1997

CPA's guide to information security

John Graves

Kim Hill Torrence

Kent
Information
Services

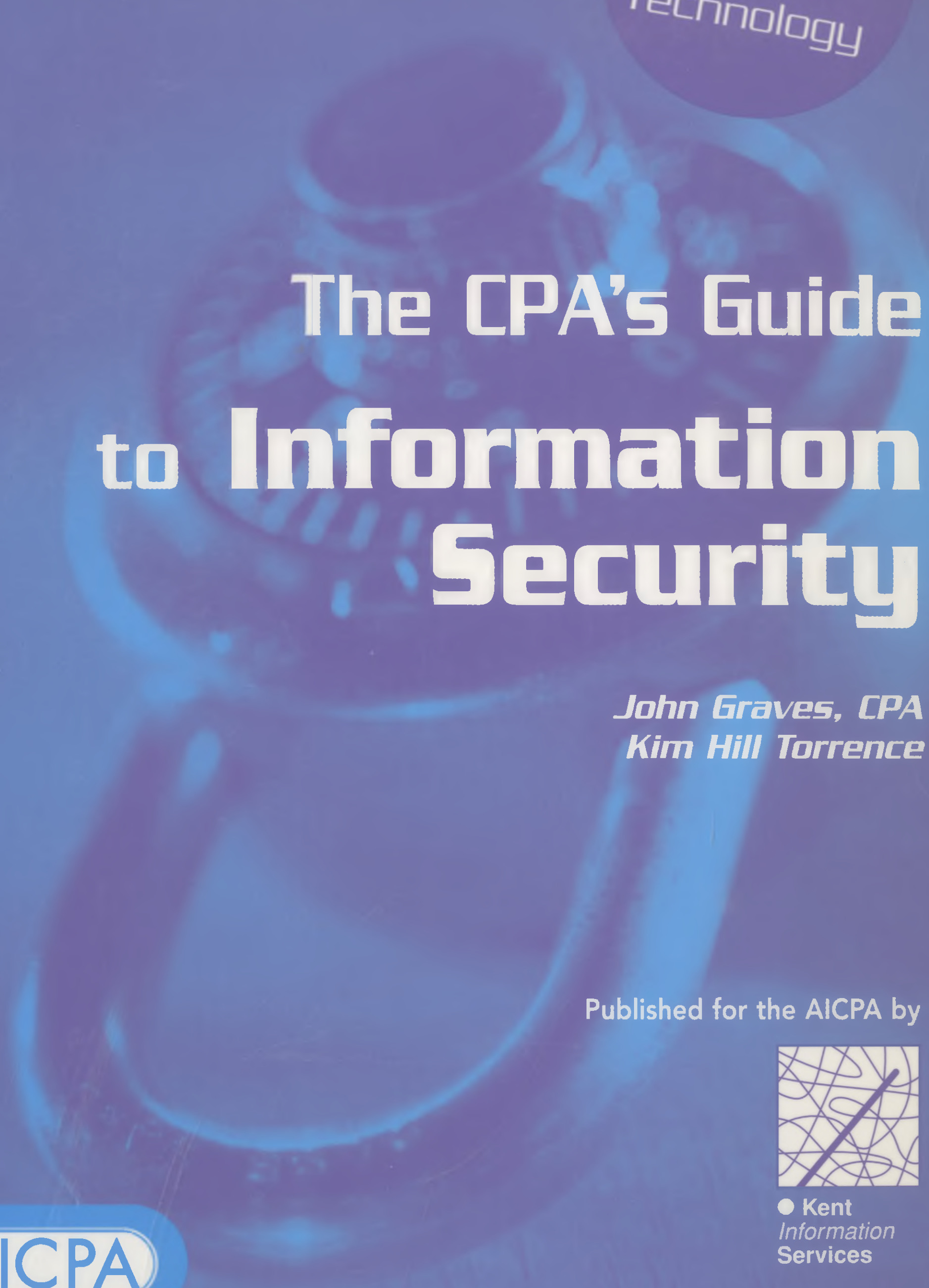
Graves
Torrence

The CPA's Guide to Information Security

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

A Top 10 Technology



The CPA's Guide to Information Security

John Graves, CPA
Kim Hill Torrence

AICPA

Published for the AICPA by
Kent
Information
Services

AICPA Technology Series

The CPA's Guide to Information Security

John Graves, CPA
Kim Hill Torrence

Published for the AICPA by

Kent
Information
Services

AICPA Technology Series

Title:

THE CPA'S GUIDE TO INFORMATION SECURITY

Authors:

John Graves, CPA
Kim Hill Torrence

Kent Information Services, Inc.
155 N. Water St., Suite 205
Kent, OH 44240
http://www.kentis.com
email@kentis.com
+1 330.673.1300 voice
+1 330.673.6310 fax

Table of Contents

Acknowledgements

Although publications typically credit one or two primary authors, the development of this book has truly been a team effort. We would like to thank the following colleagues who contributed their knowledge, skills, and time to the creation of this book:

Matt Curtin, Chief Scientist with Megasoft Online, Inc., who wrote Chapter 6, "Network Security," provided material for other sections of the book, and completed a technical review of the entire manuscript.

The policy authors and information security teams at Contra Costa County, California, Hermann Hospital, and the Arctic Region Supercomputing Center, who generously gave permission to reprint their security-related documents in Appendix A.

Lisa F. Allen, Editor at Kent Information Services, Inc., who compiled the "Information Security Resources" list of Internet sites, the Glossary, and the Index of this text.

Scott Stillisano and Christopher Graves of Kent Information Services, Inc., who performed page layout and document production tasks with patience and good humor.

May 30, 1997
John Graves, CPA
Kim Hill Torrence

Chapter 1
Information Security Planning

In the 1996 Datapro Information Security Survey, 67% of US companies responding stated that they had a dedicated corporate function for information security. Fifty-four percent of companies confirmed having a published information security policy in place, and another twenty-six percent said that they planned to develop such a document in the next 12 months. In view of these statistics, it is clear that information security planning is a major concern of companies nationwide, and that it will continue to be so in the years to come. Currently, the response to information security concerns seems to be the establishment of a formal information security function and the publication of various security and computer-use policy documents in accordance with an information security planning process.

This book will prepare you to coordinate your organization's information security planning through a step-by-step method using a team approach. By considering the topics presented in chapter order, you will make your way through the various concepts related to information security and conduct comprehensive information security planning in the process. Along the way, you'll consider the benefits of documents such as a Computer Use Policy and an Information Security Policy, and decide which components of these documents are relevant to your organization. By way of introduction, we'll review the following topics in this chapter:

- The role of the CPA in information security.
- The balancing concept of risk management.

- The Information Security Team–who should participate?
- The coordination of planning, practice, and policy in information security, and how best to use this book.

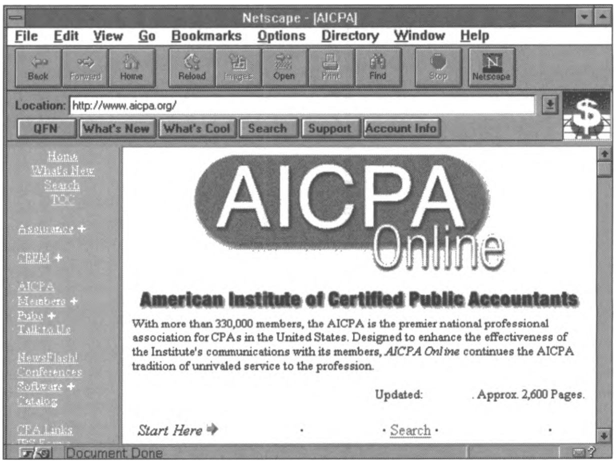
The Role of the CPA in Information Security

Few of us have been left untouched by the information revolution. Workpapers and analyses that used to be prepared with pencils and ledger sheets are now prepared with personal computers with spreadsheet programs. The two- or three-day delivery mailed letter has been replaced by the five-minute delivery electronic mail message. We maintain databases of information that we can access with a keyboard or mouse instead of rifling through file drawers. The flow of information has gotten bigger, faster, and, to be honest, more difficult to control.

For a profession such as accounting, in which issues of confidentiality and assurance are paramount, electronic information presents new and important challenges. Few of us would give up our notebook computers or Internet research capabilities, but many of us would like to know just who has access to our computer system and what information is available to them. In addition to our own concerns, we have clients and colleagues asking us which data security measures are most effective and how to construct information security policies and plans.

For these reasons and many others, the Information Technology Division of the AICPA rated "Security" the number one technology affecting the accounting profession in 1997. The explosive growth in use of local area networks, portable computers, and the Internet have all contributed to the critical importance of this subject. At a time when the popular press is reporting almost daily on Internet scares and cracker intrusions, accountants need to be able to separate the hype from the legitimate concerns and construct effective information security mechanisms for themselves, their organizations, and their clients.

In many organizations, especially smaller offices and mid-sized companies, the CPA serves as a general business manager and information services expert. In addition, CPAs are entering technology consulting in increasing numbers. In his inaugural address to the AICPA in late 1996, current president Robert Mednick stressed the important roles that CPAs can play in advising clients on the selection of technology for their needs and building procedures for its effective use. You can find many documents addressing the role information technology in the accounting profession at the *AICPA Online* Web site at **http://www.aicpa.org**.


Netscape - [AICPA]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop Netscape
Location: http://www.aicpa.org/
QFN What's New What's Cool Search Support Account Info
Home
What's New
Search
TOC
Assurance +
CEFM +
AICPA
Members +
Pubs +
Talk to Us
NewsFlash!
Conferences
Software +
Catalog
CPA Links
AICPA
Online
American Institute of Certified Public Accountants
Start Here
Search
Document Done

With more than 330,000 members, the AICPA is the premier national professional association for CPAs in the United States. Designed to enhance the effectiveness of the Institute's communications with its members, *AICPA Online* continues the AICPA tradition of unrivaled service to the profession.

Updated: . Approx. 2,600 Pages.

Figure 1.1
AICPA Online Web site, source of information on how technology is affecting the accounting profession.

In addition, CPAs are often responsible for specific security-related tasks in information systems projects. Audits and quality assurance reviews are commonly the responsibility of the CPA, who is often also the operations, administrative, or accounting manager leading the systems development project. As new transaction-oriented systems built on electronic commerce and electronic data interchange (EDI) models flourish, this role is likely to expand and extend into other departments.

Experts project that 6.5 billion dollars' worth of retail sales will take place via the Internet in the year 2000 (Forrester Research, Cambridge, Massachusetts). This very specific security concern is only one of the issues for corporations in the technology age: consider, for instance, the thousands of corporate Internet sites that do not utilize electronic commerce, and the hundreds of thousands of local area networks in use in organizations today. When we broaden our perspective to include the millions of stand-alone desktop and laptop personal computers in use by businesspersons–computers containing valuable documents that represent work product and proprietary corporate information–well, the security concerns can be overwhelming indeed.

Fortunately, pioneering information scientists and security analysts have developed organized, methodical approaches to considering information security issues. For instance, the 1996 Datapro survey discussed above indicates that corporate information security planning usually falls into the following categories:

- Authorized software use.
- Computer viruses.
- Microcomputer/PC security.
- Disaster recovery.
- Release of proprietary information.
- Dial-up security.
- Mainframe security.

- Computer ethics.
- Client/server security.

In addition, US organizations describe the major threats and risks to information security in a relatively small group of categories, ranked in order of perceived importance:

- Viruses and malicious code.
- Unauthorized network/system access.
- Internet access.
- Password exposure.
- Theft of computer equipment.

When seen from this vantage point, information security planning seems a little more manageable, and the results seem much more predictable. By following the step-by-step approach presented in this book, you can help your organization or a client's company plan for information security and implement the policies appropriate for specific computer-use scenarios.

Risk Management: The Balance of Security

It's very important to understand that, in security, one simply cannot say "What's the best firewall?" or "How can I prevent absolutely any theft from occurring in my office space?" There are two extremes: absolute security and absolute access. It is an old adage among security experts that the closest we can get to an absolutely secure computer is one unplugged from the network and its power supply, locked in a safe, and thrown to the bottom of the ocean. Unfortunately, the computer isn't terribly useful in this state. By contrast, a machine with absolute access is extremely convenient to use–it's simply there, and will do whatever you tell it, without questions, authorization, passwords, or any other mechanism. However, this isn't terribly practical (or safe), either. Corporate networks and the public Internet are, unfortunately, the media of some destructive persons.

This is no different from our daily lives. We constantly make decisions about what risks we're willing to accept. When we get in a car and drive to work, there's a certain risk that we're taking. It's possible that something completely out of control will cause us to become part of an accident on the highway. When we get on an airplane, we're accepting the level of risk involved as the price of convenience. However, most people have a mental picture of what an acceptable risk is, and won't go beyond that in most circumstances. For instance, if you happen to be upstairs at home, and you want to leave for work, you're probably not going to jump out the window. Yes, it would be faster and more convenient, but the risk of injury outweighs the advantage of convenience. Similarly, every organization needs to decide where between the two extremes of total security and total access it needs to be. In the approach recommended in this book, you will be making these decisions in the context of a group of managers and stakeholders in the information of your organization–the Information Security Team.

For financial professionals, computer consultants, and attorneys, risk analysis is a common activity with structured parameters. For instance, the illustration below shows the model developed by Jyrki Kontio at the University of Maryland for assessing risks in software development (**http://www.cs.umd.edu/~jkontio/Riskit.html**):

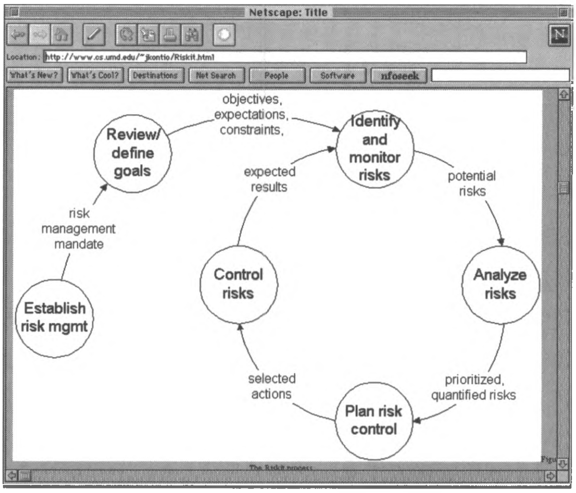


Figure 1.2 *The Riskit process of the "Riskit Method for Software Risk Management."**

The concepts used in information security risk analysis are really quite similar. In Chapter 7, we'll show you how to bring together the information you've gathered throughout the planning exercises in this book and establish a comprehensive information security policy based on the assets you're trying to protect and the likely threats to those valuable information resources.

The Information Security Team

If you are planning security for a single PC used by one person, clearly that person is the only one that needs to be involved in the planning. If the system is larger or shared by multiple users, the planning gets a bit more complex. The more you include various groups in security planning, the more easily accepted the final security measures will be. A security guideline needs to be followed to be effective, and it is much easier to get people to adhere to rules that they have been a part of creating. This is especially the case if your organization decides to implement a

* Figure reprinted with permission. Copyright 1997, Jyrki Kontio, all rights reserved.

Computer Use Policy or an Information Security Policy as part of its information security planning.

An important first step in security planning is making contact with all parties that will be affected by the security measures to be implemented. If passwords have never been required and you have decided that they should be utilized, users need to be contacted and the change in practice explained. People can also be designated as responsible parties for various aspects of the site's security. The security planning should also define the responsibilities of users, system administrators, and system managers. In most offices, the computers or local area networks are overseen by a network administrator, who might be a dedicated staffer or someone whose responsibilities include coordinating network activity.

Deciding who will be part of your organization's information security team is a relatively simple matter if you use the concept of "stakeholder" to guide you. In the field of data processing, a stakeholder is anyone in the organization who has a role in creating or using the documents and data stored on the computers or networks. For instance, the marketing department is a stakeholder in mailing list and marketing database data and applications; the accounting department is a stakeholder in the accounts payable and receivable and payroll data; and the R&D group is a stakeholder in the research databases residing on an organization's system. In addition, each of these departments probably would have at least several users of shared computing resources, such as a network, and, therefore, would be affected by security measures such as new virus protection practices. When building your information security team, be sure to include: a coordinator (perhaps yourself), the system or network administrator, a representative of each group of users of the system(s), and a representative of all stakeholder groups.

Planning, Practice, and Policy: Using this Book

This book is about information security PLANNING. The concept of security planning is much more broad than simply buying anti-virus software or drafting a policy. An adequate information security planning process will address: mechanisms for revisions and update when technology changes; assigned responsibilities for security issues; and a clear statement of an organization's information security objectives and acceptable levels of risk. An information security plan might be a simple, one-page document stored in the network administrator's file cabinet, and the contents of the plan might be put into practice simply through the network administrator's activities. In larger organizations, or ones with more complex information systems, the information security plan will be a large, distributed entity that encompasses several policies, a set of formal procedures, and additional documentation such as logs. Specific documents such as an Information Security Policy and a Computer Use Policy might cover only certain topics or address a more narrow range of issues.

In this text, we first present a consideration of issues that the PC and Internet users of your organization need to consider. Chapter 2, "Individual Computer Use," discusses how you and your organization's staff can protect sensitive personal information when communicating via electronic mail or the World Wide Web. You'll learn how to help employees devise and use effective system passwords. In addition, we review important issues such as acceptable use, appropriate Internet conduct, and copyrights which can affect how you use the information you find on the Internet, and how to determine appropriate computer-use practices for employees.

The next three chapters present terms and concepts involved in organizational information security in three categories: physical security; viruses, and encryption. In Chapter 3, "Physical Security," you'll learn about the mechanisms available to protect your organization's computers from theft and tampering. The importance of regular and adequate data backups is discussed, along with a presentation of the various types of backup media and equipment available. Finally, we'll take a look at the importance of planning for how your organization will move forward with critical business functions in the event of a physical disaster that destroys computer equipment.

Chapter 6, "Network Security," presents an overview of the considerations important for groups of interconnected computers and networks connected to the Internet. Rather than taking an environment-specific approach, this chapter presents concepts common to all networks, giving advice on how to customize the strategies for specific platforms such as Novell's *Netware* or *Windows NT.* Through a consideration of the general ISO/OSI Reference Model for networks, this chapter explains the levels of network operation and the security concerns related to each.

At the end of each of these chapters, you will find a planning section and a worksheet. Here, you can assess your organization's current practice or policy in the subject area of the chapter and plan for the changes you might recommend to your information security team. You can use the worksheet yourself or in the context of your team's planning effort to ensure that you have considered and planned for the security risks discussed in each chapter.

The final chapter, "The Information Security Policy" discusses what you need to consider to build an organization-wide Information Security Policy for your own or a client's site. From analyzing risks and threats to dealing with policy infractions, this chapter presents a comprehensive listing of those issues that will impact your organization's implementation of a formalized policy.

Each of the chapters of this book shares several features. As noted above, the final section of each chapter is comprised of a list of planning considerations and a worksheet. Before the planning section, each chapter contains a list of sources of additional information on the chapter's subject, under the "Learning More About . . . " heading. At the end of this text, you will find a listing of Internet sites with useful information for CPAs organized under the categories of Accounting, Auditing, Searching, and Security.

In addition, Appendix A contains sample security-related policies for your review, and Appendix B contains the text of the InterNIC's important Site Security Handbook, reprinted for your convenience.

Chapter 2
Individual Computer Use

When planning for your organization's information security, you will likely assign responsibility for certain tasks to different persons. For instance, your local area network administrator might be responsible for assigning and implementing the rights to certain server directories and stored information, and your operations manager might be responsible for implementing the physical security measures discussed in Chapter 3. However, there will be certain security concerns that are common to all employees of the organization, or, at least, all employees that use the computing resources of the firm.

In addition, when employees begin to traverse a space like a local area network or the Internet with work computers, the circumstances can sometimes change faster than the rules. In this chapter, we will alert you to some risks involved when employees use work computers and additional risks they incur when accessing the Internet or other online services at work and how to avoid them, including:

- Acceptable use.
- Information access rights.
- Passwords.
- Personal information and the Internet.
- Professional presence and professionalism.

Lastly, we'll discuss a specific document you can use to structure each person's use of your organization's information resources: The Computer Use Policy. Organizations that implement such policies often use them to address individual rights and responsibilities when using computers and to define the parameters of acceptable activities.

Acceptable Use

The phrase "acceptable use" covers a wide range of behavior and activities. In general, it is used to describe what an organization will allow employees and users to do with its computer systems. Acceptable use parameters can clarify issues such as whether or not employees are permitted to use computers for personal work such as freelance jobs or college papers, whether or not games or other non-work-related activities are allowed, and what the intended uses of organizational computer systems are. For instance, the "Acceptable Use" section of the Security Policy of the Queensland Parallel Supercomputing Facilities stipulates that the following activities are prohibited by users of computer resources: (1) playing games; (2) accessing other computers to play games; (3) antisocial activities; and (4) activities that are likely to detrimentally affect other users (see the full policy online at **http://www.qpsf.edu.au/admin/security.html**).

Many organizations documents the terms of acceptable use of computer equipment, along with the penalties for deviating from acceptable uses, in the form of an employee policy. As with the other security issues discussed in this chapter, you may wish to document such terms in a Computer Use Policy to be distributed to all employees. When defining what will constitute acceptable use of your organization's computers, you and your Information Security Team may want to consider specifically prohibiting the following types of uses, depending on the level of protection you wish to enforce:

- Personal correspondence via email.
- Personal work.
- Playing computer games.
- Installing personal software.
- Violating any software license agreement.
- Distribution of proprietary or confidential company information.
- Accessing, or attempting to access, unauthorized confidential information, files, or data.
- Any illegal activity under federal, state, or local law.
- Using computers for any purposes other than specifically defined in an acceptable use statement (such as using a specific set of applications or programs to complete work-related tasks).

Information Access Rights

In addition to the risks posed by misconduct, you will probably wish to protect certain types of confidential or propietary information that resides on either stand-alone computers or networked computers in your office. The people who pose a risk for compromising this information reside in two places: inside your organization and outside your organization. This section will cover concerns related to threats from internal personnel. Chapters 5, 6, and 7 cover issues related to external persons.

When thinking about internal information access rights, you can use the simple analogy of a filing cabinet to consider the threats and alternatives for protection. For instance, if you are the payroll manager of a large corporation, it is likely that you keep your hard-copy payroll files under lock and key all day long. Probably only one or two other persons have access to these files–maybe your secretary and perhaps your boss, the vice president of administration. If a manager of a particular department comes to you for payroll information on her department's employees, you will release to her the files relevant to her own employees, not the files for her peer managers or the employees of another department. It would be understood that this manager would not release the payroll information for one employee to another, and that she would not publish her department's payroll information company-wide or world-wide.

