is provided in electronic format on the companion website.

B

Bibliography

A list of recommended materials for public libraries, describing network security using Windows NT/2000 operating systems

In Print

Anderson-Redick, Stacey. *Windows System Policy Editor*. Sebastopol, CA: O'Reilly & Associates, 2000. ISBN: 1565926498. $34.95. For an intermediate audience.

Benson, Allen C. *Securing PCs and Data in Libraries and Schools: A Handbook with Menuing, Anti-Virus, and Other Protective Software*. Neal-Schuman, 1998. ISBN: 1555703216. $125.00. A guide to the various aspects of workstation security, for a non-technical-to-intermediate audience.

Freed, Les and Frank J. Derfler, Jr. *How Networks Work*. Que Corporation, 1998. ISBN: 0789715953. $29.99. For a non-technical audience.

Kosiur, David. *Building & Managing Virtual Private Networks*. John Wiley & Sons, 1998. ISBN: 0471295264. $44.99. For a technical audience.

McInerney, Michael J. *Windows NT Security*. Prentice Hall, Inc., 1999. ISBN: 0130839906. $49.99. Well-rounded configuration manual, for an intermediate-to-technical audience.

Norberg, Stephan. *Securing Windows NT/2000 Servers for the Internet*. Sebastopol, CA: O'Reilly & Associates, 2001. ISBN: 1565927680. $29.95. Concise configuration manual, for an intermediate-to-technical technical audience.

Penfold, R. R. C. *Computer Security: Businesses at Risk*. Robert Hale. 1998. ISBN: 0-7090-6253-2. $24.95. A general guide for managers.

The SANS Institute. *Windows NT Security Step by Step*. The SANS Institute, 1999. $49.00. A concise, consensus guide (approved by 87 security professionals) to securing the Windows NT operating system, for a technical audience.

Scambray, Joel, Stuart McClure, and George Kurtz. *Hacking Exposed*. Second edition. McGraw-Hill Professional Publishing, 2000. ISBN: 0072127481. $39.99. Good coverage of a variety of network vulnerabilities, for an intermediate-to-technical audience.

Schultz, E. Eugene. *Windows NT/2000 Network Security*. Macmillan Technical Publishing, 2000. ISBN: 1578702534. $45.00. For a technical audience.

Wadlow, Thomas A. *The Process of Network Security: Designing and Managing a Safe Network*. Reading, MA: Addison-Wesley, 2000. ISBN: 0201433176. $34.95. Thorough coverage of the concepts of network security for managers.

Whitehead, Paul, and Ruth Maran. *Teach Yourself Networking Visually*. IDG Books Worldwide, Inc., 1997. ISBN: 0-7645-6023-9. $29.99. For a non-technical audience.

Wilson, Casey, and Peter Doak. *Creating and Implementing Virtual Private Networks*. Scottsdale, AZ: The Coriolis Group, 2000. ISBN: 1576104303. $39.99. For a technical audience.

Wood, Charles Cresson. *Information Security Policies Made Easy*. 7th Edition. Baseline Software. ISBN: 1881585069. $795.00. For an intermediate audience; especially recommended for regional library system professional collections. Offers over 1,000 "ready-to-use" sample network security policies on a comprehensive set of security issues. http://www.baselinesoft.com/ispme.html

Zwicky, Elizabeth D., Simon Cooper, and D. Brent Chapman. *Building Internet Firewalls*. 2nd edition. Sebastopol, CA: O'Reilly & Associates, 2000. ISBN: 1565928717. $44.95. An excellent resource, for a technical audience.

On the Web

10 Tips for Creating a Network Security Policy. Online: http://secinf.net/info/policy/10tips.htm (Available August 5, 2001).

Blackford, John and Al diGuido. "Business Guide to Network Computing." *Computer Shopper Extra*, July 1998. Online: http://www.zdnet.com/computershopper/edit/cshopper/content/extra/9807/ (Available August 5, 2001).

Bys, Cory. "Securing Windows 2000 Server," The SANS Institute, May 20, 2001. Online: http://www.sans.org/infosecFAQ/win2000/sec_server.htm (Available August 5, 2001).

CERT Coordination Center. *Windows NT Configuration Guidelines*. Carnegie Mellon Software Engineering Institute. April 2000. Online: http://www.cert.org/tech_tips/win_configuration_guidelines.html (Available August 5, 2001).

Cisco Corporation. *Networking Essentials for Small and Medium-sized Businesses*. Online: http://www.cisco.com/warp/public/779/smbiz/netguide/ (Available August 5, 2001).