Now, for comparison, let's suppose that you have an automated payroll software system that runs from the server of your local area network. Perhaps that system has built-in password authorization levels in place for managers to access information in their employees' payroll records. Perhaps the system administrator has implemented a step whereby a manager can only read that information, but to change it, say, to give an employee a pay raise, she must have the approval of you, the payroll manager. These are useful security measures, and you should use them as appropriate for your organization, but their efficacy depends on each authorized person using the information only as intended. As an example: what good would the multi-level password system be if the manager accessed the confidential information in an authorized manner, but then printed it on her laser printer, photocopied it, and gave a copy to each company employee?

What you need in this instance is a clear definition of the information access rights of each level of employee in your organization. Even if these "rights" are defined by software parameters, you should document why they are in place and how employees should handle data after they have retrieved it. If, for instance, the marketing research your company spends millions of dollars to conduct is crucial to its competitiveness, employees should be made aware that it is proprietary, protected information. We know of one company that administers its local area network as follows: each employee has only a workstation computer and operating software on their desk; all application software and data reside on the network server; and it is a violation of policy for any employee to store any company data on the hard drive of their desktop computer workstation–period. Another firm handles the same issue in this slightly different way: each department stores the data necessary for its operation in a separate sub-directory of the network server; certain employees have password rights to retrieve (but not modify) the data in certain departments' sub-directories; however, no one is authorized to store a copy of protected data from another department's sub-directory in their own department's sub-directory.

When deciding about information access rights, you can use a rule of thumb common to the medical and legal professions, called the "need to know" rule. According to this rule, only employees who need to know information to perform their jobs should have it. For instance, a manager who evaluates employees' performance and grants merit raises obviously needs to know her employees' salaries, but very few other people do. Everyone in the company probably needs to know the contents of the company's strategic plan, but very few people need to know the competitor analysis on which certain aspects of the plan were based. As you work through the level of information that particular classes of employees "need to know," you can use a table to keep track of your decisions.

Passwords

Passwords are the oldest line of computer defense. Although passwords have been used for almost 30 years, they are still misunderstood and misused. Employees who think nothing of using a key to get into their offices may balk when asked to enter a password to use the company computer system. In the early days of mainframe computing, physical access to the computer console could be controlled and a system would have only 30 to 100 users. Today a computer that is fully connected to the Internet has millions of potential users. In this section you will learn to make your own computer system passwords safer, and, by extention, how to include such guidelines in company-wide practices.

If you have an account on a shared system, such as a *Unix* system, you may think that since you have nothing sensitive in your account, you don't need to worry about the security of your password. Most system attacks involve more than just the account to which the intruder gains access; that account is used as a springboard for further attacks, so the security of the entire system depends on the security of each account. At Kent State University, the Department of Mathematics and Computer Science runs a large network of *Unix* machines. The department was not concerned about password security, until a visiting professor left her account open to remote log-ins. Someone used her account to install and run programs designed to crack the root password to gain access to every file on the system. System administrators worked two weeks of 24-hour days to clean up and secure the system. You should make every effort to use a secure password. Implementing every other aspect of information security correctly can be instantly negated by ineffective user passwords.

Some common password problems are easy to avoid. The most common password security problems are "Joes." Joes are account passwords that are variations of the name of the account's owner. One consulting company theorized that there is at least one "Joe" account on every system, and found at least one such account on every client's system that the team tested. This problem most often results when users are assigned default passwords, such as their last names, when accounts are created, and then employees don't change them to something more secure. To avoid this problem, accounts should never be given default passwords that are easily guessed, and users should be informed how to change their passwords and advised to do so the first time they use their account to log-in to the system.

Another password problem occurs when accounts have no password or some commonly-known default password. Some application programs that need access to shared information will create an account for the program at installation and set the password to some common default. Even some operating systems set up guest or demo accounts with no password when they are installed. To prevent problems like these, always make sure that you understand the installation of system software and its effect on the password files. If the software requires shared accounts, be certain that you change the password to something other than the default so every purchaser of the software doesn't have access to the account on your machine. (Consult Chapter 6 about network security in local area network environments.)

Some users of your system may have accounts on many machines within the company or elsewhere. These users will often use the same password for each account they hold. Using the same password for different systems is secure only when

- The two systems are logically equivalent, like two PC file servers in the same company.
- The two systems are run by the same information system center with the same security measures.

If the systems are run by different organizations, have different security levels, or have different operating systems, users should have a unique password for each system. Let's say that you have an account on your local file server and also on a commercial database system. If someone cracks your password on the local system and they discover that you have an account on the database server, the cracked password will be the first thing they try when they attempt to gain access to your other account.

Password Security Checklist

Use this list to help employees choose passwords that are safe and appropriate. You might wish to include the checklist as part of your organization's Computer Use Policy or Information Security Policy.

1. Is your password shorter than eight characters? Increasing the length of your password from six to eight characters makes a cracker check many more possibilities.
2. Is your password "letmein," "password," "hello," or some other clever response to the password prompt? These are commonly known and are the first checked by cracker programs.
3. Is your password your log-in name in any form? Is it your license plate number, telephone number, street name, or the make of car you drive? Information like this is easy to discover, and so it makes an insecure password.

4. Is your password all digits (like "12345678"), or a repeated character (like "aaaaaaaa")? Is it a repeated sequence of digits, or a keyboard pattern (like "12341234" or "asdfasdf")? Passwords like these significantly decrease the length of time needed to crack a password.
5. Is your password in ANY dictionary? Crackers first check words in online dictionaries, both in English and some other languages.
6. Is your password a word in a dictionary modified by prepending or appending a digit? Passwords like "house1" are not secure; cracker programs check appended and prepended digits as a matter of course.
7. Is your password a word constructed by rotating or reversing one of the above classes? For example, Frank may think that "knarf" (his name backwards) or "rankf" (his name with the first character moved to the end) is more secure than his name, but this is not true.
8. Is your password an example taken from a printed source?

If you answered "no" to all of the questions above, your password is probably secure. If it is not, consider the following suggestions:

1. If the system distinguishes between upper and lower case letters in a password, mix the case of letters in your password. "TomCaT" is more secure than "tomcat" or "TOMCAT."
2. Use non-alphabetic characters INSIDE the password. "Tom3CaT" is more secure than "TomCaT" or "TomCaT3."
3. Choose a line or two from a favorite song or poem and use the first letters of each word. For example, "To be or not to be, that is the question'' becomes "2Bon2btit?"

4. Choose two short words and concatenate them together with a punctuation character between them. For example: "dog+rain," "book!mug," "kid?goat."
5. Choose an adjective, a noun, a verb, and an adverb. This will make a (possibly nonsense) sentence that you can remember. Now use the first two letters of each word for your password. For example: "Orange Cars Fly Silently" becomes "OrCaFlSi."

You often will find warnings about not writing your passwords down. Keeping them online in a file is certainly not advised, nor is writing them on Post-It notes and sticking the notes to your monitor or to the underside of your keyboard. But, keeping a note in your purse or wallet containing your password is probably OK. It is better to have a secure password that you have to write down to remember for the first couple of weeks than it is to have a password that is so easy to remember that anyone could crack it.

Personal Information

Many employees are unaware of the conventions of network and Internet conduct, and, more importantly, they also are not familiar with the security risks of using computers in such an environment. You can help employees avoid some of these risks by making them aware of how and when to release personal information on computer networks, how to apply the standards of professional conduct in the online world, and how to protect sensitive or copyrighted organizational information. You may wish to include guidelines to this effect in your organization's Computer Use Policy. This section describes how to handle personal information on the Internet and how to help your employees do the same.

In general, the "billboard maxim" is a good rule of thumb to remember when using all areas of the Internet. The billboard maxim goes something like: "When using the Internet, never post anything that you would not mind seeing on a billboard." Would you want your credit card number painted on a billboard? Probably not. Would you want your home address and phone number to be there? Would you wish to see your checking account number, the name and addresses of your kids' schools, or your car license plate number on a busy freeway billboard? See how it works? On the other hand, you probably wouldn't mind having your company name, your office address, your position title, or your email address distributed publicly–many businesspersons routinely do this to promote their services. You might even feel comfortable painting your work phone number or pager number on a billboard. If you use this rule of thumb before posting personal information, you can avoid unintentionally compromising your own privacy.

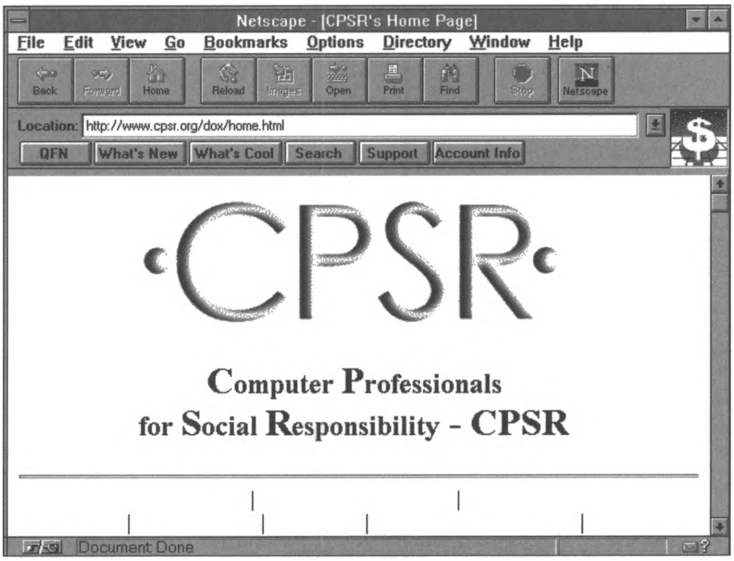
In the case of transmitting credit card numbers, extra caution is mandatory. Never release your credit card number to anyone on the Internet through a public area such as Usenet or a subscription mailing list. Even email is a risky way to transmit such information. Remember that the shared communication lines of the Internet can be compared to the telephone party lines of years gone by. Anyone with a couple of pieces of equipment and moderate programming skill can "crack" their way into Internet communication lines and search for distinctive sequences of characters like credit card numbers.

Reputable commercial online services, Internet service providers, and online vendors have put considerable effort toward protecting your credit card number when you conduct online transactions. They will always inform you of these measures when asking you to provide your number. For instance, *CompuServe*, a major commercial online service, informs users that they are accessing the *CompuServe* computers through secured, closed telephone circuits when they provide credit card information during the initial procedure for obtaining an Internet account. In addition, commercial online services such as *CompuServe* provide secured communication lines for dial-up users, and they store credit card information on computers that are not attached to the Internet. Unless you are accessing your commercial online service account through an Internet-based function, like Telnet, your line is very secure. If you don't feel certain that appropriate security measures are in place, don't release your credit card number. Instead, send an email to any prospective vendor asking what protection is in place, or find another way to order goods or services from that vendor.

In recent months, software developers have been working to find convenient ways to conduct secure credit card transactions via the World Wide Web (see Chapter 5 for a discussion of how the process of encryption fits into these methods). This will be an important development for commercial use of the Internet. You may even be thinking about the services you could provide to clients over the Internet and how you might obtain payment for them. It is cumbersome and expensive to achieve security by dedicating one computer to credit card transactions and another to Internet access.

Chris Hibbert, of the Computer Professionals for Social Responsibility, makes a very good argument for protecting your Social Security Number with the same rigor as any other confidential information. Hibbert reminds us that a Social

Security Number is often the only piece of verifying information an institution will ask for before releasing highly sensitive information such as credit history or medical records to a requesting party. To learn about techniques for protecting yourself from invasion of privacy through access to your Social Security Number, retrieve and read the FAQ document at **ftp://cpsr.org/cpsr/privacy/ssn/oldSSN/ssn.faq.html**. This site also contains other information on computer security and privacy issues and the group also maintains a Web site at **http://www.cpsr.org/dox/home.html**.


Netscape - [CPSR's Home Page]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop Netscape
QFN What's New What's Cool Search Support Account Info
·CPSR·

Location: http://www.cpsr.org/dox/home.html

Computer Professionals for Social Responsibility - CPSR

Document Done

Figure 2.1 *Computer Professionals for Social Responsibility Web site.*

Electronic Mail

Sending email over the Internet is like sending a post card. Email messages can be intercepted, read, and altered, unless you make your messages secure. Sales of software that insures the security of Internet messages have been soaring among corporate accounting and finance departments, banks, investment advisors, and stock brokers. These groups have been using the Internet to communicate sensitive financial data and have a compelling need to keep their communications secure. While it is easy to understand why a stock broker and client might need to have a channel for secure messages, it is more difficult to consider this need in terms of casual or general messages. To consider your need for message security, remember the billboard maxim. Do you regularly send messages via an internal network or the Internet, perhaps personnel recommendations or contracts, that you would not wish to see painted on a billboard? If so, you may want to investigate message security systems. In general, message security is provided by encryption software. See Chapter 5 for a complete discussion of the processes of encryption and decryption, how they work, and how to select good encryption software. If you intend to require that employees use a method for keeping email messages secure, you will want to include guidelines for this process in your Computer Use Policy or Information Security Policy as discussed in Chapter 5.

Professional Presence on the Internet

Many companies are giving employees access to electronic mail and other Internet functions, and for good reason. Electronic communication greatly enhances productivity and reduces overhead costs for items such as express delivery and long distance calling. Online research can save time and dollars, and the information to be gleaned from subscription mailing lists and Usenet newsgroups is very valuable. However, granting employees Internet access carries with it an additional set of risks. It is much more difficult to control your company's image and the information released when each employee can speak on behalf of the company in a world forum of many millions of Internet users. One way to lessen the risks of employee Internet access is to establish guidelines for company and personal use of tools such as email. Another is to provide information to employees about how to handle sticky online situations and present your organization in the best possible light. Taken together, the rules of Internet conduct are sometimes called "Netiquette." Although they may seem like only niceties, Netiquette guidelines can determine how your organization is perceived through the individual Internet communications of its employees. Observing these guidelines can help your organization protect one of its most valuable assets–its image. In addition, intellectual property and copyright issues can expose your firm to a whole new set of risks.

Netiquette

Just like any other kind of manners, the rules of behavior on the Internet, collectively called "Netiquette," are based mostly on common sense and common goals. The Internet is a community of millions of individuals interacting with each other. It has grown by leaps and bounds over the last several years because it is the fastest, most economical, most efficient way to communicate with others. The tenets of Netiquette aim to keep the Net just that way: fast, economical, and efficient. If you keep these goals in mind during your Net travels, you'll avoid embarrassing errors and project the competent, helpful image so important to accounting professionals.

Email

Most of your Internet communication with individuals will be through email. You'll certainly use email to correspond with clients and colleagues, and you may use it to take up private conversations with people you've met online (perhaps in a Usenet newsgroup or subscription mailing list). In both cases, you will want your reader to be able to easily identify your message, understand its contents clearly, and do both of these things quickly. So, the Netiquette guidelines for email aim toward the objectives of identification, clarity, and brevity.

If your mail program has an option for inserting your real name in the **From** field on your email messages, use it. It is much easier to recognize a person's name than an email address. Most *Unix* shell accounts allow a user to customize the **From** field as an option while composing each message. PC-based mail management software allows the user to change the **From** field so it will appear in modified form on every message. In addition, you can further identify your message by using a clear and descriptive subject line. Subjects like "Response," "Request," and "Query" are not very helpful to readers who may receive 50 such emails per day. On the other hand, subjects like "Request for Book Prices" or "Staff Meeting Minutes (4/30)" can help your readers organize their correspondence and their workdays.

Netiquette guidelines for writing style are the subject of lively debate among Internet users of all types. There is certainly room for individual expression and style in email writing, and each person must decide what it means to be clear and concise. Long-time Internet guru Mark Moraes has compiled a useful set of writing guidelines for Usenet postings; they apply equally well to all kinds of Internet correspondence. You can find this guide, called *Hints on Writing Style for Usenet* in the newsgroup ***news.announce.newusers***, where it is posted regularly. In addition, there are some general points on which most people can agree when discussing the text of email messages:

Your Reader Cannot See You: Email, although lightning fast and very cheap, leaves some important channels of interpersonal communication closed. In email, you cannot highlight certain phrases in your message with facial expressions, body language, or gestures. While you may make a comment jokingly, your email reader may take it seriously. Using emoticons such as a smiley face :) or markings such as the grin symbol <g> can help to make up for the chuckle that your reader cannot hear, although overuse of such markings can be annoying to readers.

In contrast, the Internet equivalent of shouting at someone is TYPING IN ALL CAPITAL LETTERS. You may be perfectly calm and friendly, but the use of all capital letters will convey an aggressive tone in email correspondence. Save the use of all caps for strong emphasis only, and you'll avoid startling your readers. This guideline applies to email message subject lines as well. It is very annoying to be confronted with a list of email headers shouting their subjects first thing in the morning on a busy office day.

Business as Usual: Always remember that the documents you send via the Internet are just as real, official, and enduring as the ones you send on your company letterhead. This means that you should give email messages and discussion group postings the same attention as your printed correspondence. Take the time to check the spelling and grammar of your messages. Use the same professional tone in Usenet postings as you would in any other letter. Your Usenet and email messages might be stored on disk for months or years and used for later reference–make sure they represent you professionally.

In addition, some basic conventions of business communication become even more important in electronic communication. Perhaps the most important is making sure that the objective of your correspondence and the desired action of the reader are perfectly clear. You can test your message by reading it over before you send it and asking yourself what you would do if you received it. Will your reader know what action should be taken in response to your message? Have you identified an action step (like, "Please respond by December 11 if you will be attending the conference")? Does your reader know how to reach you, via phone or regular mail if not by email? Is your reason for sending the message clear to your reader (for instance, "I am commenting on your draft of the overtime policy")?

Use Excerpts Sparingly: Many Internet correspondents include excerpts of previous messages in their responses to emails or Usenet postings. This can be very helpful to a reader who can use the excerpt to identify the conversation to which the message belongs and place your response in context. The common practice is to precede each line of an excerpt with a special character such as a caret (>) and to set it off from the rest of the message by indenting it or double-spacing it from the body of the message text. Many PC-based mail management programs now have automatic functions for handling excerpts, as do many *Unix* shell mail management tools. While this courtesy can be helpful, it can also be over-used. Consider your reader's perspective when deciding whether or not to excerpt a message you're responding to. Will the excerpt help your reader remember an issue or topic of discussion? Will it clarify your message? Or, will it merely add bulk to your message or take the place of a sentence or phrase that you could have written? We recommend using excerpts only when other ways of expressing your point are not as effective or feasible.

Keep Your Signature Simple: In email jargon, the word signature refers to a standardized document closing that appears at the bottom of an email message or Usenet posting. Many types of Internet software allow a user to create a personalized signature block that is automatically appended to each message the user sends. Most people use the signature section to include helpful contact information such as company name, company phone number, organizational affiliation, or return address. Some imaginative persons, however, use this space to create elaborate drawings with ASCII characters or to insert a favorite quote from a politician or philosopher. It's a matter of personal taste, of course, but we strongly recommend against elaborate, creative signatures. A signature of three lines or less is usually considered appropriate. Again, the criterion for judging your own signature block is simple: does this signature contribute to the goal of fast, economical, efficient communication? If not, don't use it.

Usenet Newsgroups

The basic Netiquette guidelines for Usenet newsgroups are the same as those for email, outlined above. However, the sheer number of persons participating in newsgroups makes for more potential problems. So, first remember that your Usenet posting is essentially an electronic mail message–one that will be delivered to hundreds or thousands of readers. Whatever you do will impact those thousands of persons, and you should plan accordingly. The guidelines outlined below have one thing in common: in newsgroups, time solves most problems. Take the time to learn about the subject of the newsgroup; take the time to think before sending a message; and give the other newsgroup subscribers a chance to respond or drop a volatile subject.

It's easy to identify "newbies" in a newsgroup (newbies are inexperienced Internet users). They are the people who post inappropriate questions; for instance, they post a message to the Celtic Culture newsgroup (***alt.celtic***) asking how to delete email messages from their mail program in-boxes. Also easy to spot are online crabs. Crabs spend time correcting trivial facts in other postings. They split hairs on subjects tangent to the thread discussion. They are quick to point out spelling and grammar errors in others' messages. Even worse, newbies and crabs sometimes make postings under a particular thread subject that are entirely irrelevant to the thread. If you spend a little time observing a particular newsgroup before jumping into the discussion, you'll avoid tipping anyone off to your newbie status or presenting yourself as an online crab.

First, subscribe to the newsgroup and do nothing but read the postings for a week. You'll soon be able to identify the frequent and prolific participants in the newsgroup and their particular areas of expertise. Second (and you can do this during your week of waiting and reading), download and read the newsgroup's FAQ (list of frequently asked questions). FAQs are some of the most useful resources available on the Net, compiling the questions frequently asked by users new to the group or new to the subject. The answers have been honed over time by experts on the subject. FAQs are often subject to public review and revision, so you can usually be confident that the information in this document is fairly accurate and current. Then, dip your toes into the newsgroup by posting a question or a response to someone else's question. By now, you'll be confident that you are posting your comment to the appropriate newsgroup in a relevant subject area. Keep your comments brief and to the point, and you're on your way to rewarding newsgroup interactions.

The Internet equivalent of picking bar fights is called "flaming." Flaming is the practice of being unnecessarily belligerent, rude, denigrating, or otherwise hostile in Internet email, newsgroups, mailing lists, or other public-accessible space on commercial online services, such as discussion forums. Flaming usually occurs in Usenet newsgroups, and it is annoying and time-wasting for the thousands of other newsgroup members who wish to use the Internet to exchange useful information and take part in constructive conversations.

The best way to put out flames is to ignore them. If someone's posting is out-of-line or inappropriately negative and personal, simply don't respond. Perhaps the other newsgroup subscribers will follow suit, and the flamer will lose interest. Even if the debate continues, at least you are not stuck spending time on childish name-calling. If you feel that you must respond to a flame, perhaps because it was directed at you or you feel strongly about the subject, compose your reply carefully and with a level head. Then, leave your computer keyboard for a few moments and send the reply only after you have returned and reconsidered sending it. If you cannot avoid the temptation of responding to a flame, send only one reply to avoid escalating the interchange into an unnecessary waste of time and Internet resources.

If you are having a hard time ending an online disagreement with someone because they will not let the matter drop, you can report the harassing behavior to the system administrator of the offender's Internet service provider. The address of a system administrator is usually sysadmin followed by the domain, as in: **sysadmin@domain.name**. If this address does not work, you can try addressing a complaint to the system postmaster: **postmaster@ domain.name**. Either way, use this option as a last resort, because system administrators are very busy people and arbitrating between Internet users is not a very good use of their time.

If you feel that any online behavior directed toward you or anyone else is illegal (such as physical threats or fraud), you should report this behavior to your local law enforcement authorities. As a last note of caution, remember that divulging your home address or phone number in a newsgroup posting is roughly equivalent to painting it on a billboard. Newsgroups are public discussions, and you have no control over who reads your postings. If you would like to share personal information with someone you have met online, make sure that you know and can trust your correspondent, and then release the information only in a private email message. And, NEVER release your credit card number or bank account number to anyone in a newsgroup. Legitimate vendors provide separate, secured circuits for online ordering, and they inform their customers of these security measures as part of the ordering process.

Subscription Mailing Lists

When participating in Internet mailing lists, you should follow the same guidelines as those described for Usenet, above. There is one other possible slip to make with mailings lists, however, and you should be careful to avoid it. When requesting information on a mailing list, subscribing to, or un-subscribing from the list, remember to address your email message properly to the **majordomo, listserv,** or **listproc** as indicated in the subscription instructions. If you send such a message to the list name, your administrative message will be sent to all list subscribers. It will annoy them, embarrass you, and, in the case of a new subscription, it will provide a very poor introduction for you in the group of Internet and professional peers you are hoping to join.

Marketing and Commercial Use

This subject covers a great deal of ground, and marketing on the Internet has become a very murky area since the Net was opened for commercial use. An important distinction to remember is the difference between the public and the commercial areas of the Internet. If you keep this distinction in mind, you can avoid participating in inappropriate commercial activity in public Internet areas. Public areas are the newsgroups, mailing lists, and document repositories of sites open to the public. In general, commercial solicitation and marketing activities are prohibited in public areas. Commercial areas are sites established by for-profit entities specifically for commercial activity. You can conduct marketing in these areas only.

For instance, posting a newsgroup message listing your accounting expertise, contact information, and hourly fees is not permitted on Usenet–this is marketing in a public area. Posting such a message to many newsgroups (called "spamming") is very poor form and is prohibited by most Internet service providers (who will cancel your account if you do it). However, posting such a message in the Classified Advertisements section of a commercial online service such as *CompuServe* is entirely appropriate, and so is sending an email message to someone in a newsgroup or mailing list who specifically requests this information. You can also respond to a specific request for this type of information in the context of a related newsgroup.

Savvy users of the Internet realize the great benefit to be gained by establishing a presence as an expert in particular newsgroups or mailing lists. While this is not strictly considered marketing activity, it is certainly one way to promote your expertise and reputation. For instance, if you gain the respect and trust of newsgroup users by consistently answering questions on accounting topics with reliable and clear information, you'll probably find that other newsgroup subscribers occasionally contact you via private email to inquire about your services. At this point, you are free to negotiate with this potential client and do any self-promotion you wish.

Copyrights

An initial caveat: This section is intended to guide Internet users in learning about the concept of copyright and the issues relating to copyright pertinent to Internet use. This is not legal advice or a substitute. If you think you need legal advice regarding your own material or your use of someone else's copyrighted material, please consult with an attorney. Discussing the exact facts of your situation with an attorney is the best way to protect yourself.

The basic concept of copyright, although intimidating and confusing for many, is really fairly simple. The first portion of the word, "copy," refers to text–that is, words appearing in a certain order as expressed by a certain person or entity. The words you are reading in this text constitute copy. They are words expressed by authors in a certain order and manner, and they appear here on the page as copy. The second part of copyright, the "right" part, refers to the legal concept of holding rights to intellectual property. So, a copyright is a way of expressing the legal rights of someone who has created an original text or work.

Basically, anyone who creates a work (and this category includes many non-language objects such as songs, photographs, and computer programs) holds a group of rights relating to the work's reproduction, distribution, revision, performance, and other related activities. Since 3/1/89, when the U.S. adopted the International Berne Convention, the creator of an original work holds copyright to the work from the moment it is fixed in a tangible form, whether or not the document is published and whether or not a copyright notice appears on the work. Anyone who wishes to use the work for any purpose other than personal information is obligated to obtain the creator or copyright owner's permission to do so. This is the law, and it's that simple–use any portion of someone else's words or creative work without permission, and you've violated their copyright.

In reality, and in the courts, there are certain circumstances in which one can technically violate copyrights of another without being legally liable. This group of circumstances is sometimes referred to as "fair use." Unfortunately, there are no objective measures of fair use, and this legal concept gets interpreted in many different ways. In general, fair use is reproduction or use of a work which both does not harm the commercial value of the original work and also indicates no potential for commercial gain on the part of the user. Some examples of activities that could be considered fair use are: quoting a copyrighted work in a critical review of the work, reproduction of a small portion of a work for educational purposes, and using illustrative passages from a work in a scholarly article. For our purposes, using the Internet to conduct business and personal communication, we can assume that everything appearing on the Internet in any form is copyrighted unless the document specifically states that its creator has released it to the public domain, thereby forfeiting all copyright benefits. This assumption applies to all objects on the Internet, including newsgroup postings, email messages, computer programs, digitized photographs, clip art, and so on. Many files you will encounter on the Internet are already in violation of copyright by virtue of being posted to the Net; for instance, images scanned from published documents are the intellectual property of the document creator or publisher. Thus, you cannot use any file you find on the Internet for anything other than your personal information or its intended purpose (reading an email, using a program on your personal computer, or responding to a posting) unless you have the permission of the work's creator. Period. This is the safe and courteous way to operate on the Internet, and it avoids possible confusion regarding permissible fair use, various copyright laws and their years of effect, and legal interpretation of limited licenses.

For the most part, it's fairly easy to avoid infringing someone's copyright. Most importantly, copyright does not apply to facts and figures, only to the author's original way of expressing the information. For instance, as part of our research in creating this text, we have read Terry Carroll's excellent six-part FAQ on copyright available in many Usenet newsgroups or for FTP download from **rtfm.mit.edu** (you should download it and read it too–it's the most comprehensive and understandable document available regarding copyright issues and Internet use). Some of the facts we have used, such as the fact that the U.S. adopted the Berne Convention in 1989, came from that document. However, we have refrained from using, or even substantially paraphrasing, Terry Carroll's own words and expression in that document, because such activities would infringe his copyright. It happens that Carroll has included a copyright notice on his FAQ, but we would be obliged to respect his copyright even if he had not done so.

If you wish to use someone's copyrighted material in your own document, permission is usually easy to obtain (provided, of course, that you will not benefit from the use at the author's expense). For instance, suppose that you would like to quote a paragraph of someone's informative mailing list message regarding relational databases in your own report for a client recommending the purchase of personal computer software. You can simply drop the author a note explaining your request and exactly how the material will be used. If the author grants permission, keep a copy of the letter or email message for your file and proceed with your use. However, if you change the use you are making of the material, even if only by distributing it more widely than you originally described, you must obtain permission again.

As you might assume, copyright violations are usually only litigated in serious cases where the creator/plaintiff has the financial resources to bring the suit to court and the defendant has made a blatant violation and has gained financially from the violation at the creator's expense. However, using someone else's material without their permission, whether or not you intend to gain financially, is both against the law and is in very poor Netiquette taste. To keep the Internet the cooperative, mutually beneficial community it has come to be, always respect copyright and give permission freely for reasonable use of your own material.

The best way to ensure that people are aware that you intend to protect your own copyright to a work is to place a copyright notice on it. A notice is not necessary for a copyright to be in effect; however, if your document carries a notice, you can now easily show that a person who violated your copyright was indeed aware that the document was copyrighted, and this can be useful in litigation. To construct a copyright notice on your document, use these three components: (1) the letter "c" within a circle or the word copyright spelled out, (2) the year of the work's first publication, and (3) the name of the owner of the copyright. For instance, the copyright notice appearing on this text is:

Copyright 1997. Kent Information Services, Inc.

Another level of protection for you as an author or creator of a work is to register your copyrighted work with the U.S. Copyright Office. Registration consists of sending two copies of the work to the Copyright Office, along with a registration form and filing fee. Call the Copyright Office hotline at (202) 707-9100 to obtain information and registration packets for all types of works. U.S. law currently requires a U.S. copyright owner to register a work before infringement litigation. This may change, but registration is surely a good way to communicate your intent to protect a work.

The Computer Use Policy

All of the issues discussed in this chapter can be documented in a Computer Use Policy and distributed to all employees. In addition, employees should be made aware of their responsibilities for performing information security tasks such as virus scanning, encryption of messages, and protection of physical equipment, as discussed in other chapters of this book. To begin a Computer Use Policy, you can use the following topics as a starting point. Then, as you progress through this book, you will probably add individual rights and responsibilities as they come up in your Information Security Team's planning activities.

- Acceptable use parameters.
- Devising and using appropriate system passwords.
- Releasing personal information over the Internet.
- Appropriate and professional Internet behavior.
- Releasing confidential or proprietary organizational information to anyone, internal or external.
- Guidelines for use of copyrighted material.

The policy should state clearly what the penalties will be for violation of certain terms, and whom employees should contact if they need clarification of topics covered in the policy.

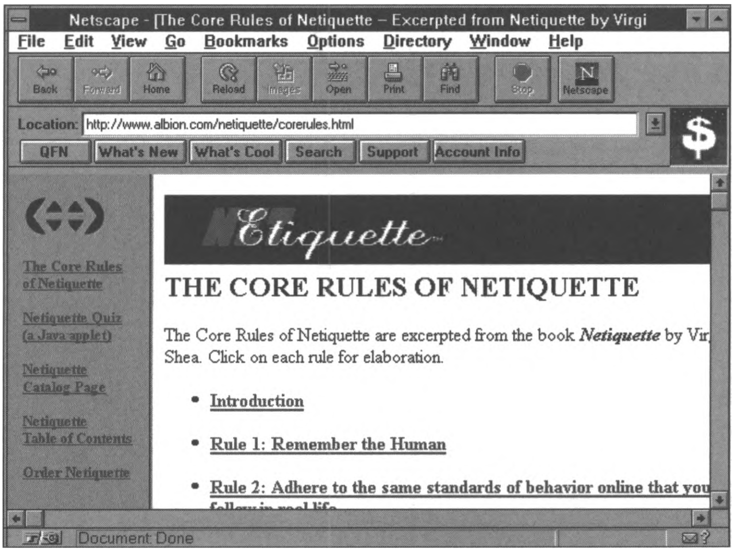
Learning More about Individual Computer Use Issues

If you decide to establish a Computer Use Policy for employees, there are several samples available online that you can use as a basis. One well-researched one is provided by the Computer

Professionals for Social Responsibility group discussed above. At their Web site (**http://www.cpsr.org**), CPSR provides "A sample E-mail and Voice-mail policy" (**http://www.cpsr.org/dox/program/emailpolicy.html**). ON Technology, a provider of network security software, has issued a white paper to help companies compose Internet usage policies, available at **http://www.on.com**.

The Privacy Rights Clearinghouse, a non-profit group begun at the University of San Diego, operates a Web site located at **http://www.privacyrights.org/**. Here you can find a series of papers on personal security and privacy and how technology affects individual rights. This site also contains a list of useful links on security and privacy issues.

To learn more about Netiquette, visit *The Core Rules of Netiquette* site at **http://www.albion.com/netiquette/corerules.html**. This site is provided by Albion Books, publisher of Virginia Shea's book called *Netiquette*. Shea has here provided links to excerpted material in many of the categories she treats in her book.



Netscape - [The Core Rules of Netiquette – Excerpted from Netiquette by Virgi

Location: http://www.albion.com/netiquette/corerules.html

THE CORE RULES OF NETIQUETTE

The Core Rules of Netiquette are excerpted from the book ***Netiquette*** by Vir
Shea. Click on each rule for elaboration.

- Introduction
- Rule 1: Remember the Human
- Rule 2: Adhere to the same standards of behavior online that you follow in real life

Document Done

Figure 2.2 *The Core Rules of Netiquette Web site containing excerpts from the book Netiquette.*

Visit the informational Web site at **http://spam.abuse.net/spam/** to learn more about guidelines for appropriate commercial use of Internet functions. Established by an international group of concerned Internet users, this site provides definitions, sample policies, and specific techniques for users and site administrators to block unwanted "spamming" activity.

CCC Online is a site maintained by the Copyright Clearance Center (CCC), a not-for-profit organization created at the suggestion of Congress to help organizations comply with U.S. copyright law (**http://www.copyright.com**). At this site, you can learn how to obtain an account to automate your payments for use of copyrighted material. You can also visit the "Resource Center" section of the site to find links to many other sources of information on copyright law.

Individual Computer Use Planning Worksheet

Area	Current Policy or Practice	Points For Revised Policy/Practice
Define the acceptable use of organizational computing resources.	Policy [ ] Practice[ ]	
Establish information access rights for various categories and levels of data and employees (attach separate table if necessary).	Policy [ ] Practice[ ]	
Ensure that passwords comply with the Password Security Checklist beginning on page 20.	Policy [ ] Practice[ ]	
Familiarize employees with personal security issues as they affect use of Internet functions such as email, Usenet newsgroups, and subscription mailing lists.	Policy [ ] Practice[ ]	

Familiarize employees with the guidelines of Netiquette.	Policy [ ] Practice[ ]	
Educate employees about copyright law and ensure that it is observed.	Policy [ ] Practice[ ]	
Establish what organizational information is confidential or proprietary and establish guidelines for its distribution.	Policy [ ] Practice[ ]	
With the Information Security Team, decide whether individual computer use issues will be addressed in an Individual Computer Use Policy or with the organization's Information Security Policy.	Policy [ ] Practice[ ]	

Chapter 3
Physical Security

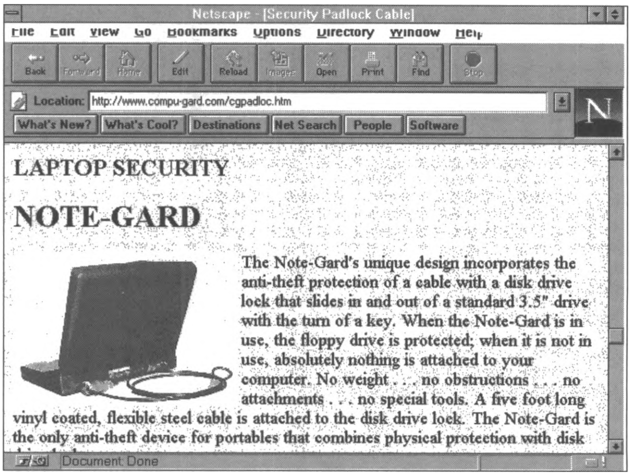
Many businesspersons think that information security is concerned exclusively with complicated computer code and system administration schemes. But, in fact, sophisticated software-based approaches cover only one aspect of information security. Planning for the physical security of your organization's information systems can be just as important. For instance, what good does an elaborate, password-based security system do if someone can walk into your offices and walk out with the PC on which the crucial data is stored? In this chapter, we'll review

- Secure office computing concepts.
- Data backup procedures.
- Disaster recovery planning.

Secure Office Computing

For some reason, many managers just don't think about their computers in the same light as other important company resources such as marketing plans, the checkbook, or personnel files. But they should–computers hold all of the information contained in these traditional items and much more. Strategies for keeping computers physically safe are much the same as keeping any other office resource safe, and they are based on limiting access to the equipment, making the equipment stationary, and securing the office in which the equipment resides.

Common sense is the best guide in office security. By placing computers only in lockable rooms, you can gain a great measure of security. For computers that must be located in common areas such as reception rooms or shared cubicle installations, office supply companies sell a variety of cables and plates that can be used to deter theft. Computer Security Products, Inc. (**http://www.ComputerSecurity.com/**), a company that provides such equipment, reports that the theft of computers now accounts for over 10 billion dollars per year in losses. Compu-Gard, another physical security product vendor, sells a unique disk locking and cable combination device that also protects notebook computers, which are very vulnerable to theft:


Netscape - [Security Padlock Cable]
File Edit View Go Bookmarks Options Directory Window Help
Back
Forward
Home
Edit
Reload
Images
Open
Print
Find
Stop
Location: http://www.compu-gard.com/cgpadloc.htm
What's New?
What's Cool?
Destinations
Net Search
People
Software
Document: Done

LAPTOP SECURITY

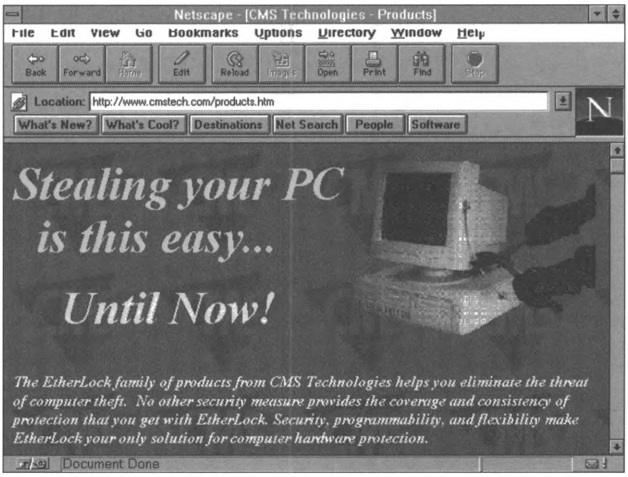
NOTE-GARD

The Note-Gard's unique design incorporates the anti-theft protection of a cable with a disk drive lock that slides in and out of a standard 3.5" drive with the turn of a key. When the Note-Gard is in use, the floppy drive is protected; when it is not in use, absolutely nothing is attached to your computer. No weight . . . no obstructions . . . no attachments . . . no special tools. A five foot long vinyl coated, flexible steel cable is attached to the disk drive lock. The Note-Gard is the only anti-theft device for portables that combines physical protection with disk

Figure 3.1 *Compu-Gard's Note-Gard product for securing notebook computers.*

For offices that may have problems with the theft of internal computer components, Barracuda Security (**http://www.powernet.co.uk/barracuda/**) provides an expansion-card device that detects unauthorized tampering and emits a loud alarm. The card also distributes indelible dye on internal PC components when activated, making it more difficult for someone to sell stolen parts such as highly-portable random-access memory chips or communication cards. CMS Technologies (**http://www.cmstech.com/products.htm**) has designed a product that protects PC workstations on a LAN through the existing network wiring. Their Web page gives a graphic illustration of how easy it can be to clip the cables on lock-down devices (just like cutting a bicycle lock cable):

Figure 3.2 *CMS Technologies Web site, featuring various computer security products.*


Netscape - [CMS Technologies - Products]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://www.cmstech.com/products.htm
What's New? What's Cool? Destinations Net Search People Software
N
Stealing your PC is this easy...
Until Now!
Document: Done

The EtherLock family of products from CMS Technologies helps you eliminate the threat of computer theft. No other security measure provides the coverage and consistency of protection that you get with EtherLock. Security, programmability, and flexibility make EtherLock your only solution for computer hardware protection.

When selecting among these types of security products, you will need to balance the potential risks against the expense and installation costs of the devices. For instance, if you have an elaborate office alarm system with motion detectors and video cameras, it probably would be redundant to install security devices on each PC. However, if your client has a PC located in a very public area with wide access, such as a sales desk in an auto supply store, you would be wise to recommend equipment to physically secure the computer to the counter. And, once you have made sure that computers are installed securely, you should also ensure that only authorized employees have keys to the offices where they are kept and that there is a rigorous procedure for distributing the keys and reclaiming them. Lastly, you should make sure that your computers are properly insured so they can be replaced promptly if the worst happens.

Data Backup Procedures

Security experts who plan for the data security of large mainframe installations use complex terms like volume dumps, incremental dumps, synchronization, and geometric device differences. These IS professionals are responsible for planning for the possible restoration of the contents of many large data storage devices, each of which can hold many gigabytes of information–often the data of organizations such as banks, healthcare facilities, and universities. When disaster strikes such a data center, the lives of hundreds or thousands of persons can be affected by the loss of the data.

In contrast, most physical incidents associated with personal computers and local area networks are, relatively speaking, minor problems. When the hard drive on an employee's desktop computer finally gives out, you can usually have a new one installed by the next office day. If a computer gets dropped during an office move, your insurance policy provides for its replacement. If a worker's notebook computer is stolen during a business trip, you can arrange for shared time on an office machine while a new one is purchased.

But, what about the data that is lost during these incidents? If you don't have backup copies of your critical files and software applications, what should be a minor inconvenience can become a major productivity set-back, or worse. Companies that don't provide for some sort of regular, procedure-driven backup system are asking for big trouble. However, those that do so are able to weather the small and large storms associated with being so dependant on those "boxes" on our desks.

When you think about data backup procedures for your organization, you have two categories of decisions to make. The first is technology-dependent: what hardware and software will you use to make duplicate copies of the contents of the hard drives of computers? The second category of decisions is situation-dependant: what procedural system makes the most sense for your organization? Because data backup technology runs the gamut of prices, it might make sense to approach the technology category first by deciding how much your organization is willing to spend for reliable backups and how much training you are willing to provide to employees. Then, you can integrate these factors into the data backup procedures.

The simplest and least expensive way to perform a backup of the contents of a PC's hard drive is to use the backup function of the computer's operating system. *DOS, Windows 95, Unix,* and *OS/2* all provide for some sort of prompted backup from the hard drive to floppy diskettes. If you've ever used this method, you've probably already discovered some of its problems–it's time-consuming and cumbersome to perform a "manual" backup. To make manual backups somewhat easier, you can purchase specialized backup or utility software. *Norton Utilities, FastBack,* and *PC Tools* are examples of DOS and Windows-based programs that are inexpensive and easy to use. UniTrends Software Corp. (**http://www.unitrends.com**) is one of the many companies making such programs for the *Unix* platform.

Next on the cost/complexity continuum is a group of hardware devices for backing up data. Still the most-used of such equipment, streaming tape drives were very popular in the late 1980's and early 1990's. Designed as either internal devices (requiring a card slot) or external devices using a serial or parallel port, tape drives provide convenient storage of large amounts of data on high-volume tapes formatted especially for the purpose.

Tecmar Technologies (**http://www.tecmar.com**) is a large producer of tape backup hardware in several formats.