Computer Security Resource Center (CSRC). *FIPS 191: Guideline for The Analysis of Local Area Network Security*. National Institute of Standards and Technology, November 1994. Online: http://csrc.nist.gov/publications/fips/index.html (Available August 5, 2001). The version at the CSRC site is in Postscript format. A PDF version of the document is available at http://www.rlwconsulting.com/ netsec/fips191.pdf

Crabb-Guel, Michele D. *The Network Security Roadmap Poster*. SANS Institute. Online: http://www.sans.org/newlook/publications/roadmap.htm (Available August 5, 2001).

Culp, Scott. "The Ten Immutable Laws of Security," Microsoft TechNet. Microsoft Corporation, October 2000. Online: http://www.microsoft.com/technet/columns/security/10imlaws.asp (Available August 5, 2001).

Culp, Scott. "The Ten Immutable Laws of Security Administration," *Microsoft TechNet*. Microsoft Corporation, November 2000. Online: http://www.microsoft.com/technet/columns/security/10salaws.asp (Available August 5, 2001).

Curry, David A. "Selecting Good Passwords." Online: http://www.alw.nih.gov/ Security/Docs/passwd.html (Available August 5, 2001).

Edwards, Mark Joseph. *Internet Security with Windows NT*. 29th Street Press, 1998. ISBN: 1882419626. $49.95. Online: http://www.windowsitlibrary.com/Documents/Book.cfm?DocumentID=121 (Available August 5, 2001). An introduction to network and Internet security for Windows NT for the intermediate audience.

Fraser, B., ed. *Site Security Handbook.* RFC2196. September 1997. Online: ftp://ftp.isi.edu/ in-notes/rfc2196.txt (Available August 5, 2001).

Gibson, Steve. "Shields Up: Internet Connection Security for Windows Users." Gibson Research Corporation. Online: http://grc.com/su-firewalls.htm (Available August 5, 2001).

Howard, Michael. "Secure Internet Information Services 5 Checklist," *Microsoft TechNet.* Microsoft Corporation, June 29, 2000. Online: http://www.microsoft.com/ technet/security/iis5chk.asp (Available August 5, 2001).

Kelley, Marcey and Wendall Mason. *Windows NT Network Security: A Manager's Guide* (CIAC-2317). CIAC, U. S. Department of Energy, December 1997. Online: http://www.ciac.org/ciac/documents/ CIAC-2317_Windows_NT_Managers_Guide.pdf (Available August 5, 2001).

Linksys International. *How to Build a Network.* Online: http://www.linksys.com/faqs/default.asp?fqid=15 (Available August 5, 2001).

Microsoft Corporation. "Implementing Guidelines for Strong Passwords," *Technical Resources, Security Services.* Microsoft Corporation, September 19, 1998. Online: http://www.microsoft.com/ ntserver/techresources/security/password.asp (Available August 5, 2001).

Microsoft Corporation. "Microsoft Internet Information Server 4.0 Security Checklist," *Microsoft TechNet.* Microsoft Corporation, March 15, 2000. Online: http://www.microsoft.com/technet/itsolutions/ security/tools/iischk.asp (Available August 5, 2001).

Microsoft Corporation. "Windows NT 4.0 Workstation Configuration Checklist," Microsoft TechNet. Microsoft Corporation, August 14, 2000. Online: http://www.microsoft.com/technet/itsolutions/ security/tools/wrkstchhk.asp (Available August 5, 2001).

Navy Secure Windows NT Guide. Department of the United States Navy, September 2000. Online: https://infosec.navy.mil/TEXT/ COMPUSEC/ntsecure.html (Available August 5, 2001).

National Center for Educational Statistics. *Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security.* U. S. Dept. of Education. Online: http://nces.ed.gov/pubs98/ safetech/index.html (Available August 5, 2001).

"Network Security Product Guide." *Resources for Librarians.* Texas State Library and Archives Commission. Online: http://www.tsl.state.tx.us/ld/pubs/ security/index.html (Available August 5, 2001).

NIST's Special Publication: Internet Security Policy: A Technical Guide [DRAFT]. Online: http://csrc.nist.gov/isptg/ (Available August 5, 2001).

Nolle, Tom. "Security Is Everybody's Business." *Network Magazine*. May 1, 2000. Online: http://www.networkmagazine.com/article/NMG20000517S0105 (Available August 5, 2001).

NSA Glossary of Terms Used in Security Intrusion Detection. Online: http://www.sans.org/newlook/resources/glossary.htm (Available August 5, 2001).