Netscape - [Tecmar Technologies, Inc.]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://www.tecmar.com/prod/prod.html
What's New? What's Cool? Destinations Net Search People Software
N
TECMAR TECHNOLOGIES
WANGTEK • WANGDAT • PROLINE
PRODUCT INFORMATION
WANGTEK
Document: Done

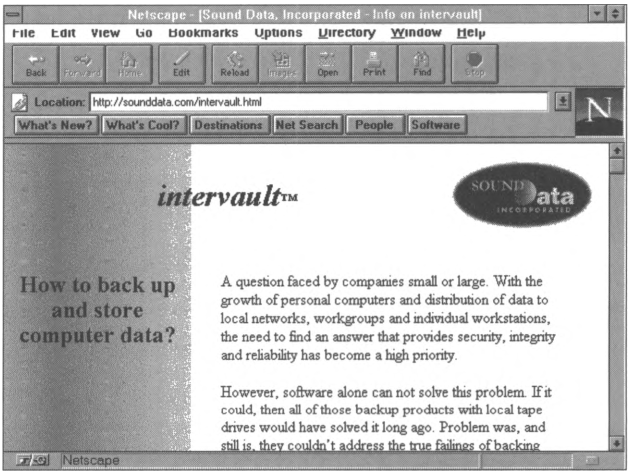
Easily the most popular of all tape formats, the Travan and DC6000 QIC drives are ideal for backup and data storage applications for workstations, personal computers and LAN backup. Capacities range from 250 megabytes to 8GB.

Figure 3.3 *Web site of Tecmar Technologies, producer of tape backup systems.*

Tape backup can be very convenient for organizations with a LAN, on which the server backup can be performed by one person, or organizations that assign one person responsibility for backing up each PC every week or specified interval. However, due to the linear nature of magnetic tape wrapped around spooling reels, these storage tapes do not generally accommodate any other uses than restoring data. Many smaller organizations find tape drive backup systems expensive and difficult to use, and they do not have the staff necessary to dedicate one person's time to ensuring that everyone's PC is backed up regularly.

More recently-developed backup and storage options work around some of these problems. Bernoulli and Iomega are two companies that manufacture lines of disk drives that use high-volume, removable disks. With one of Iomega's *zip* drives, for instance, a user can backup selected files to a 100-megabyte or larger *zip* disk and restore them to any other computer equipped with Iomega's software and a *zip* drive. Of course, data backup is only one of the many uses of such a device–professionals such as architects and graphic designers are quickly learning the advantages of transporting very large files between computer systems conveniently.

Some innovative Internet services companies are beginning to understand the problems associated with backup hardware and software, and they are offering products to solve those problems. For instance, Sound Data Incorporated offers a service called *Intervault,* which combines client software for each employee's PC, software for the office network's server, transmission of the data via the Internet, and vaulted storage of the data for one fee. The data on each PC is backed-up, gathered by the network server, encrypted, sent to the Sound Data server, and stored by the company for a specified interval.


Netscape - [Sound Data, Incorporated - Info on intervault]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location:
What's New? What's Cool? Destinations Net Search People Software
SOUND Data INCORPORATED
Netscape

Location: http://sounddata.com/intervault.html

intervault™

How to back up and store computer data?

A question faced by companies small or large. With the growth of personal computers and distribution of data to local networks, workgroups and individual workstations, the need to find an answer that provides security, integrity and reliability has become a high priority.

However, software alone can not solve this problem. If it could, then all of those backup products with local tape drives would have solved it long ago. Problem was, and still is, they couldn't address the true failings of backing

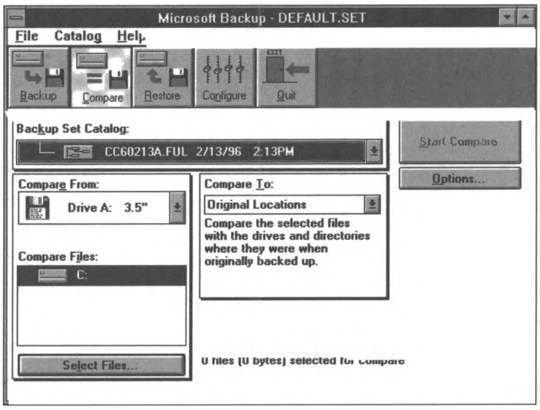
Figure 3.4
The Intervault backup service of Sound Data Incorporated.

Another company, Data Recall, LLC, offers a similar service that is also usuable with a stand-alone PC. By dialing directly to Data Recall on a modem with communication software, the PC can perform an automatic, encrypted backup for itself during off hours. Data Recall offers a multi-media presentation and demonstration of its product at its Web site at **http://www.datarecall.com**.

Whatever combination of backup hardware and software you choose, the most critical aspect of making sure that you will have your important data when you need it is your organization's backup procedure. If each employee is responsible for making a backup of important data each week, this task should be written into job descriptions or the Computer Use Policy. If one employee is responsible for the task, that person should should document the operation of the equipment and train another person to do this job as a contingency measure.

Many organizations use an interval iteration scheme to organize backed up data. This process ensures that there is more than one copy of any particular computer's data and that at least one copy is stored off-site. For instance, a large healthcare facility we know of requires that each employee in its data center backup each PC's entire hard drive to *zip* disks once per week. The most recent backup is stored in the locked media room of the data center. The second-oldest backup is transported to the data center's off-site storage facility. The oldest backup is rotated back from the off-site storage facility for the disks to be distributed and re-used for the current week's iteration. (See the "Off-Site Processing and Storage" section below for a discussion of off-site facilities.)

A final note on backups: A surprise that many businesspersons encounter when trying to restore backed up data is that the backup did not work. Unbelievable as it seems (especially at the time), this is a frequent problem. There can be many problems with backup media: old, worn-out tapes or disks; media that gets damaged in transit; an employee using the backup software improperly. At regular intervals, you should ensure that your organization tests its data backups to verify their integrity. Most backup software has a verification function, wherein the original data will be compared to the backed up data. If your software does not, you can restore a small, selected portion of backup data to another computer and compare the contents of the file to the original. For instance, the *Microsoft Backup* program verifies backed up data with the **Compare** function, as illustrated below:



Backup Set Catalog: CC60213A.FUL 2/13/96 2:13PM

Compare From: Drive A: 3.5"

Compare Files: C:

Compare To: Original Locations

Compare the selected files with the drives and directories where they were when originally backed up.

0 files (0 bytes) selected for compare

Figure 3.4
Using Microsoft Backup to verify the integrity of backed up data.

Disaster Recovery Planning

According to disaster recovery planning consulting firm Koehn Consulting (**http://www.mailbag.com/users/koehn/drp.html**), disaster recovery plans can vary widely among organizations, but thorough ones share some common elements:

- A list of recovery team members, and alternates.
- Locations where backup equipment and additional copies of the plan are stored.
- A description of what constitutes a disaster and how to notify key personnel.

- Names and locations of key vendors and other external companies.
- Recovery procedures.
- Policies to prevent disasters from occurring.
- Procedures for updating the plan.

In very large organizations, the disaster recovery plan is one portion of a larger document called a contingency plan. The contingency plan covers many aspects of how the business will approach any unusual incident or interruption in business activities, and the disaster recovery plan deals specifically with how the business will react to such things as earthquakes, terrorism, fires, and floods.

For smaller organizations, the disaster recovery plan may be the only portion of a contingency plan in place, and it may be a very simple document. But any organization needs to plan for the possibility that the physical location, or offices, can be inaccessible or destroyed. In such a scenario, the information processing portions of the organization's tasks will need to be performed elsewhere–at an off-site location.

Off-Site Processing and Storage

In the past, only the managers of large, mainframe-based data centers have seen the need to plan for where information processing will occur in the case of the destruction of the data center. There are many companies specializing in providing such services, and most large IS departments have a contract with such a site. Terms of the contract usually provide that the off-site facility will install and run the mainframe operating software, along with necessary application systems and databases, in the case of an emergency shut-down of the organization's primary data center.

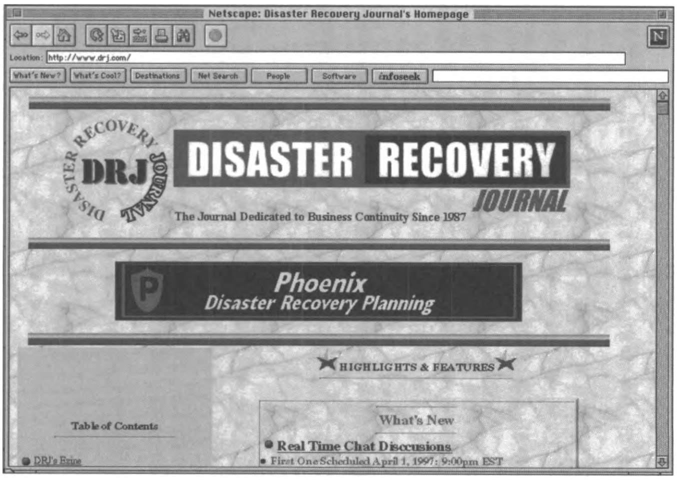
Fortunately, planning for off-site processing is somewhat less complicated for a small or medium-sized organization that uses personal computers for data processing. One accountant we know has the simplest off-site processing plan of all. He has a comparably capable PC system to the ones in his office at home, and he has installed his crucial office application software on that PC. In the event of a physical disaster at his office, he can still run payroll and support other critical functions on his home PC. Other businesses establish procedures for quickly acquiring identical or compatible computer hardware and re-installing software applications quickly.

Although the larger disaster recovery firms generally specialize in mainframe-based services, some do contract with customers to provide ready access to personal computer equipment in the case of an emergency. Other options for off-site processing for smaller enterprises are: (1) making an agreement with another firm to use a stand-by PC; (2) configuring employees' notebook computers to perform business-critical functions in the case of a disaster; (3) establishing a short-term lease or rental agreement with your local computer store for acquiring replacement PCs and establishing an agreement with your building owner or another commercial real estate owner for the short-term lease of an office in the case of an emergency. Of course, all of these procedures should be researched and documented beforehand, and the disaster recovery plan should be kept in a safe storage location away from your organization's main office.

Off-site facilities can also accomodate storage of backed up data, as mentioned above. One Canadian off-site storage firm, Data Base File Tech (**http://www.islandnet.com/~cvcprod/dbft.htm**) informs potential customers that any data stored within 15 kilometers of the customer's place of business is not "safe." Again, when approaching disaster recovery planning, it makes sense to balance the risks with the benefits. How many of your critical business functions would be affected if information processing stopped for 3 days, 5 days, or a week? What are the ramifications to your clients if your electronic files are destroyed? How many security redundancies can you afford? Each of these factors will affect the choices your information security team makes when designing procedures.

Learning More About Physical Security

There are literally hundreds of vendors of computer security and backup products. Visit your favorite Internet search engine site and use queries such as **computer security**, **computer theft**, and **data backup**. The *Disaster Recovery Journal* maintains a Web site with archived articles, vendor information, and links to other security-related organizations:



Netscape: Disaster Recovery Journal's Homepage

Location: http://www.drj.com/

DISASTER RECOVERY JOURNAL

The Journal Dedicated to Business Continuity Since 1987

Phoenix
Disaster Recovery Planning

HIGHLIGHTS & FEATURES

Table of Contents

● DRJ's Ezine

What's New

● Real Time Chat Discussions

• First One Scheduled April 1, 1997: 9:00pm EST

Figure 3-5
Web site of the Disaster Recovery Journal.

For discussion of physical security topics applicable to your organization's computing platform, check a hardware-specific newsgroup such as ***comp.sys.ibm.as400.misc***. The ***comp.security.misc*** newsgroup often carries discussions of backup strategies and disaster recovery planning.

Physical Security Planning Worksheet

Area	**Current Policy or Practice**	**Points For Revised Policy/Practice**
Limit access to computing equipment.	Policy [ ] Practice[ ]	
If necessary, make the computing equipment stationary with the use of lock-down or other containment devices.	Policy [ ] Practice[ ]	
Secure the offices in which the computers reside, and establish who will have access to the offices.	Policy [ ] Practice[ ]	
Select backup technology: hardware and software.	Policy [ ] Practice[ ]	
Document backup procedures and train employees.	Policy [ ] Practice[ ]	

Regularly verify the integrity of backup data.	Policy [ ] Practice[ ]	
Determine which information processing applications are critical to your organization's operation.	Policy [ ] Practice[ ]	
Determine how you will acquire access to computing equipment and space.	Policy [ ] Practice[ ]	
Establish a procedure for restoring backup data to the off-site or contingency systems.	Policy [ ] Practice[ ]	
Document the disaster recovery plan and keep it in a safe, remote location.	Policy [ ] Practice[ ]	

Chapter 4 Viruses

The very mention of the word "virus" causes managers, system administrators, and personal computer users to shudder. Almost everyone has a story to tell about a co-worker or friend who lost that irreplaceable report or crucial database due to a damaging virus. A recent National Computer Security Association survey reports that about 98% of the corporations and large organizations in North America have experienced virus infection of their personal computers. But, the good news is that viruses rarely adversely affect computers immediately, and the damage is often minimal. With some basic information, a few precautions, and good software, your organization can use its PCs with a high degree of confidence that its computers are safe from virus damage. In this chapter, we'll review

- What computer viruses are, and how they can affect personal computers.
- Signs of virus infection on a PC.
- How to protect your organization's PCs from viruses and virus-caused damage.
- Where to find virus protection software, and how to install and use it.
- Where to find more information on computer viruses.

This chapter deals with viruses as they affect stand-alone PCs–those that are used in isolation to perform tasks and access Internet sites using client software. In the case of a local area network, especially one containing an Internet server, virus protection gets more complicated. Network security issues are covered in more detail in Chapter 6.

What Is a Computer Virus?

A computer virus is simply a program designed to reproduce and spread within a computer system or network without revealing its presence. A computer virus attaches to files or to boot sectors of hard or floppy disks (the portions of the disk that contain system configuration information). Once in a computer system, the virus replicates itself; in fact, some viruses do nothing else. Even so, there is no such thing as a truly harmless virus, since, at the very least, viruses expand, taking up hard-drive space and slowing the performance of a computer.

Viruses are typically classified by the way they "infect" a computer's system. For example, viruses that infect executable programs residing on a computer (such as *.exe* files) are referred to as "program viruses." Viruses that infect the boot section or partition tables on a hard disk or floppy disk are called "boot viruses." Viruses that are capable of infecting both are referred to as "multipartite viruses." Viruses that are contained within automated step sequences in a data file are called "macro" viruses, due to the fact that these step sequences are called macros by many software manufacturers. Because a virus is simply computer code, once it enters a computer system, it can spread by being transmitted along with any legitimate software or file that is running or stored on the computer or a floppy disk.

A typical virus program consists of four main parts: the replication instructions, the protection instructions, the trigger, and the payload. The replication instructions are simply the parts of the program that allow the virus to copy itself. The protection instructions are the parts of the program that protect the virus from being detected. (Protection can include encryption or a "stealth" technique that interferes with anti-virus software). The trigger is the part of the program that controls when the virus is triggered into activity. A virus can remain inactive on a computer for a long time before the trigger activates it. For example, a virus might remain inactive until the computer has been turned on a specific number of times or until the computer's clock indicates a certain day or time (such as the infamous Michelangelo virus that is triggered on March 6). The payload is that part of the program that is executed when the trigger is activated. Sometimes payloads are simply messages that indicate that the PC has been infected, but other payloads are more damaging, such as the deletion of files or the altering of data.

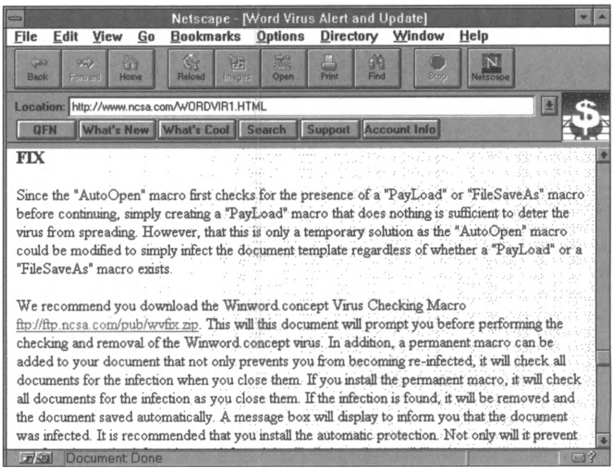
Once a computer is infected by a virus, many types and levels of damage can result. Some levels may be considered negligible, as in the cases of viruses that do nothing more than replicate or viruses that alter or delete files that can be easily reloaded when the viruses are removed. Other viruses might destroy all the files on a computer's hard drive, and, although this sounds like an overwhelming loss, if backups have been made regularly, even this level of damage can be easily corrected by removing the virus and reloading programs and data from the backups. More difficult to recover from are viruses which slowly corrupt data over a long period of time without ever revealing their presence in the system. In cases such as this, backups are corrupted as well, and data must be rebuilt from scratch. Perhaps the most dangerous types of viruses are those designed to do nothing except discover and report crucial system information, such as the password of the system administrator of a LAN. If one of these "discovery" viruses is successful, unlimited damage to the system and its data is possible.

Signs of Computer Viruses

Although these descriptions are chilling to those of us who depend heavily on our computers, there are simple ways to protect ourselves from these viruses and ways to recognize when certain types of viruses are residing on our systems. Some of the symptoms of a computer infected by a virus include

- Changes in the sizes of programs.
- Longer load times for programs.
- Slower system operation.
- Unusual error messages.
- Reduced memory or disk space.
- Unusual screen activity.
- Incorrect changes in file dates and time information.
- Unexpected writes to a drive.

For instance, a journalist we know found that her laptop computer was infected with a version of the Word Concept virus. This is a macro virus with several variations that is carried in the *.doc* files created by Microsoft's very popular *Word for Windows* word processing program. The symptom she noticed was that the **Save As** command under the **File** menu did not work properly–it was disabled at odd times and did not allow her to save documents under new names. Fortunately, a quick trip to the National Computer Security Association, or NCSA, Web site was all she needed to download the correction for the virus (**http://www.ncsa.com**). By following the NCSA instructions for opening the "fix" document that contained ameliorative macros (illustrated below), she was able to remove the virus and repair all affected documents as she opened and re-saved them during the course of the next few weeks.


Netscape - [Word Virus Alert and Update]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop Netscape
Location: http://www.ncsa.com/WORDVIR1.HTML
QFN What's New What's Cool Search Support Account Info
Document: Done

FIX

Since the "AutoOpen" macro first checks for the presence of a "PayLoad" or "FileSaveAs" macro before continuing, simply creating a "PayLoad" macro that does nothing is sufficient to deter the virus from spreading. However, that this is only a temporary solution as the "AutoOpen" macro could be modified to simply infect the document template regardless of whether a "PayLoad" or a "FileSaveAs" macro exists.

We recommend you download the Winword.concept Virus Checking Macro ftp://ftp.ncsa.com/pub/wvfix.zip. This will this document will prompt you before performing the checking and removal of the Winword.concept virus. In addition, a permanent macro can be added to your document that not only prevents you from becoming re-infected, it will check all documents for the infection when you close them. If you install the permanent macro, it will check all documents for the infection as you close them. If the infection is found, it will be removed and the document saved automatically. A message box will display to inform you that the document was infected. It is recommended that you install the automatic protection. Not only will it prevent

Figure 4.1 *The "Fix" page for the Word Concept virus at the NCSA Web site.*

A systems engineer we know was not quite so fortunate. As she worked from her home office, she noticed over the course of a couple of days that several data files on her primary PC seemed to be missing–she received error messages when trying to retrieve them. Within a few more days, she also noticed that some programs did not run properly, creating system errors and protection faults. After running disk analysis software, she discovered many corrupted and damaged files on the hard disk. More investigation with anti-virus software uncovered the fact that her hard disk contained a particularly destructive stealth virus in the boot sector, and that the virus had replicated to affect nearly all programs and data files on the PC. She was able to boot her PC from a floppy diskette with anti-virus protection and locate and delete the virus from the hard drive; however, the damage was irreversible and extensive. She spent several days re-installing her operating system and programs and chasing down duplicate copies of important documents and files. Because she uses her home PC to support clients remotely for her employer, a healthcare software company, the potential for spreading the virus was great. "My team spent a few frantic hours checking all my clients' systems for evidence of the virus," she reports. "Luckily, it had not spread, but if it had, we probably would have had to spend weeks repairing the damage."

Both these examples show how a seemingly unimportant system oddity can really be an indication of much more serious trouble. In the first example, the journalist should have investigated the change in available menu options right away, especially one she had used so regularly in the past, such as the **Save As** command. In the second example, the systems engineer should have immediately suspected trouble when data files began disappearing. Of course, both incidents probably could have been avoided through the regular use of anti-virus software.

Protecting Your PC From Viruses

There are a few relatively simple steps you can take to eliminate the majority of virus threats to your documents and programs. The first, and most important, is to protect against the damage a virus might do by keeping complete and regular backups of your system. (See Chapter 3 for more information on system backups.) In addition, you should follow these guidelines:

1. Back up all your work and system files regularly.
2. Install and use reputable anti-virus software.
3. Update your anti-virus software regularly.
4. Always scan floppy disks and CD-ROMs for viruses.
5. Do not boot your PC from a floppy disk unless you are sure the disk is virus-free.
6. Whenever possible, use the write-protect tab when using floppy disks to prevent viruses from copying themselves.
7. When downloading from the Internet, scan files for viruses before running them.

8. Use only licensed copies of software obtained from reputable sources.

The most effective way to avoid virus damage is to obtain virus detection software and to use it consistently. Most of these programs work by allowing you to perform scans of your random-access memory (RAM), hard disk, and floppy disks for suspicious strings of executable code. Several, such as *Norton Anti-Virus*, also allow you to inoculate files on floppy disks or your hard disk to detect future virus infection (that is, the deposition of viruses known to the program). Some programs even allow you to keep them running in memory so that an infected program file can be caught as soon as it is copied, launched, or identified. And, the newest and most sophisticated virus protection software automatically scans files as they are downloaded from Internet sites to determine their safety.

One of the most important characteristics of virus protection software is its currency. A particular software package can only recognize viruses that have been identified, classified, and defined in the program. Most programs provide a virus definition table so that you can determine which viruses a particular program update can identify, such as the Virus List from *Microsoft Anti-Virus* program illustrated below:

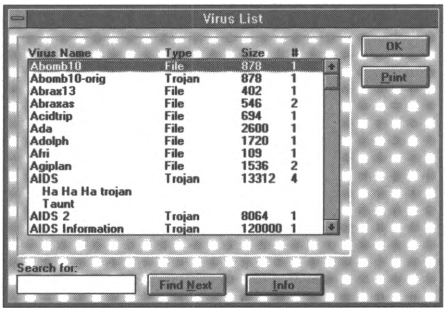


Figure 4.2 *The Virus List screen of the Microsoft Anti-Virus program.*

Virus Name	Type	Size	#
Abomb10	File	878	1
Abomb10-orig	Trojan	878	1
Abrax13	File	402	1
Abraxas	File	546	2
Acidtrip	File	694	1
Ada	File	2600	1
Adolph	File	1720	1
Afri	File	109	1
Agiplan	File	1536	2
AIDS	Trojan	13312	4
Ha Ha Ha trojan			
Taunt			
AIDS 2	Trojan	8064	1
AIDS Information	Trojan	120000	1

For this reason, most of the leading software manufacturers maintain extensive update programs through their Web sites. For instance, users of the popular McAfee anti-virus software, *VirusScan*, can visit the McAfee site at **http://www.mcafee.com** to download the very latest virus definition tables (DAT files) for their software, as shown below.

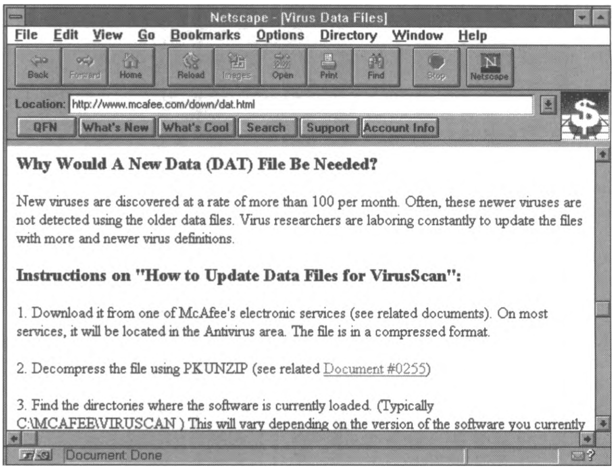


Figure 4.3 *Downloading anti-virus software updates from the Mcafee Web site.*

Location: http://www.mcafee.com/down/dat.html

Why Would A New Data (DAT) File Be Needed?

New viruses are discovered at a rate of more than 100 per month. Often, these newer viruses are not detected using the older data files. Virus researchers are laboring constantly to update the files with more and newer virus definitions.

Instructions on "How to Update Data Files for VirusScan":

1. Download it from one of McAfee's electronic services (see related documents). On most services, it will be located in the Antivirus area. The file is in a compressed format.

2. Decompress the file using PKUNZIP (see related Document #0255)

3. Find the directories where the software is currently loaded. (Typically C:\MCAFEE\VIRUSCAN) This will vary depending on the version of the software you currently

Document Done

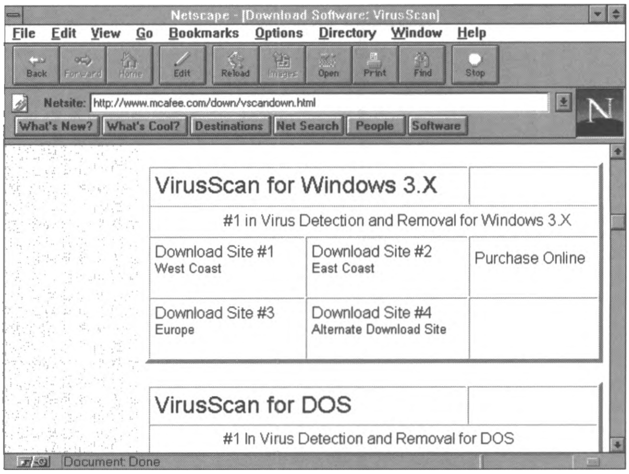
The NCSA survey mentioned above found that over two-thirds of virus infections among large organizations were caused by the use of infected floppy disks. Therefore, it is crucially important for you to scan every floppy disk every time you insert it into a drive on your computer. And, since the Word Concept virus and similar macro-type viruses are both very common and difficult to identify, you should scan floppies before opening any documents from them and scan documents attached to email messages just as consistently as you scan program files.

Downloading, Installing, and Using Anti-Virus Software

Downloading and Installing Anti-Virus Software

Most virus protection software is available for online download. In the case of McAfee products, you can download a 30-day trial version from the McAfee Web site at **http://www.mcafee.com**. To download and install the *VirusScan* program, follow these steps:

⇒ Use your Web browser client software to visit the download page of the McAfee site at **http://www.mcafee.com/leads/evallead.html**, illustrated below:



Netscape - [Download Software: VirusScan]

Netsite: http://www.mcafee.com/down/vscandown.html

VirusScan for Windows 3.X		
#1 in Virus Detection and Removal for Windows 3.X		
Download Site #1 West Coast	Download Site #2 East Coast	Purchase Online
Download Site #3 Europe	Download Site #4 Alternate Download Site	

VirusScan for DOS	
#1 In Virus Detection and Removal for DOS	

Document: Done

Figure 4.4 *Download page for Mcafee's VirusScan program.*

⇒ Fill in the requested information in the form on the page.

⇒ Click on the button labeled **Submit this form**.

⇒ On the next page, click on the link for the software you wish to download. For this example, we chose **VirusScan**.

⇒ On the next page, select the appropriate version for your PC's operating system and choose one of the compressed files to download, as illustrated below:

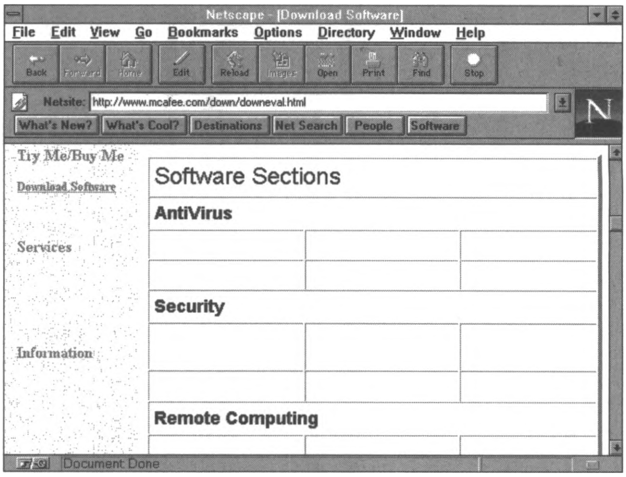

Netscape - [Download Software]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Netsite: http://www.mcafee.com/down/downeval.html
What's New? What's Cool? Destinations Net Search People Software
N
Try Me/Buy Me
Download Software
Services
Information
Software Sections
AntiVirus
Security
Remote Computing
Document Done

Figure 4.5 *Choosing a version of VirusScan.*

⇒ When prompted by your browser software, select the *temp* sub-directory for storing the downloaded file.

⇒ Unzip the downloaded file (called *X.zip*, where X is the name of the version you chose).

⇒ Run the *setup.exe* file by double-clicking on it in **File Manager**, selecting it through the **Run** function under the **File** menu of **Program Manager**, or executing it through *Windows 95* **Start** menu.

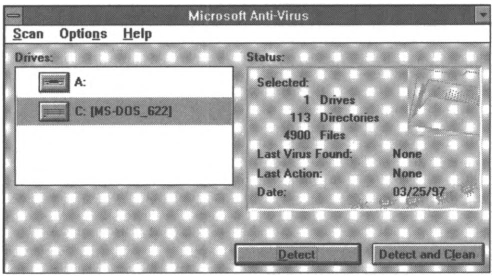
⇒ Follow the on-screen instructions to complete the program installation.

Using Anti-Virus Software

To use anti-virus software, you will need to follow the manufacturer's instructions, which can usually be found on the **Help** screens or in a *readme.txt* file supplied with the software. However, most virus software packages operate with similar features. The example described below uses the *Microsoft Anti-Virus* program.

⇒ Open the program by double-clicking on the *Microsoft Anti-Virus* icon (or choosing the program from the Windows 95 **Start** menu).

⇒ Select a disk drive to scan for viruses by double-clicking on the drive in the left-hand box, as illustrated below:



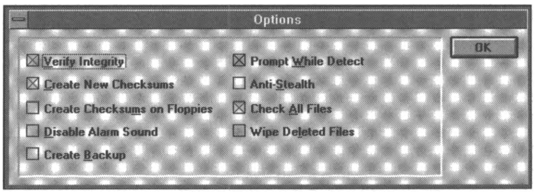
Drives:
A:
C: [MS-DOS_622]

Status:
Selected:
1 Drives
113 Directories
4900 Files
Last Virus Found: None
Last Action: None
Date: 03/25/97

Figure 4.6
Selecting a drive to scan for viruses with Microsoft Anti-Virus.

⇒ Choose either **Detect** or **Detect and Clean** by clicking on the appropriate button. If you choose Detect only, and the program finds a virus, you will be prompted to respond **OK** to a **Clean** function

Many virus protection programs include an "options" or "preferences" menu in which you can customize your program's operation and select those functions of the software you wish to use. The **Options** screen of *Microsoft Anti-Virus* is shown below:



☒ Verify Integrity
☒ Create New Checksums
☐ Create Checksums on Floppies
☐ Disable Alarm Sound
☐ Create Backup
☒ Prompt While Detect
☐ Anti-Stealth
☒ Check All Files
☐ Wipe Deleted Files

Figure 4.7
The Options screen of Microsoft Anti-Virus.

In addition, some products are designed to run as memory-resident programs, enabling them to check all files transmitted via a network or downloaded from the Internet as the transmission occurs (rather than the user performing a separate checking step before opening or executing the file).

Learning More About Viruses

If you are responsible for a network or for advising your clients on how to avoid losses due to computer viruses, you will need to make sure that you stay updated on new developments in this field and on the new viruses infecting computers. One way to do so is to regularly read the messages posted to the ***comp.virus*** Usenet newsgroup, or to subscribe to its companion email discussion list, *Virus-L*. To subscribe to *Virus-L*, send a message addressed to **listserv@lehigh.edu** with the following in the body of the message: **SUB VIRUS-L Your Name**. Before posting any messages to the mailing list or newsgroup, be sure to read the excellent FAQ sheet on this subject maintained by Nick FitzGerald. You can download the FAQ from the ***comp.virus*** archive site at **ftp.infospace.com/pub/virus-l/**. *Note:* Because computer security experts understand the importance of message encryption and authentication, you will find that many documents distributed by them, including this FAQ, are digitally signed, encrypted, or both. This FAQ is digitally signed with Nick FitzGerald's PGP key, and you can use *PGP* software to determine the authenticity of the copy you download if you wish (see Chapter 5 for a full discussion of message authentication and *PGP* software).

In addition to ***comp.virus*** and ***Virus-L***, there is a wealth of information available online about computer viruses. Many companies that sell anti-virus software market their products online. To attract potential buyers to their sites, they also provide useful information about viruses and virus prevention. These sites can be rich resources for virus research, and, not coincidentally, very good sources for purchasing reputable virus-prevention and recovery software. One such site is the *Symantec Antivirus Research Center* at **http://www.symantec.com/avcenter/index.html**. The Symantec site includes a virus research library with many useful descriptive documents, coverage of recent viruses, a virus information database, a downloadable software library, special coverage of Macintosh viruses, and, of course, product information about Symantec software.

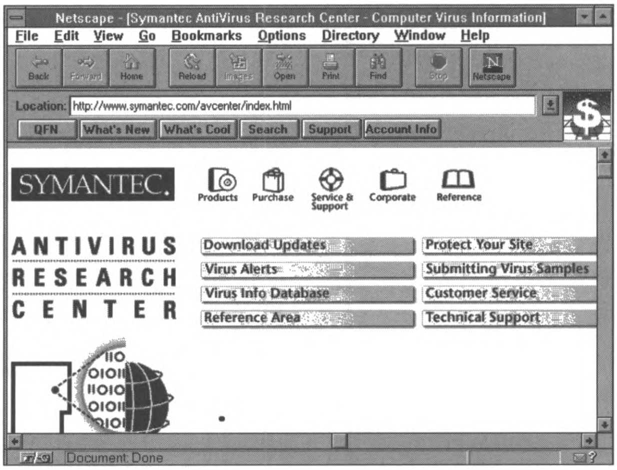

Netscape - [Symantec AntiVirus Research Center - Computer Virus Information]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop Netscape
Location: http://www.symantec.com/avcenter/index.html
QFN What's New What's Cool Search Support Account Info
SYMANTEC.
Products Purchase Service & Support Corporate Reference
ANTIVIRUS RESEARCH CENTER
Download Updates
Virus Alerts
Virus Info Database
Reference Area
Protect Your Site
Submitting Virus Samples
Customer Service
Technical Support
Document: Done

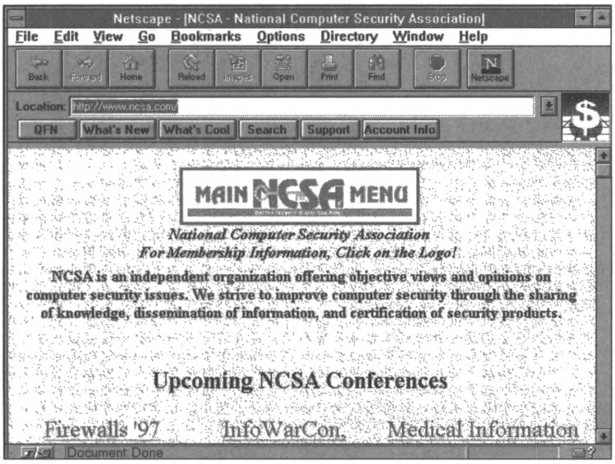
Figure 4.8 *The Symantec Antivirus Research Center Web site.*

Another software site that offers valuable information is *Dr. Solomon's Online* at **http://www.sands.com**. *Dr. Solomon's Online* is an information center for users of Dr. Solomon's anti-virus products. The site includes a virus tutorial, virus alerts, and information about Dr. Solomon's software (such as technical support, white papers, and independent comparative reviews). Similarly, Seven Locks Software at **http://www.sevenlocks.com** provides a good deal of technical information in support of their

Safe@Home anti-virus product. A list of white papers available at this site includes topics such as "Viruses and Windows NT," "Virus Prevention Policies that Work," and "Managing Computer Virus Incidents."

Other virus resources are developed and maintained by groups without particular software products to market, such as the National Computer Security Association at **http://www.ncsa.com**. The NCSA describes its mission this way: "To foster improvement in all aspects of world-wide digital security, reliability and ethics, providing key services to three principal constituencies: end users of digital technologies, computer and communications industry product developers and vendors, and computer and information security experts." To fulfill these objectives, the NCSA provides access to an in-depth virus study (in addition to the survey discussed above), a listing of conferences and seminars, a catalog of books and journals on information security issues, virus information alerts, and links to NCSA-certified software producers.

Figure 4.9
Web site of the National Computer Security Association.



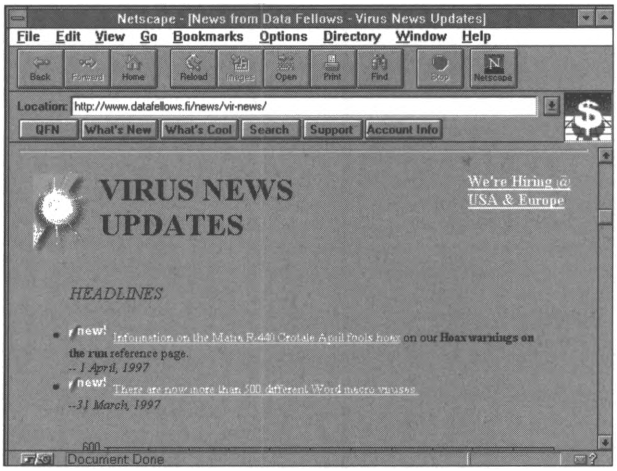
National Computer Security Association
For Membership Information, Click on the Logo!

NCSA is an independent organization offering objective views and opinions on computer security issues. We strive to improve computer security through the sharing of knowledge, dissemination of information, and certification of security products.

Upcoming NCSA Conferences

Firewalls '97 InfoWarCon, Medical Information

To find more specific information on a particular virus, visit Data Fellows *Virus News Updates* page at **http://www.datafellows.fi/news/vir-news/**. At this site you can access a database of information about viruses through an alphabetical listing or through a keyword search form. The database entries provide descriptions of how viruses spread, what they do, and alerts users to any variants of the virus that may also be circulating.



Location: http://www.datafellows.fi/news/vir-news/

VIRUS NEWS UPDATES

We're Hiring @ USA & Europe

HEADLINES

- new! Information on the Matra R.440 Crotale April fools hoax on our **Hoax warnings on the run** reference page.
  -- 1 April, 1997
- new! There are now more than 500 different Word macro viruses.
  --31 March, 1997

Figure 4.10
Virus News Updates page at Data Fellows Web site.

Virus Protection Planning Worksheet

Area	Current Policy or Practice	Points For Revised Policy/Practice
Identify the potential sources of virus infection of the organization's computers.	Policy [ ] Practice[ ]	
Select and install virus protection software.	Policy [ ] Practice[ ]	
Establish guidelines for likely sources of virus infection, such as floppy disks brought from home or programs downloaded from the Internet.	Policy [ ] Practice[ ]	
Familiarize all employees with the use of virus software (if the responsibility of employees) and the signs of computer viruses.	Policy [ ] Practice[ ]	
Ensure that the anti-virus software is updated regularly.	Policy [ ] Practice[ ]	

Chapter 5
Encryption

One way to protect the information assets of your organization is to physically secure them, as we described in Chapter 3. Another way is to make sure that damaging pieces of computer code, called viruses, cannot infect PC systems and damage the programs and data residing on them, as discussed in Chapter 4. However, there may be times when the sensitive and valuable information your company has worked long and hard to compile and store is exposed to the "open air." Perhaps an element of your physical security system will fail, and data files will be taken from computer storage. Perhaps your company will wish to send email and work files over a network using public telephone lines, such as the Internet, or conduct electronic commerce through a company World Wide Web site. Or, perhaps your organization wishes to transmit sensitive material, such as payroll records, over a wide area network (WAN) or local area network (LAN). The best way to keep information private and secure when transmitting it or storing it is to make it unreadable and unrecognizable through a process called encryption. In this chapter, we'll review

- The basics of encryption theory and the current status of encryption programs.
- Ways that encryption is currently used: data archive, email, and WWW browsers.
- Governmental issues related to encryption.
- How to select quality encryption software.
- Where to find more information on encryption.

An Old Strategy Meets the Information Age

Encrypting information through the use of a secret code is an age-old tactic. For thousands of years, political leaders have encoded messages before sending them via messenger, or mail, or radio wave, to friends and allies. The "shift-by-three" code of Julius Caesar is one famous legend: the recipients of the ruler's messages could only read them by replacing each letter in the message text with a letter three positions away from it in the alphabet. For instance, the word *hello* would be encoded to appear as *khoor,* and the recipient could decode it by shifting each letter three positions to its left in the listing of alphabet letters.

Today, the study of encryption and decryption, called *cryptology,* is a field populated by experts in mathematics, information theory, and computer science. Simple schemes such as "shift-by-three" have developed into complex algebraic algorithms, and most of the activities of cryptologists center on computers and sophisticated software. Discovering the secret codes used in encryption, through a process called *cryptanalysis,* is considered the necessary basic training for all aspiring cryptologists and anyone who sets out to create a credible encryption system. Some cryptanalysis techniques used in World War II are believed to be so advanced and valuable that they are still categorized as "classified" by the US government.

A Few Basic Concepts

No matter how sophisticated the mathematical techniques behind an encryption system are, there are a few concepts that are common to all systems. For instance, any process of encryption endeavors to create a *ciphertext* (an encoded, unreadable string of characters) from a *plaintext* (the original characters of the message). This is the process of encrypting, or encoding, information. The reverse process of creating plaintext from ciphertext is called decrypting, or decoding.[1]

Encryption software is based on the mathematical conversion of plaintext to ciphertext (and back) through the use of a mathematical formula called an algorithm. A *key*, which is a unique string of characters, is fed into the algorithm along with the text to be encrypted. Thus, keys become part of the process that is used to encode and decode messages. Keys are widely used in many types of computer programs. For instance, your word processing software might have a function that uses a password key to lock and unlock your documents. File compression utilities, such as *WinZip*, use various compression and decompression keys to make files more compact for storage.

Encryption systems can be classified according to how they handle the creation and distribution of these unique strings of characters called keys. *Symmetric* encryption systems require both the sender and recipient of the data to have the same key, and they are often called *secret key systems*. The private key is used by the sender to encrypt the data and the very same key is used again by the recipient to decrypt the data. In this type of system, two or more correspondents must each have a copy of the program or secret key. While this type of system is a very efficient way to keep messages secure, it also has disadvantages. To use a secret key system, you must know the person with

[1] Portions of the text of this chapter, along with a good deal of useful information, have been gleaned from the Internet document called *Snake Oil Warning Signs: Encryption Software to Avoid* by Matt Curtin and others (copyright 1997, Matt Curtin, all rights reserved, adapted and reprinted with permission). Referred to as *Snake Oil FAQ*, the latest version of this document is archived at ***ftp://rtfm.mit.edu/pub/usenet/news.answers/cryptography-faq/snake-oil***.

whom you wish to exchange messages and provide them with the software and secret key in advance of sending any messages. In addition, the secret key must be sent through a secure channel (not the Internet), because if the secret key is intercepted, the security of all messages among members of the group using the system will be compromised.

An example of a secret key system is *Kerberos,* developed by the Massachusetts Institute of Technology (MIT). In this system, there is a designated Internet site called the Kerberos server that generates keys whenever a group of users wishes to send messages. Another secret key system is called *DES* (see the "Governmental Issues" section below for more discussion of *DES*). Parties that wish to share encoded messages use a common numerical string (*DES* key) along with the *DES* program to encode and decode messages.

Asymmetric encryption systems, in contrast, assign one pair of keys each to the sender and the receiver. Also called *public key systems,* asymmetric encryption tools provide for the sender and receiver to have both a *public key* and a *private key.* Public key systems were designed so that users would not need to access other sites to generate keys and so users could distribute keys through unsecured channels, such as the Internet. Users distribute their public keys to anyone to wishes to send a secure message. Public keys are posted at key distribution sites so that anyone with access to the Internet can acquire anyone else's public key.

For example, if a client wanted to send private financial data to her accountant over the Internet using a public key system, she would locate and verify the accountant's public key, use the accountant's public key to encrypt her file with encryption software, and send the encrypted file via email to the accountant. (Anyone who knows that the accountant has a public key could visit the Internet site serving as the repository of public keys for the accountant's chosen encryption system and do the same thing.) The accountant would then use his private key, which only he knows, to decrypt the message after receiving it. *PGP,* or *Pretty Good Privacy,* is an example of a public key encryption system. To better understand the differences between private key and public key systems, compare Figures 5-1 and 5-2.