"NT Security Issues." *Internet/Network Security*. About.com. Online: http://netsecurity.about.com/compute/netsecurity/msub3.htm (Available August 5, 2001).

Others: Network Security Library: Network Security Policy. Online: http://secinf.net/ipolicye.html (Available August 5, 2001).

Rekhter , Y., B. Moskowitz, D. Karrenberg, et. al. *Address Allocation for Private Internets*. RFC 1918. February 1996. Online: ftp://ftp.isi.edu/in-notes/rfc1918.txt (Available August 5, 2001).

Rosch, Winn L. "Planning a Small Network," *The Winn L. Rosch Hardware Bible*. Fifth edition. Online: http://hardwarebible.com/Network%20Guide/ (Available August 5, 2001).

The SANS Institute. "Windows Issues," *Information Security Reading Room*. The SANS Institute. Online: http://www.sans.org/infosecFAQ/win/win_list.htm (Available August 5, 2001).

The SANS Institute and Network Computing. "Security Alert Consensus: Windows Alerts," *SANS Institute Security Digests*. The SANS Institute. Online: http://www.sans.org/newlook/digests/SAC/windows.htm (Available August 5, 2001).

Satnam Bhogal, Satnam. *FAQ for How to Secure Windows NT*. The SANS Institute, March 8, 2001. Online: http://www.sans.org/infosecFAQ/win/NT_FAQ.htm (Available August 5, 2001).

secinf.net. *Network Security Library*. Online: http://secinf.net/ (Available August 5, 2001).

"Security Services," *Windows NT. Technical Resources*. Microsoft Corporation, April 21, 1999. Online: http://www.microsoft.com/ntserver/techresources/security/default.asp (Available August 5, 2001). Various papers on configuring Windows NT security and using Windows NT security utilities.

SecurityFocus.com. Online: http://www.securityfocus.com/ (Available August 5, 2001). A general security site with a variety of security information.

Stein, Lincoln D., and John N. Stewart. *The World Wide Web Security FAQ*. Version 3.1.0. July 28, 2001. Online: http://www.w3.org/Security/Faq/ (Available August 5, 2001).

"What Do I Put in a Security Policy?" Online: http://secinf.net/info/policy/policy.htm (Available August 5, 2001).

Windows IT Security. http://www.ntsecurity.net/ (Available August 5, 2001). A Windows-specific security site.

Windows Registry Guide. Online: http://registry.winguides.com (Available August 5, 2001).

Windows Security Guide. Online: http://security.winguides.com (Available August 5, 2001).

By E-mail

SANS Newsletter Subscription Service. The SANS Institute. Online: http://www.sans.org/sansnews (Available May 1, 2001). A site providing free sign-up for three e-mail-based security newsletters.

Product Security Notification. Microsoft Corporation. Online: http://www.microsoft.com/technet/security/bulletin/notify.asp (Available August 5, 2001). Description of free service providing e-mail notification of product security bulletins. Recommended for the security administrator for Microsoft products.

Periodicals & Columns

Information Security Magazine. TruSecure Corporation. Online: http://www.infosecuritymag.com/ (Available: August 5, 2001).

Network Magazine. CMP Media, Inc. Online: http://www.networkmagazine.com/ (Available: August 5, 2001).

"Security." *Network Computing*. CMP Media, LLC. Online: http://www.networkcomputing.com/core/core7.html (Available: August 5, 2001).

Testing & Analysis Tools

DumpEvt. "SomarSoft Utilities," SystemTools.com. Online: http://www.somarsoft.com/ (Available August 5, 2001).

DumpSec (formerly DumpACL). "SomarSoft Utilities," SystemTools.com. Online: http://www.somarsoft.com/ (Available August 5, 2001).

netcat. "netcat 1.1 for Win95/NT is released," L0pht Heavy Industries. Online: http://www.l0pht.com/~weld/netcat/ (Available August 5, 2001).

Nmap (Unix/Linux version). insecure.org. Online: http://www.insecure.org/ (Available August 5, 2001).

nmapNT (Windows NT version). "nmapNT sp1 from eEye Digital Security," eEye Digital Security. Online: http://eEye.com/html/Research/Tools/nmapnt.html (Available: August 5, 2001).

SAINT (Security Administrator's Integrated Network Tool; Unix/Linux). World Wide Digital Security, Inc. Free version. Online: http://www.wwdsi.com/saint/downloads/saint-3.2.3.tar.gz (Available August 5, 2001).