Figure 5.1 *Message traffic flow in a secret key system.*

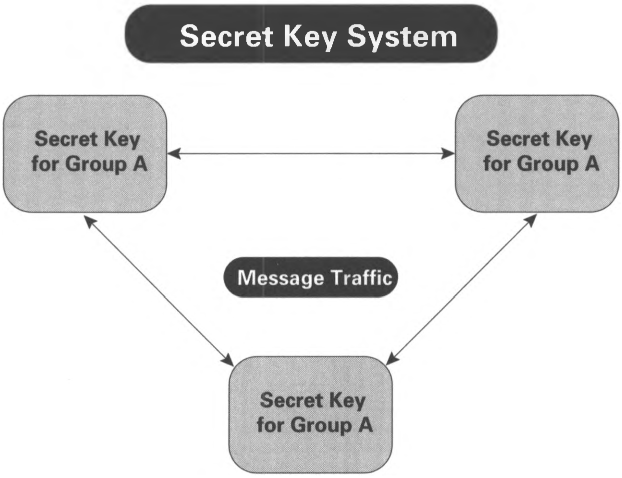
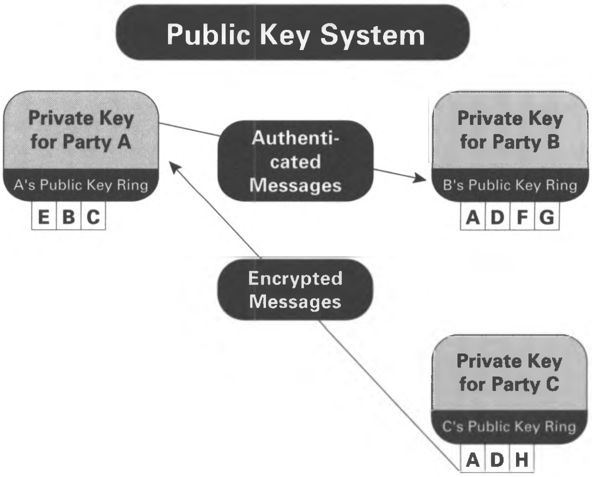


Figure 5.2 *Message traffic flow in a public key system.*



In both symmetric and asymmetric encryption systems, the length of the key is a crucial factor. In a world where sophisticated computer programs can be used to analyze and "break" encryption schemes, the longer the key, the more robust the encryption system. Because cryptanalysis techniques use various probability schemes to discover keys, the time required to break a system increases exponentially with each incremental increase in key length. This is why both the sales hype and the technical discussions of encryption center on key length. And, this is why the US government is concerned with encryption systems and their export (see the "Governmental Issues" section below).

In addition to encrypting and decrypting data, encryption software vendors often also build in features that protect files from being altered in transit or from being transmitted by impostors. The process of verifying that a message was sent by the person who has signed it and that it has not been altered during transmission is called *authentication*. In practice, authentication usually uses a form of *digital signature* to assure that a document has been sent legitimately by its stated sender and that the contents remain unaltered. In public key systems, a message recipient can also use someone's public key to verify their digital signature and thus assure that the message is authentic.

Uses of Encryption

Individuals and organizations generally use encryption for three purposes: (1) to protect archived data; (2) to protect email transmissions; and (3) to protect World Wide Web transmissions, such as electronic commerce transactions.

Archival Encryption

As mentioned above, one of the factors determining whether or not an encryption system is "breakable" through cryptanalysis techniques is time–figured as how much computing power is needed to perform the cryptanalysis. The longer it takes to discover a system's key, the more secure it is considered to be. However, the factor of time impacts different data types differently. For instance, the time an email message must remain secure and confidential might be only one day, while banking account information and personnel records need to be kept confidential for much longer. Therefore, many experts recommend that organizations use much stronger encryption systems for archived data than for message transmission. So, when planning for the security of an organization's archived information, you should consider both its physical security (see Chapter 3) and the merits of the encryption system used.

Email Encryption

The most popular system used for the encryption of email messages is *PGP, or Pretty Good Privacy,* developed by Philip Zimmerman and others. *PGP* uses a formula to create a numerical string (key) from two prime numbers using the RSA, Inc. public-key system invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The key is used to encode messages, and to encode them, one must know the two original prime numbers. *PGP* public keys can also be used to authenticate signatures and ensure message integrity, as discussed above. For instance, a bank may wish to send its customers a message changing a deposit procedure. The bank can use *PGP* to create an elaborate digital signature that contains not only the bank's signature but also an encrypted digest of the message. The customer can process the bank's message and signature with *PGP* and the bank's public key and verify that the message was from the bank and that it was not altered on its way.

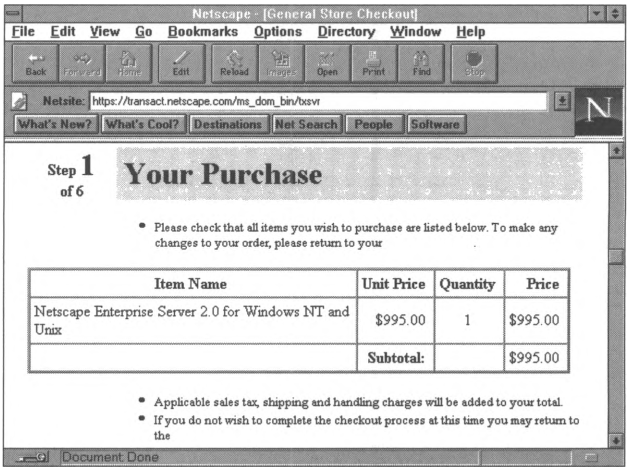
PGP is available for non-commercial use by using Telnet to visit the **net-dist.mit.edu** site. Log-in as **getpgp**, answer the questions, and then use FTP to visit the **net-dist.mit.edu** site and follow the directions to download and install the software. *PGP* for commercial use is available from PGP Inc. (**http://www.pgp.com**). The commercial version, called *WinPGP*, is much more integrated with *Windows* software programs and provides an efficient cut-and-paste method of encrypting and decrypting messages.

In addition to third-party encryption systems, such as *PGP*, various email programs are beginning to include encryption as components of email composition and transmission software. One protocol gaining acceptance as a broad standard for Internet email security is S-MIME, based on the RSA encryption system. When using an email package, such *as Netscape Mail* or *Eudora Pro*, that supports S-MIME, encryption and decryption takes place transparently to the user. As the export issues surrounding encryption systems are resolved and users pressure software makers for easier ways to protect Internet messages, this type of embedded encryption will become more and more popular.

World Wide Web Encryption

In the continuing debate about Internet standards, the encryption of HTTP transmissions is a hot topic. At stake is the security of all electronic commerce conducted via Web sites. Some companies, like Netscape, are advocating for standardization on open, non-proprietary security schemes, such as their proposed Secure Sockets Layer, or SSL. Other firms, especially makers of specialized electronic commerce systems, would like to see each site using the software of their choice, which may or may not be based on a proprietary encryption system.

As of this printing, SSL seems to be fast gaining acceptance as a standard for secure Web transmissions. As Netscape has envisioned it, SSL is a layer of protocol located logically between Internet client software (such as software used to access the Telnet, FTP, or Usenet functions of the Internet) and the TCP/IP software (also called the TCP/IP stack or the winsock). In addition to data encryption based on the RSA system, SSL provides for server authentication, client authentication, and message integrity. When accessing a server that supports SSL, you will see that the protocol indicator at the beginning of the URL begins with HTTPS (as opposed to HTTP). In addition, if you are using an SSL-enabled WWW browser you will see an indication on your browser screen that you are connected with a secure server–for instance, when using *Netscape Navigator,* the small key icon at the lower left-hand corner of the browser screen changes from a broken key to an intact key, as illustrated below on the order screen for Netscape's *Enterprise Server* software:



Netscape - [General Store Checkout]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Netsite:
What's New? What's Cool? Destinations Net Search People Software
N
Document Done

https://transact.netscape.com/ms_dom_bin/txsvr

Step 1 of 6

Your Purchase

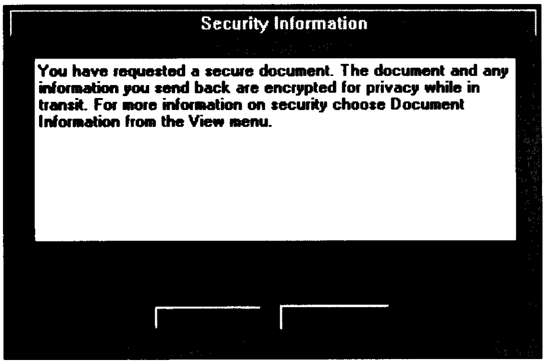
- Please check that all items you wish to purchase are listed below. To make any changes to your order, please return to your

Item Name	Unit Price	Quantity	Price
Netscape Enterprise Server 2.0 for Windows NT and Unix	$995.00	1	$995.00
	Subtotal:		$995.00

- Applicable sales tax, shipping and handling charges will be added to your total.
- If you do not wish to complete the checkout process at this time you may return to the

Figure 5.3
Secure WWW connection to a Netscape server.

When you are sending information, such as credit card data or account information, to an SSL-enabled server with an SSL-enabled client, the data is encrypted automatically with the server's public key on the client side and is decrypted with a private key on the server side. The same is true in reverse; however, the private and public keys are generated randomly by the client software and the user is not required to perform any special decrypting steps. *Netscape Navigator* informs the user when a secure form has been requested through the browser software with the following screen:



You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit. For more information on security choose Document Information from the View menu.

Figure 5.4 *Security Information screen of Netscape Navigator.*

Governmental Issues

You've probably seen references in the popular press to the debate about the US government's role in restricting the export of encryption technology. This issue will continue to affect encryption software development and distribution. In order for you to make informed choices about selecting and implementing encryption software in your organization, you should be aware of the history and progression of this public policy.

In 1968, Congress passed the Omnibus Crime Act, an act that allowed law enforcement agencies to conduct electronic surveillance. In brief, the Congress decided that "the public safety interests [are] important enough within the confines of the Fourth Amendment to warrant extremely strict regimes of control to be implemented, adhered to, and vigorously enforced" (**http://www.fbi.gov/crypto.htm**). In the early seventies, debates began to rage in Congress about whether or not the same logic applies to the Internet. Should the government or law enforcement officials have complete access to the electronic information being relayed on the Internet?

These debates continue today. According to the Director of the FBI, Louis Freeh, in his speech given before the Congress on September 21, 1995, this debate is essentially about the same issues that the Congress was facing in 1968, only now the Congress is questioning who is permitted to encrypt what information and how well that information can be encrypted. The American government has maintained a policy of only allowing 40-bit encryption on messages transferred outside of the US. Furthermore, US companies are forbidden to sell encryption systems of over 40-bits to other countries. This policy has, of course, hurt companies attempting to conduct international electronic commerce because they cannot transfer secure messages over the Internet, and it has hurt American encryption companies who wish to market and sell their products in the growing overseas arenas.

Both the US and other governments are worried that encryption techniques that allow information to be encoded too well will allow all manner of "bad guys" (such as terrorists, organized criminals, nuclear smugglers, drug traffickers, or spies) to send messages and make plans over the phone lines–right under the government's nose–hence the ban on the export of any encryption system over 40-bits. D. James Bidzos, President of RSA Data Security, Inc., a leading manufacturer of encryption software, says of his company's role in producing encryption tools, "I am occasionally asked how I feel about heading a company that is developing and marketing technology that may allow criminals to conceal their activities from the government... I'm sure that my response is similar to the response you would get if you asked the automotive industry how they feel about making a product that will, with absolute certainty, cause the deaths of more than 40,000 people annually....the risk is acceptable because it is outweighed by the benefits, and the alternatives are unacceptable" (**http://www.rsa.com/PRESSBOX/releases/commit~1.htm**).

Peter Trei, a senior software engineer at Process Software Corporation of Framingham, Massachusetts, says of the current encryption ban, "The whole law's kind of ridiculous." Trei claims that 40-bit encryption technology is neither strong enough to safeguard commercial transactions nor to protect against industrial espionage (**http://techweb.cmpcom/cwi/current/50n1.html**). Witness to this statement is Damien Doligez, a French researcher who cracked the encryption code of the non-US version of *Netscape Navigator* in just eight days. "Once the bugs are worked out," Doligez said, "a group of computers will be able to crack Netscape's 40-bit code in as little as half a day." And, just as he predicted, two separate groups recently accomplished the task in under four hours.

The debate over encryption and the loss of international trade due to the lack of appropriate encryption software has been a hot issue during the Clinton administration. In 1994, a product developed by the National Security Agency, the "Clipper Chip," was touted by the Clinton administration as the answer to international encryption problems. The Clipper system is based on the idea of key-escrow. Basically, for any company subscribing to the Clipper Chip, two government agencies would hold the keys to encryption in "escrow." Then, anytime a law enforcement official desires to view the company's electronic records, the two government agencies would supply the keys to unlock the code–all subject to court order, of course.

US companies that develop and produce encryption hardware and software are justifiably anxious about the potential market that they are losing overseas. D. James Bidzos testified to the Congress in June of 1996 that European and Middle Eastern companies are currently manufacturing and selling high-powered encryption systems to companies all over the world using encryption technology originally developed right here in the United States. Bidzos claims that the US ban on encryption export "did not recognize the threat to US industry from foreign competition. . . . Lost market share is hard to recover" (**http://www.rsa.com/PRESSBOX/releases/commit~1.htm**). Bidzos also insinuated that the US firms that develop and distribute encryption software are not only losing the competitive edge in the international market, but also within the US market, for the United States does not have any type of import ban on encryption systems.

All of this controversy has caused businesses wanting to implement electronic commerce sites to be, legitimately, skeptical and somewhat fearful about implementation. However, a solution to the government encryption ban is in sight. The Clinton administration announced in August of 1996 that it would "soon release an alternative to the US government's Clipper Chip system that would allow companies to export software with 64-bit encryption capabilities" (**http://techweb.cmp.com/cwi/current/50n1.html**). A 64-bit system, being longer, would require more time and computing power to decode and would be secure enough to protect most electronic transfers, according to Mike Homer, Vice President of Marketing at Netscape.

On October 1, 1996, Vice President Al Gore announced the Clinton administration's answer to the encryption ban policy and the new initiative of the government to promote international electronic commerce and encryption sales. The new initiative did not allow for the export of the expected 64-bit encryption systems, but, instead, systems with 56-bit encryption capabilities will be released for export beginning on January 1, 1997 (**http://doradus.einet.net/tradewave/press/pr.govtstandards.1096.html**). Gore stated that "under this initiative, the export of 56-bit key length encryption products will be permitted under a general license after one-time review, and contingent upon industry commitments to build and market future products that support key recovery" (**http://www.rsa.com/PRESSBOX/releases/56bitGore.htm**). This type of encryption system also operates under the "key escrow" idea, except that the keys are not held by the US government, but by some trusted third party, maybe even someone internal to the user's organization. Access to these keys would, of course, be limited to the laws of the country in which the business is operating, but Gore says that here in the US, the administration will introduce legislation that will "facilitate commercial key recovery, including providing penalties for improper release of keys, and protecting key recovery agents against liability when they properly release a key" (**http://www.rsa.com/PRESSBOX/releases/56bitGore.htm**).

Choosing Encryption Software

Software makers will come and go, but the basics of choosing good encryption software are relatively simple. Use the two sections below to establish what your objectives are in encrypting data and to measure the marketing claims of software companies.

Organizational Encryption Objectives

For many users of computer-based encryption, preserving the contents of a message is as important as protecting its secrecy. Damage caused by tampering can often be worse than damage caused by disclosure. For example, it may be disquieting to discover that a cracker has read the contents of your funds-transfer authorization, but it's a disaster for him to change the transfer destination to his own account.

Encryption by itself does not protect a message from tampering. In fact, there are several techniques for changing the contents of an encrypted message without ever figuring out the encryption key. If the integrity of your messages is important, don't rely on just secrecy to protect them. Check how the vendor protects messages from undetected modification.

Key Sizes

Even if a cipher is secure against analytical attacks (which form the basis of most cryptanalysis techniques), it will be vulnerable to brute-force attacks with moderate computing power if the key is too small. In a brute-force attack, the attacker simply tries every possible key until the right one is found. How long this takes depends on the size of the key and the amount of processing power available. So when trying to secure data, you need to consider how long it must remain secure and how much computing power an attacker can use. Any reliable encryption software vendor should be able to provide you with estimates of how long it would take to break the system it uses and the conditions under which that could occur.

Keys vs. Passphrases

A *key* is not the same thing as a *passphrase* or *password.* In order to resist cryptanalysis techniques, all possible keys must be equally probable. If some keys are more likely to be used than others, then an unauthorized person can use this information to reduce the work needed to break the cipher. Essentially, the key must be random. However, a passphrase generally needs to be easy to remember, so it has significantly less randomness than its length suggests. For example, a 20-letter English phrase, rather than having 20 x 8 = 150 bits of randomness, only has about 20 x 2 = 40 bits of randomness. So, most encryption software will convert a passphrase into a key through a process called *hashing* or *key initialization.* Avoid encryption systems that skip this phase by using a password directly as a key.

Implementation Environment

Other factors that can influence the relative security of a product are related to its environment. For example, in software-based encryption packages, is there any plaintext that's written to disk (perhaps in temporary files)? What about operating systems that have the ability to swap processes out of memory on to disk? When something to be encrypted has its plaintext counterpart deleted, is the extent of its deletion a standard removal of its name from the directory contents, or has it been written over? If it's been written over, how well has it been written over? Is that level of security an issue for you? Are you storing encryption system keys on a multi-user machine? If so, the likelihood of having your keys illicitly accessed is much higher.

Software Warning Signs

Below is a list of claims and practices that should make you think twice about a particular software vendor. Some very reputable systems might use one of these marketing angles to promote their product, but, in general, any vendor that makes impossible claims or unreasonable assurances is probably over-stating their system's security. When buying encryption software, that old adage is unfortunately true: "If it sounds too good to be true, it probably is."

Trust Us, We Know What We're Doing

Perhaps the biggest warning sign of all is the "trust us, we know what we're doing" message that's either stated directly or implied by the vendor. This message is usually communicated in lieu of a complete explanation of the security features of the product, with the implication that describing the product in exhaustive detail would somehow compromise the secret "inner workings" of the system. If the vendor is concerned about the security of their system after describing exactly how it works, it is certainly of questionable effectiveness. Regardless of whether or not they tell, cryptanalysts will be able to figure it out.

Technobabble

If the vendor's description appears to be confusing nonsense, it may very well be so, even to an expert in the field. One sign of technobabble is a description which uses newly-invented terms or trademarked terms without actually explaining how the system works. Technobabble is a good way to confuse a potential user and to mask the vendor's own lack of expertise. And consider this: if the marketing material isn't clear, will the user manual be any better? Even the best product can be compromised if it isn't used properly. If you can't understand what a vendor is saying, you're probably better off finding something that makes more sense.

Secret Algorithms

Avoid software which uses secret algorithms. This is not considered a safe means of protecting data. If the vendor isn't confident that its encryption method can withstand scrutiny, then you should be wary of trusting it. A common excuse for not disclosing an algorithm is that "crackers might try to break the program's security." While this may be a valid concern, it should be noted that sophisticated cryptanalysts can reverse-engineer the program to see how it works anyway. This is not a problem if the algorithm is strong and the program is implemented properly. Using a well-known and trusted algorithm, providing technical notes explaining the implementation, and making the source code available are signs that a vendor is confident about its product's security.

Revolutionary Breakthroughs

Beware of any vendor who claims to have invented a "new type of cryptography" or a "revolutionary breakthrough." True breakthroughs are likely to show up in research literature, and professionals in the field typically won't trust them until after years of analysis, when they're not so new anymore. The strength of any encryption scheme is only proven by the test of time.

Unbreakability

Some vendors will claim that their software is "unbreakable;" however, no algorithm is unbreakable. Even the best algorithms are susceptible to brute-force attacks, though this can be impractical if the key is large enough. Some companies that claim unbreakability actually have serious reasons for saying so. Unfortunately, these reasons generally depend on some narrow definition of what it means to "break" security. For example, one-time pads (see the next section) are technically unbreakable as far as secrecy goes, but only if several difficult and important conditions are true. Even then, they are trivially vulnerable to known plaintext attacks on the message's integrity. Other systems may be unbreakable only if one of the communicating devices (such as a laptop computer) isn't stolen. So be sure to find out exactly what the "unbreakable" properties of the system are, and see if the more breakable parts of the system also provide adequate security.

One-Time-Pads

A vendor might claim the system uses a one-time-pad (OTP), which is provably unbreakable. Technically, the encrypted output of an OTP system is equally likely to decrypt to any same-size plaintext. For example, the ciphertext below:

598v *$ _+~xCtMB0

has an equal chance of decrypting to any of these:

The answer is yes
The answer is no!
You are so naive!

An OTP system works by having a "pad" of random bits in the possession of both the sender and recipient, but absolutely no one else. Originally, paper pads were used–thus, the term *pad.* The pad must be sent from one party to the other securely. To encrypt an n-bit message, the next n bits in the pad are used as a key. After the bits are used from the pad, they're destroyed, and can never be used again.

The bits in the pad cannot be generated by an algorithm or other encryption tool. They must be truly random, using a real random source such as specialized hardware. The real limitation to practical use of OTPs is the generation and distribution of truly random keys. You have to distribute at least one bit of key for every bit of data transmitted. So OTPs are awkward for general-purpose cryptography. Further, if pads are provided by a vendor, you cannot verify the quality of the pads. Also, some vendors may try to confuse random session keys or initialization vectors with OTPs.

Recoverable Keys

If there is a key-backup or key-escrow system, are you in control of the backup and organizational implementation of key escrow or does someone else hold a copy of the key? If the vendor claims it can recover lost keys without using some type of key-escrow service, the security is obviously flawed.

Exportable from the USA

If the software is made in the USA, can it be exported? As discussed above, strong cryptography is considered dangerous munitions by the United States and requires approval from the US State Department before it can leave the country. Chances are, if the software has been approved for export, the algorithm is weak or crackable, as the recent demonstrations of the exportable version of *Netscape Navigator* demonstrate.

Military Grade

Many encryption system vendors claim that their system is "military grade." This is a meaningless term, since there isn't a standard that defines "military grade," other than the fact that a system is actually being used by various armed forces. Unfortunately, many reputable makers of reliable encryption software use this marketing claim.

Other Considerations:

- Avoid vendors who don't seem to understand any concepts described in this chapter.
- Avoid any system that doesn't let you generate your own keys (e.g., the vendor sends you keys in the mail, or keys are embedded in the copy of the software you buy).
- Avoid anything that allows someone inappropriately accessing the software on a particular PC to retrieve

encrypted data without needing some sort of key or passphrase.

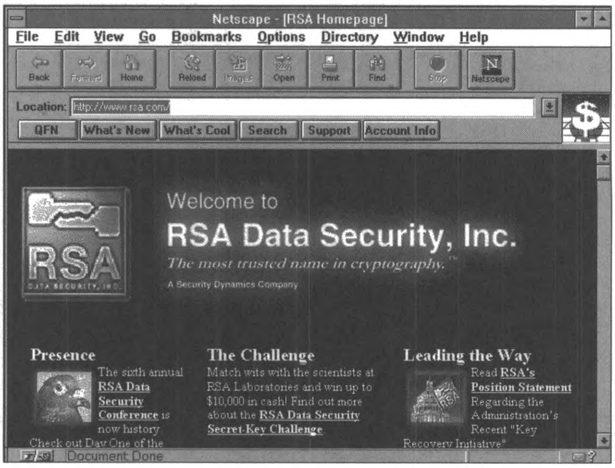
- Beware of products that are designed for a specific task, such as data archiving, and have encryption as an additional feature. Typically, it's better to use an encryption utility for encryption, rather than some tool designed for another purpose that adds encryption as an afterthought.
- No product is secure if used improperly. Make sure that your organization includes the appropriate use of encryption systems in procedures and policies.
- Interface isn't everything: user-friendliness is important, but be wary of a system that puts too much emphasis on ease of use without due consideration to cryptographic strength.

Learning More About Encryption

Since the experts in cryptology are computer scientists and theoretical mathematicians, you can find lots of discussion among cryptologists on the Internet. The Usenet newsgroup ***sci.crypt*** is the place to find serious, theoretical discussion of new encryption systems and their testing. For discussion of general social and regulatory issues regarding encryption tools, try ***talk.politics.crypto***. In ***misc.legal.computing***, you can find lively debate about issues like the patenting of encryption technologies, privacy rights, and government involvement.

The very long, 10-part *Cryptography FAQ* provides a comprehensive overview of the terms and concepts cryptologists use to discuss their work. You can find it in the ***sci.crypt*** newsgroup (posted every 21 days), and the most recent version is archived at ***ftp://rtfm.mit.edu/pub/usenet/news.answers/cryptogrpahy-faq/***. Section 3 of this document, titled "Basic Cryptology," is an especially useful basic introduction to various kinds of systems and their efficacy.

The RSA Data Security Web site is another good source of general encryption information and discussions of organizational issues involving information security (**http://www.rsa.com**). At this site, you can find a very informative FAQ on export issues called *Answers to Frequently Asked Questions About Cryptography Export Laws* in *Adobe Acrobat* PDF format. In addition, RSA publishes a customer newsletter called *Ciphertext*, each issue of which is also posted as a PDF file at the Web site.



Welcome to

RSA Data Security, Inc.

The most trusted name in cryptography.™

A Security Dynamics Company

Presence

The sixth annual **RSA Data Security Conference** is now history Check out Day One of the

The Challenge

Match wits with the scientists at RSA Laboratories and win up to $10,000 in cash! Find out more about the **RSA Data Security Secret-Key Challenge**.

Leading the Way

Read **RSA's Position Statement** Regarding the Administration's Recent "Key Recovery Initiative"

Figure 5.5 *Web site of encryption vender RSA Data Security, Inc.*

If you want to learn more about Secure Sockets Layer (SSL) and Netscape's plans for its integration into browser software and other Internet functions, take a look at the following two online documents: *On Internet Security* (**http://home.mcom.com/info/security-doc.html**) and *Netscape Data Security: An Overview of Implementations and Plans from Netscape Communications* (**http://home.mcom.com/newsref/ref/netscape-security.html**).

You can also subscribe to Netscape's discussion mailing list about SSL by sending mail to **ssl-talk-request@netscape.com** and including the word **subscribe** in the body of your message.

Encryption Planning Worksheet

Area	Current Policy or Practice	Points For Revised Policy/Practice
Establish the organization's uses for encryption technology--archived data, email transmissions, World Wide Web transactions.	Policy [ ] Practice[ ]	
Establish organizational encryption objectives.	Policy [ ] Practice[ ]	
For archived data, establish the length of time the data must remain secure.	Policy [ ] Practice[ ]	
For email transmissions, select between the PGP or S-MIME protocols.	Policy [ ] Practice[ ]	

For World Wide Web transactions, select between the SSL standard of a proprietary protocol.	Policy [ ] Practice[ ]	
Select encryption software and establish procedures for its use and employee training.	Policy [ ] Practice[ ]	

Chapter 6
Network Security*

As we discussed in Chapter 2, the security issues of stand-alone PCs are relatively simple. If the person using the PC is aware of computer use and corporate image issues, and the PC does not provide any server functions over the Internet, the risks are low. The data residing on the PC can be kept confidential and safe through the appropriate use of encryption, anti-virus, and physical security measures, as discussed in Chapters 3, 4, and 5. However, when computers are networked, and especially when that network is connected to a larger communication channel such as the Internet, the risks are much more numerous and the measures needed to protect the system are more complex. In this chapter, we'll review

- Network basics.
- TCP/IP: the Internet protocol.
- Network risk management.
- Types and sources of network threats.
- Firewalls.
- Secure network devices.

Introduction to Networking

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section,

* This chapter was authored by Matt Curtin, Chief Scientist with Megasoft, Inc. (**cmcurtin@research.megasoft.com**; **http://www.research.megasoft.com/people/cmcurtin/**).

we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. Following that, we'll take a more in-depth look at TCP/IP, the network protocol suite that is used to run the Internet and many intranets.

What Is a Network?

A "network" has been defined as "any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances" (The New Lexicon Webster's Encyclopedic Dictionary of the English Language). This definition suits our purpose well: a computer network is simply a system of interconnected computers. How they're connected is variable–as we'll soon see, there are a number of ways to do this.

The ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them (see Figure 6.1). Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card and the wires that connect the cards together.

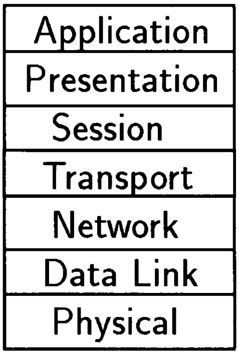


Figure 6.1
The ISO/OSI Reference Model.

An easy way to look at this is to compare this model with something we use daily: the telephone. In order for you to talk to someone out of earshot, you need a device like a telephone. (In the ISO/OSI model, this is at the application layer.) The telephones, of course, are not useful unless they have the ability to translate the sound into electronic pulses that can be transferred over wire and back again. (These functions are provided in layers below the application layer.) Finally, there is the physical connection: both must be plugged into an outlet that is connected to a switch that's part of the telephone system's network of switches.

If I place a call to you, I pick up the receiver and dial your number. This number specifies which central office to which to send my request, and then which phone from that central office to ring. Once you answer the phone, we begin talking, and our session has begun. Conceptually, computer networks function exactly the same way. Thus, each layer of the ISO/OSI Reference Model cannot work without the services provided by the layer below it.

What Are Some Popular Networks?

Over the last 25 years or so, a number of networks and network protocols have been defined and used. We're going to look at two of these networks, both of which are "public" networks. Anyone can connect to either of these networks, or use types of networks to connect their own hosts (computers) together without connecting to the public networks. Each type takes a very different approach to providing network services.

UUCP

UUCP (*Unix*-to-*Unix* CoPy) was originally developed to connect *Unix* hosts together. UUCP has since been ported to many different architectures, including PCs, Macs, Amigas, Apple IIs, VMS hosts, and many other types of devices. Additionally, a number of systems have been developed around the same principles as UUCP.

Batch-Oriented Processing

UUCP and similar systems are batch-oriented systems–everything that they have to do is added to a queue, and then at some specified time, everything in the queue is processed.

Implementation Environment

UUCP networks are commonly built using dial-up (modem) connections. However, this doesn't have to be the case. UUCP can be used over any sort of connection between two computers, including an Internet connection. Building a UUCP network is a simple matter of configuring two hosts to recognize each other and know how to get in touch with each other. Adding on to the network is simple; if hosts called A and B have a UUCP network between them, and C would like to join the network, then it must be configured to talk to A or B. Naturally, anything that C talks to must be made aware of C's existence before any connections will work. Now, to connect D to the network, a connection must be established with at least one of the hosts on the network, and so on. Figure 6.2 shows a sample UUCP network.

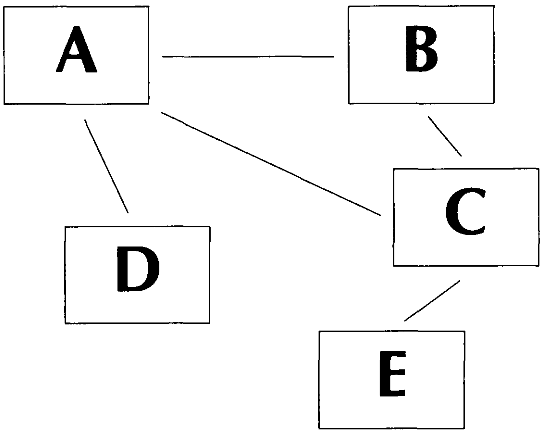


Figure 6.2
A sample UUCP network.

In a UUCP network, users are identified in the format **host!userid**. The "!" character (pronounced "bang" in networking circles) is used to separate hosts and users. A *bangpath* is a string of host(s) and a userid like **A!cmcurtin** or **C!B!A!cmcurtin**. If I am a user on host A and you are a user on host E, I might be known as **A!cmcurtin** and you as **E!you**. Because there is no direct link between your host (E) and mine (A), in order for us to communicate, we need to do so through a host that has connectivity to both E and A. In our sample network, C has the connectivity we need. So, to send me a file, or piece of email, you would address it to **C!A!cmcurtin**. Or, to take the long way around, you can address me as **C!B!A!cmcurtin**. The "public" UUCP network is simply a huge worldwide network of hosts connected to each other.

Popularity

The public UUCP network has been shrinking in size over the years, with the rise of the availability of inexpensive Internet connections. Additionally, since UUCP connections are typically made hourly, daily, or weekly, there is a fair bit of delay in getting data from one user on a UUCP network to a user on the other end of the network. UUCP isn't very flexible, as it's used for simply copying files (which can be news, email, documents, etc.). Interactive protocols (that make applications such as the World Wide Web possible) have become much more the norm, and are preferred in most cases.

However, there are still many people whose needs for email and Usenet news are served quite well by UUCP, and its integration into the Internet has greatly reduced the amount of cumbersome addressing that had to be accomplished in times past.

Security

UUCP, like any other application, has security trade-offs. Some strong elements in its security are: (1) it is fairly limited in what it can do, and it's therefore more difficult to trick into doing something it shouldn't; and (2) it's been around a long time, and most of its bugs have been discovered, analyzed, and fixed. Because UUCP networks are made up of occasional connections to other hosts, it isn't possible for someone on host E to directly make contact with host B and take advantage of that connection to do something unauthorized.

On the other hand, UUCP typically works by having a system-wide UUCP user account and password. Any system that has a UUCP connection with another must know the appropriate password for the **uucp** or **nuucp** account. Identifying a host beyond that point has traditionally been little more than a matter of trusting that the host is who it claims to be, and that a connection is allowed at that time. More recently, there has been an additional layer of authentication, whereby both hosts must have the same sequence number that is incremented each time a connection is made.

Hence, if I run host B, I know the **uucp** password on host A. If, though, I want to impersonate host C, I'll need to connect, identify myself as C, hope that I've done so at a time that A will allow it, and try to guess the correct sequence number for the session. While this might not be an easy attack for someone to make, the process isn't considered very secure.

The Internet

The Internet is the world's largest network of networks. When you want to access the resources offered by the Internet, you don't really connect to the Internet–you connect to a network that is eventually connected to the Internet backbone, a network of extremely fast (and sometimes, unfortunately, overloaded) network components. This is an important point: the Internet is a network of networks, not a network of hosts. A simple network can be constructed using the same protocols that the Internet uses without actually connecting it to anything else. Such a basic network is shown in Figure 6.3.

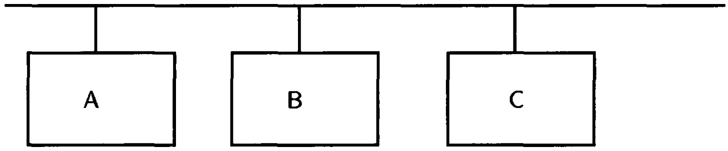


Figure 6.3 *A simple local area network.*

Let's say that I have a host connected to one of my employer's networks. We have a number of networks, which are all connected together on a backbone, a network of our networks. Our backbone is then connected to other networks, one of which is an Internet Service Provider (ISP) whose backbone is connected to other networks, one of which is the Internet backbone.

If you have a connection "to the Internet" through a local ISP, you are actually connecting your computer to one of their networks, which is connected to another, and so on. To use a service from my host, such as a Web server, you would tell your Web browser to connect to my host (by entering my URL). Underlying services and protocols would send packets (small datagrams) with your query to your ISP's network, and then a network they're connected to, and so on, until they found a path to my employer's backbone, and to the exact network my host is on. My host would then respond appropriately, and the same would happen in reverse–packets would traverse all of the connections until they found their way back to your computer, and then you would be viewing my Web page.

In Figure 6.4, the network shown in Figure 6.3 is designated "LAN 1" and shown in the bottom-right of the picture. This shows how the hosts on that network are provided connectivity to other hosts on the same LAN, within the same company, outside of the company, but within the same ISP, and then from another ISP somewhere on the Internet.

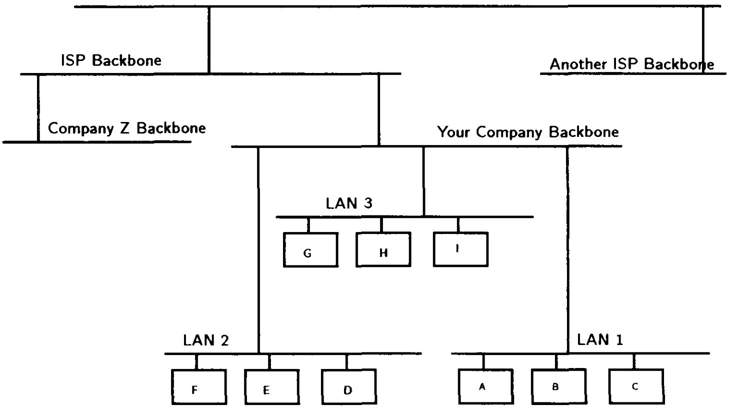


Figure 6.4
A wider view of Internet-connected networks.

TCP/IP: The Language of the Internet

The Internet is made up of a wide variety of hosts, from supercomputers to personal computers, including every imaginable type of hardware and software. How do all of these computers understand each other and work together?

TCP/IP (Transport Control Protocol/Internet Protocol) is the "language" of the Internet. Anything that can learn to "speak TCP/IP" can communicate on the Internet. This is functionality that occurs at the Network (IP) and Transport (TCP) layers in the ISO/OSI Reference Model. Consequently, a host operating system that has TCP/IP functionality (such as *Unix, OS/2, MacOS,* or *Windows NT*) can easily support applications (such as *Netscape Navigator*) that use the network.

Open Design

One of the most important features of TCP/IP isn't a technological one: the protocol is an "open" protocol, and anyone who wishes to implement it may do so freely. Engineers and scientists from all over the world participate in the IETF (Internet Engineering Task Force) working groups that design the protocols that make the Internet work. Their time is typically donated by their companies, and the result is work that benefits everyone.

IP

As noted above, IP is a "network layer" protocol. This is the layer that allows the hosts to actually "talk" to each other. Talking to each other would include such things as carrying datagrams, mapping the Internet address (such as 10.2.3.4) to a physical network address (such as 08:00:69:0a:ca:8f), and routing, which takes care of making sure that all of the devices that have Internet connectivity can find the way to each other. IP has a number of very important features which make it an extremely robust and flexible protocol. For our purposes, though, we're going to focus on the security of IP, or, more specifically, the lack thereof.

Attacks Against IP

A number of attacks against IP are possible. Typically, these exploit the fact that IP does not provide a robust mechanism for authentication, which is proving that a packet came from where it claims it did. A packet simply claims to originate from a given address, and there isn't a way to be sure that the host that sent the packet is telling the truth. This isn't necessarily a weakness, per se, but it is an important point, because it means that the facility of host authentication has to be provided at a higher layer in the ISO/OSI Reference Model. Today, applications that require strong host authentication (such as cryptographic applications) do this at the application layer.

IP Spoofing

This is an attack where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker: he can send packets to a host, perhaps causing it to take some sort of action. Additionally, some applications allow login based on the IP address of the person making the request (such as the Berkeley "r-commands"). These are both good examples how trusting untrustable layers can provide security that is, at best, weak.

IP Session Hijacking

This is a relatively sophisticated attack, first described by Steve Bellovin. It is very dangerous, however, because there are now toolkits available in the underground community that allow otherwise unskilled crackers to perpetrate this attack. IP Session Hijacking is an attack whereby a user's session is taken over, being in the control of the attacker. If the user was in the middle of email, the attacker is looking at the email, and then can execute any commands he wishes as the attacked user. The attacked user simply sees his session dropped, and may simply login again, perhaps not even noticing that the attacker is still logged in and doing things.

For a description of how this attack works, let's return to our large network of networks in Figure 6.4. In this attack, a user on host A is carrying on a session with host G. Perhaps this is a Telnet session, where the user is reading his email, or using a *Unix* shell account from home. Somewhere in the network between A and G sits host H which is run by an unauthorized person. The unauthorized person on host H watches the traffic between A and G and runs a tool which starts to impersonate A to G, and at the same time terminates A's session, perhaps trying to convince A that G is no longer on the network (which might happen in the event of a crash or major network outage). After a few seconds of this, if the attack is successful, the unauthorized person has "hijacked" the session of our user. Anything that the user can do legitimately can now be done by the attacker, illegitimately. As far as G knows, nothing has happened.

TCP

TCP is a transport-layer protocol. It needs to operate on top of a network-layer protocol, and it was designed to operate over IP. (Just as IP was designed to carry, among other things, TCP packets.) Because TCP and IP were designed together, and wherever you find one you typically find the other, the entire suite of Internet protocols is known collectively as "TCP/IP." TCP itself has a number of important features that we'll cover briefly.

Probably the most important feature of TCP is guaranteed packet delivery. Host A sending packets to host B expects to get an acknowledgment back for each packet. If B does not send an acknowledgment within a specified amount of time, A will resend the packet. Applications on host B will expect a data stream from a TCP session to be complete, and in order. As noted, if a packet is missing, it will be resent by A, and if packets arrive out of order, B will arrange them in proper order before passing the data to the requesting application.

This is suited well toward a number of applications, such as a Telnet session. A user wants to be sure every keystroke is received by the remote host, and that it gets an acknowlegment for every packet sent back, even if this means occasional slight delays in responsiveness while a lost packet is resent or while out-of-order packets are rearranged. It is not suited well toward other applications, such as streaming audio or video, however. In these, it doesn't really matter if a packet is lost (a lost packet in a stream of 100 won't be distinguishable) but it does matter if they arrive late (because of a host re-sending a packet presumed lost), since the data stream will be paused while the lost packet is being resent. Once the lost packet is received, it will be put in the proper slot in the data stream, and then passed up to the application.

UDP

UDP (User Datagram Protocol) is a simpler transport-layer protocol. It does not provide the same features as TCP, and is thus generally considered unreliable in the Internet community. However, although this is unsuitable for some applications, it does have much more applicability in other applications than the more reliable and robust TCP. One of the things that makes UDP nice is its simplicity. Because it doesn't need to keep track of the sequence of packets or whether they ever made it to their destination, it has lower overhead than TCP. This is one reason why it's more suited to streaming-data applications. We may hear more about UDP and its network applicability in the future.

Types And Sources Of Network Threats

Now, we've covered enough background information on networking to look at some specific security measures you can take to protect your network. First, we'll review the types of threats that exist for networked computers, and then we'll discuss some protective strategies.

Denial-of-Service

Denial-of-Service (DoS) attacks are perhaps the worst and most difficult to address. This is because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker without also refusing legitimate requests for service. The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to overload with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests (requests to the Web site running there, for example). Such attacks were fairly common in late 1996 and early 1997, but are now becoming less popular.

Some things that can be done to reduce the risk of your network security being comprised by a DoS attack include:

- Not running your servers at a level too close to capacity.
- Using packet filtering to prevent obviously forged packets from entering into your network address space. Obviously forged packets would include those that claim to come from your own hosts, addresses reserved for private networks as defined in RFC 1918, and the loopback network (127.0.0.0).
- Keeping up-to-date on security-related patches for your hosts' operating systems.

Unauthorized Access

"Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a Web server, and should provide anyone with requested Web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone authorized, such as a local administrator.

Executing Commands Illicitly

It's obviously undesirable for an unknown and untrusted person to be able to execute commands on your server machines. There are two main classifications of the severity of this problem, normal user access and administrator access. A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs to perform an unauthorized action. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

Confidentiality Breaches

There is certain information that could be quite damaging if it fell into the hands of a competitor, a criminal, or the public. In these cases, it's possible that compromise of a normal user's account on the machine can be enough to cause damage (perhaps in the form of advantage to a competitor or exposure of a client's personal financial records). While many of the perpetrators of these sorts of break-ins are merely thrill-seekers interested in nothing more than to see a shell prompt for your computer on their screen, there are those who are more malicious, as we'll consider next.

Destructive Behavior

Among the destructive sorts of break-ins and attacks, there are two major categories.

Data Alteration

This type of attack is likely the most difficult sort, since the fact of a break-in might not be immediately obvious. Perhaps the attacker revises the numbers in your spreadsheets or changes the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. In any case, rare is the case when you'll come in to work one day and simply know that something is wrong. An accounting procedure might turn up a discrepancy in the books three or four months after the fact. Trying to track the problem down will certainly be difficult, and once that problem is discovered, how can any of your numbers from that time period be trusted? How far back do you have to go before you think that your data is safe?

Data Destruction

In the case of wholesale destruction of data, the impact on your computing capability–and consequently your business–is not much less than if a fire or other disaster caused your computing equipment to be completely destroyed.

Where Do They Come From?

How, though, does an attacker gain access to your network? Through any connection that you have to the outside world. This includes Internet connections, dial-up modems, and even physical access. (How do you know that one of the temporary workers that you've brought in to help with the data entry isn't really a system cracker looking for passwords, data phone numbers, vulnerabilities and anything else that can get him access to your equipment?) Thus, in order to be able to adequately address network security, all possible avenues of entry must be identified and evaluated.

Lessons Learned

From looking at the sorts of attacks that are common, we can devise a relatively short list of high-level practices that can help prevent network security disasters and help control the damage in the event that preventative measures are unsuccessful in warding off an attack.

Make Sure You Have Backups

As discussed in Chapter 3, backing up data regularly is a good practice for several reasons. A breach of network security is only one source of risk to your network's data. If you have safely stored and reliable backup data, you can run your critical business applications from another location or restore damaged data on a compromised network.

Don't Put Data Where It Doesn't Need To Be

Although this should go without saying, many organizations do not observe this principle. As a result, information that doesn't need to be accessible from the outside world sometimes is, and this can needlessly increase the severity of a break-in dramatically.

Avoid Systems with Single Points of Failure

Any security system that can be broken by breaking through any one component isn't really very strong. In security, a degree of redundancy is good, and can help you protect your organization from a minor security breach becoming a catastrophe.

Stay Current with Relevant Operating System Patches

Exploiting old bugs is still one of the most common (and most effective) means of breaking into systems, so be sure that you have a staff member assigned to be responsible for staying in contact with your LAN system vendor and regularly updating your software.

Watch for Relevant Security Advisories

In addition to staying up to date with your network vendor, regularly read the publications of CERT (Computer Emergency Response Team, **http://www.cert.org/**) and CIAC (Computer Incident Advisory Capability, **http://ciac.llnl.gov/ciac/**).

Firewalls

As we've seen in our discussion of the Internet and similar networks, connecting an organization to the Internet provides a two-way flow of traffic. This is clearly undesirable in many organizations, as proprietary information is often displayed freely within a corporate intranet (that is, a TCP/IP network, modeled after the Internet, that only works within the organization). In order to provide some level of separation between an organization's LAN or intranet and the Internet, firewalls have been employed. A firewall is simply a group of components that collectively form a barrier between two networks. A number of terms specific to firewalls and networking are going to be used throughout this section, so we'll review them first.

Bastion host: A general-purpose computer used to control access between the internal (private) network and the Internet (or any other untrusted network). Typically, these are hosts running a version of the *Unix* operating system that has been customized in order to reduce its functionality to only what is necessary in order to support its functions. Many of the general-purpose features have been turned off, and, in many cases, completely removed, in order to improve the security of the machine.

Router: A special purpose computer for connecting networks together. Routers also handle certain functions, such as routing, or managing the traffic on the networks they connect.

Access Control List (ACL): Many routers now have the ability to selectively perform their duties, based on a number of facts about a packet that comes to it. This includes things like origination address, destination address, destination service port, and so on.

These can be employed to limit the sorts of packets that are allowed to come in and go out of a given network.

Demilitarized Zone (DMZ): The DMZ is a critical part of a firewall. It is a network that is neither part of the untrusted network nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous–someone who breaks into your network from the Internet should have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

Proxy: This is the process of having one host act on behalf of another. A host that has the ability to fetch documents from the Internet might be configured as a proxy server, and hosts on an internal intranet might be configured to be proxy clients. In this situation, when a host on the intranet wishes to fetch the **http://www.megasoft.com/** Web page, for example, the browser will make a connection to the proxy server and request the given URL. The proxy server will fetch the document and return the result to the client. In this way, all hosts on the intranet are able to access resources on the Internet without having the ability to direct talk to the Internet.

Types of Firewalls

There are three basic types of firewalls, and we'll consider each of them.

Application Gateways

The first firewalls were application gateways; they are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy servers. This software runs at the Application Layer of the ISO/OSI Reference Model, hence the name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy and be configured to do so) in order to use Internet services. Traditionally, these have been the most secure types of firewalls, because they don't allow anything to pass by default, but need to have the programs written and turned on in order to begin passing traffic. These are also typically the slowest, because more processes need to be started in order to have a request serviced. Figure 6.5 shows an application gateway.

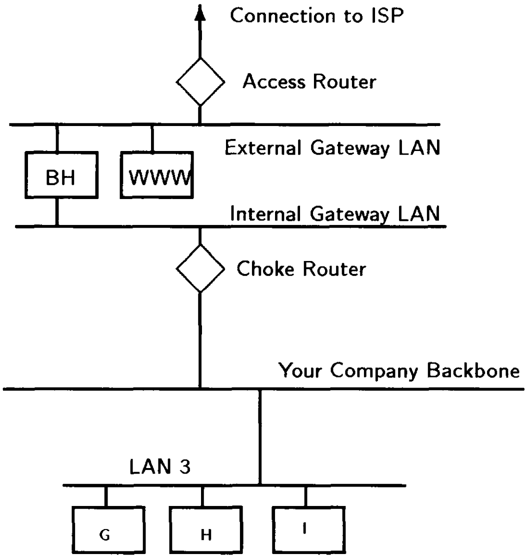


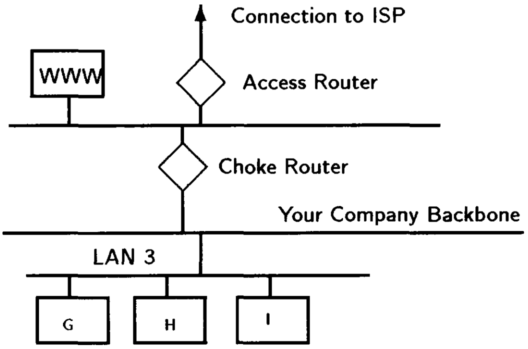
Figure 6.5 *A sample application gateway.*

Packet Filtering

Packet filtering is a technique whereby routers have ACLs (access control lists) turned on. By default, a router will pass all traffic sent though it and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Figure 6.6 shows a packet filtering gateway.

Figure 6.6
A sample packet filtering gateway.



Because this type of firewall works at a lower level than an application gateway, supporting new applications either comes automatically or is a simple matter of allowing a specific packet type to pass through the gateway. There are problems with this method, though. Remember, TCP/IP has absolutely no means of guaranteeing that the source address is really what it claims to be. As a result, we have to use layers of packet filters in order to localize the traffic. We can't get all the way down to the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal network. We can identify which network the packet came from with certainty, but we can't get more specific than that.

Hybrid Systems

In an attempt to combine the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both. In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters monitor the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) interaction are being passed.

Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection for your machines that provide services to the Internet (such as a public Web server) as well as providing the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

Making the Selection

Lots of options are available, and it makes sense to spend some time with an expert, either your in-house network administrator or an experienced consultant, who can take the time to understand your organization's information security policy and can design and build a firewall architecture that best implements that policy. Other issues like services required, cost, and upgrade options might factor in to the final design.

The business of building firewalls is in the process of becoming a commodity market. Along with commodity markets come lots of folks who are looking for a way to make a profit without necessarily keeping their customers' best interests in mind. Additionally, vendors compete with each other to try and claim the greatest security, the greatest east of administration, and the least visibility to users. In order to try to quantify the potential security of firewalls, some organizations have taken to issuing firewall certifications. The certification of a firewall means nothing more than the fact that it can be configured in such a way that it can pass a series of tests. Similarly, claims about meeting or exceeding U.S. Department of Defense "Orange Book" standards, C-2, B-1, and others, all simply mean that an organization was able to configure a machine to pass a series of tests. This doesn't mean that it was loaded with the vendor's software at the time, or that the machine was even usable.

Such gauges as market share, certification, and the like are no guarantees of security or quality. Taking a little bit of time to talk to some knowledgeable consultants can go a long way in providing you with a comfortable level of security between your organization's private network and the Internet. Additionally, it's important to note that many technical consultants are affiliated with particular vendors. Ask any consultants you talk to about their vendor affiliations, certifications, and experience in the network security field.

Secure Network Devices

It's important to remember that the firewall is only one entry point to your network. Modems, if you allow them to answer incoming calls, can provide an easy means for an attacker to sneak around (rather than through) your front door or firewall. Just as castles weren't built with moats only in the front, your network needs to be protected at all of its entry points.

Secure Modems and Dial-Back Systems

If modem access is to be provided, this entry point should be guarded carefully. The terminal server, or network device that provides dial-up access to your network, needs to be actively administered, and its logs need to be examined for strange behavior. Its password need to be strong, and accounts that aren't actively used should be disabled.

There are some remote access systems that have the feature of a two-part procedure to establish a connection. The first part is the remote user dialing into the system and providing the correct ID and password. The system will then drop the connection and call the authenticated user back at a known telephone number. Once the remote user's system answers that call, the connection is established, and the user is on the network. This works well for telecommuters working at home, but it can be problematic for users wishing to dial in from hotel rooms when on business trips.

Other possibilities include one-time password schemes, where the user enters her ID and is presented with a "challenge," a string of between six and eight numbers. She types this challenge into a small device that she carries with her that looks like a calculator. She then presses enter, and a "response" is displayed on the LCD screen. The user types the response back into the logon routine, and, if all is correct, the login will proceed. These are useful devices for solving the problems of passwords without requiring dial-back access. However, the devices have their own problems, as they require the user to carry them, and they must be tracked, much like building and office keys.

Crypto-Capable Routers

A feature that is being built into some routers is the ability to enact session encryption between specified routers. Because traffic traveling across the Internet can be seen by people in the middle, these routers are advantageous for providing connectivity between two sites–for instance, between a main and branch office.

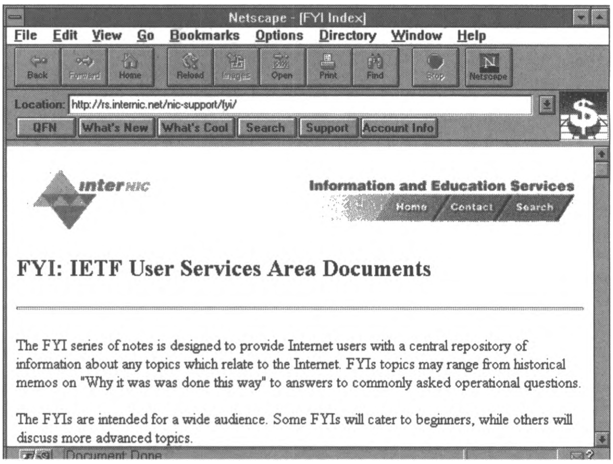
Virtual Private Networks

Traditionally, for an organization to provide connectivity between a main office and a satellite one, they had to lease an expensive, dedicated data line. Now, a solution that is often more economical is to provide both offices connectivity to the Internet. Then, using the Internet as the medium, the two offices can communicate. The danger in doing this, of course, is that there is no privacy through this communication channel, and it's difficult to provide the other office access to "internal" resources without providing those resources to everyone on the Internet.

Virtual Private Networks, or VPNs, provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although going over the Internet, is private (because the link is encrypted). A number of firewall vendors are including the ability to build VPNs in their offerings, either directly with their base product or as an add-on. If you have need to connect several offices together, this might very well be the best way to do it.

Learning More About Network Security

The most commonly referenced document available about Internet site security is the InterNIC's *Site Security Handbook,* also referred to as RFC 1244 and FYI 8. This document, originally developed in 1991, is included for your convenience in its entirely in this text as Appendix B. The Site Security Handbook is currently under revision–watch the InterNIC site (**http://internic.net**) for the posting of the new version.


Netscape - [FYI Index]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop Netscape
Location: http://rs.internic.net/nic-support/fyi/
QFN What's New What's Cool Search Support Account Info
interNIC
Information and Education Services
Home Contact Search
Document Done

FYI: IETF User Services Area Documents

The FYI series of notes is designed to provide Internet users with a central repository of information about any topics which relate to the Internet. FYIs topics may range from historical memos on "Why it was was done this way" to answers to commonly asked operational questions.

The FYIs are intended for a wide audience. Some FYIs will cater to beginners, while others will discuss more advanced topics.

Figure 6.7 *InterNIC Web site, location of RFC 1244, the Site Security Handbook.*

There are many additional resources available for locating environment-specific network security tips. One such document applicable to the *Unix* operating environment is *An Architectural Overview of Unix Network Security* by Robert B. Reinhardt of ARINC Research Corporation (**http://www.alw.nih.gov/Security/Docs/network-security.html**). You can perform a search at your favorite World Wide Web search engine to locate many more–phrase your query to include the words **network security** and the name of the operating environment you're interested in, such as ***Unix***.

For general discussions of network security issues, try the ***comp.security.misc*** Usenet newsgroup. To find more platform-specific information, try the newsgroup specific to your environment, such as ***comp.os.ms-windows***. The highly-popular Internet server operating system, *Unix*, has it's own security discussion newsgroup, ***comp.security.unix***. And, the ***comp.security.firewalls*** newsgroup contains even more specific information on firewall products, procedures, and configurations.

Network Security Planning Worksheet

Area	Current Policy or Practice	Points For Revised Policy/Practice
Identify the types and sources of network threats applicable to the organization.	Policy [ ] Practice[ ]	
With a network or system administrator, review the procedures currently used to protect the network from security breaches.	Policy [ ] Practice[ ]	
Establish procedure for regular update of system software and patches.	Policy [ ] Practice[ ]	
Determine whether or not the organization will utilize firewall technology; if so, select an appropriate firewall tool.	Policy [ ] Practice[ ]	

Determine whether or not the organization will use other types of secure network devices.	Policy [ ] Practice[ ]	
Identify who will be responsible for keeping abreast of network security issues.	Policy [ ] Practice[ ]	

Chapter 7
The Information Security Policy

Now that you have become familiar with the various types of risks and protections applicable to your organization's valuable information, you can go forward with developing a comprehensive information security plan. In most companies, information security planning ultimately takes the form of an Information Security Policy that is put in place at a high level of the organization and enforced uniformly throughout the organization. In this chapter, we'll review

- Components of the Information Security Policy.
- Risk analysis.
- Site assets.
- Identifying threats.
- Policy enforcement issues.

Components of the Information Security Policy

The authors of *Practical Unix Security* define security by saying that a computer system is secure "if you can depend on it and its software to behave as you expect it to" (Simson Garfinkel and Gene Spafford; Sebastopol, CA; O'Reilly & Assoc., 1991). Users of a computer system should be able to trust the system not only to protect their information, but also to make it available when needed.

The Information Security Policy ("security policy" for short) is a high-level document that describes the "whats" of security at a site rather than the "hows." When planning security for a single computer or a network site, the following types of security should be considered essential:

Privacy

Users of a computer or network system should be considered owners of the information (along with the company, of course) that they enter, and the system should ensure that no one has access to a user's information unless the owner of the information expressly grants that access. For instance, if you enter account information for a client at your stand-alone PC, you should be able to guarantee its confidentiality. To accomplish this security, you only need to restrict access to your PC. However, a larger network system, where employee payroll information is kept, will need to take more complicated measures to guarantee the privacy of the information.

Data Integrity

Owners of information and programs need to be assured that their information is safe from tampering. Deletion and alteration of information should be possible only with the consent of the information's owner. To extend the example above, once you enter your client's account information into your PC, you want to be assured that when you retrieve it later in the week with the client in your office that it has not been changed unless changes were made by you or someone authorized by you.

Availability

The computer system and the information it contains must be protected against threats that degrade performance or eliminate access. Again using the above example, if your client visits your office and wishes to see some account information, you need to be able to call up the information quickly. If your computer has been infected with a virus or has some other problems that don't allow you to find the file containing the client's information, the data has been compromised.

Consistency

Users of a computer system require the system to behave as expected. If programs suddenly start acting strangely, a security breach could occur. Imagine what would happen if the "dir" command were suddenly changed so that instead of listing the files in a directory, it deleted files with names beginning with "i" or "r." Consistency can fail as a result of an intruder process, but it can also be compromised as a result of a system software upgrade.

Isolation

Isolation is the aspect of security most people think of first. A system must be protected from unauthorized access both by unauthorized users external to the system and by internal users attempting to access data or resources beyond their authorization level. Returning to our example, you clearly don't want your client's competitors to have access to the accounting records you store on your PC. In addition, if you have an employee in your office whose responsibilities do not include working with your accounting files, you don't want them to be able to read or print the contents of your files.

Audit

This aspect of security handles recording activity on the system and allows administrators to identify the parties responsible for problems. Most computer system problems originate with authorized users rather than from outside attacks, so audit trails can help remedy internal problems as well as track attacks from outside the system. In a single-user system, auditing is not usually important since there are no log-in IDs to track. The file alteration dates are the only record you have of activity in the file system. Multi-user systems often have auditing facilities, and these facilities should be included in a security plan.

Planning

Advance planning is important. A well-planned security policy addresses the following issues:

1. What assets are you trying to protect?
2. From whom/what are you trying to protect these assets?
3. What is the likelihood of a threat?
4. What cost-effective measures can be taken to protect the assets?
5. What should happen if an asset is attacked?
6. What on-going reviews should be in place to keep protection up-to-date?

Notice that the security policy includes a lot of "whats" and no "hows." The security policy is a general game plan rather than a list of specific solutions to anticipated problems. If you are designing security policy and sentences like "smart cards and dial-back modems will be used on all systems" creep in, you know that you are involved in too much detail. In this case, you can wind up getting more security than you need in some areas and end up spending more money than is necessary.

One of the main reasons to take the time and come up with a detailed plan is cost efficiency. It would make little sense to spend thirty thousand dollars on a firewall system and an alarmed computer room to protect a personal computer that would cost two thousand dollars to replace. The overall goal of the security policy is to put measures in place that are the most cost-efficient and least inconvenient while still protecting the value of the computer system to the company or individual.

The security policy must also conform to existing policies, rules, and laws both inside and outside the organization. For instance, a security policy cannot deem it permissible to distribute copyrighted materials because that distribution is prohibited by U.S. and international law. Finally, the security policy needs to consider the system in a global context if it is going to be part of the Internet community. Each site needs to be aware of its responsibility for the security of the entire network.

Risk Analysis

Central to the security policy is a risk analysis of the computer system. The risk analysis will determine what assets you need to protect, from whom you need to protect the assets, how the assets can be protected, and the severity of each risk. This task will define the potential threats to the system and the methods to be used to reduce the risks posed by these threats. The costs of the risk reduction methods should also be considered at this point.

Site Assets

Although it may seem easy to pinpoint the assets of some companies, in other situations assets may be harder to identify. In a restaurant, it is easy to take a physical inventory of the stock and contents of the building, but if the restaurant is known for a particular dish, the recipe for the dish must also be considered an asset and protected against theft. Maybe the chef responsible for creating the dish would also be considered an asset, and if the recipe were written down, the recipe itself would need to be guarded against theft by the restaurant down the block. If the kitchen is run on electricity, the utility line carrying power to the building should also be considered an asset that needs protection.

The assets of a computer system might also be more than just the computer hardware. Hardware can be replaced relatively easily, but data that has been accumulated over time may be impossible to replace and invaluable to the operation of a company. The asset inventory must also include software that is important to the operation of the company.

Here's one way to begin to list the assets of a site:

1. Hardware: List all hardware items necessary to get work done. Include storage devices like hard disk drives and output devices like printers.

2. Software: List all software programs installed on the system, including operating system software and backup software.

3. Data: List all data files and online documents contained on the system. For example, if your company maintains a customer list and an inventory list online, the files involved in these databases should be considered an asset.

Once you know the things that should be protected, you need to rank them in terms of their importance. An indispensible asset should get a value of 10, while an asset that is lightly used should get a 1. (If an asset gets a 0, how could it be called an asset?) This step requires input from the users of the system. Again, if the computer is a stand-alone PC used by a single user, it will be fairly easy to rank the assets. The user just needs to look at the work done on the PC during the course of a day and make note of which hardware and software is most important to this work. In a larger company, it might be more difficult to rank the value of the system assets. You may find that users of larger systems don't know specifically which pieces of the system are needed to get their particular tasks done. In this situation, it would be better to poll the users and have them describe their uses of the system in their own words and then have a technical person review the descriptions and decide which assets are important in accomplishing the work described.

So, to get an idea of the importance of all of the assets in your list:

1. Ask all users to rate the importance of each component in the asset list using 0 if they don't use the component through 10 if they could not function without it.

2. Ask users to describe the work they do with the computer system in their own terms.

3. Re-evaluate the numeric entries after analyzing the description in Step 2.

For example, if a single user of a stand-alone computer uses a database management system to maintain a mailing list for his consulting business, the assets would include the database software and the data itself as well as the computer. This user might rate the computer as a 10 and the database program as a 10 as well, but only give the hard drive a 5. You would need to increase the rating for the hard drive since it is essential to the function of the database program. You may also need to rate the data files used by the user highly as well. This asset list might be the result of the asset review:

Asset	Value	Importance
Computer	$2,500	10
Database Management Software	$500	10
Customer List	$1,000	10
Word Processing Software	$495	1

The value of data can usually be estimated by deciding how long it would take to recreate the data files from scratch, and how much it would cost to pay the worker or workers needed to do this reconstruction. In our example, the customer list being maintained would take the single user a full work week to build again, and the data entry would cost twenty five dollars per hour, so the data file is valued at one thousand dollars. (Notice that the data itself is more valuable than the program that manages it.)

A larger company might have multiple workstations and many data files used to handle customer orders, shipping, inventory, and payroll. The asset evaluation would have to involve people from many departments in the company and would be much more complex. The main focus to keep in mind is that you need to establish not only the monetary value of the assets, but also the value to the users of the system. A single word-processing program might not be very high on the list of computer system assets in a ranking by purchase cost, but if every department in a company uses the program and all clerical work would grind to a halt if the program were unavailable for some reason, then the program must be considered very valuable to the company. It isn't uncommon to find that large systems have many users who use only a small portion of the system assets, while some assets are only used by very few users.

Now you have a list of all of the things you need to protect, and you can arrange the list according to the value of the asset to the functioning of the system and start thinking about the risks from which they need to be protected.

Identifying Threats

Once you have established a list of what is important to you and your users, it is time to consider what the possible risks to your assets could be.

Unauthorized Access

Unauthorized access can be as simple as use of an account owned by another user to access a system. John may leave his desk for lunch and leave himself logged in. Richard, who walks by the office and notices that the computer is on, uses John's terminal to retrieve information to which John has access but from which Richard is barred. Susan might remember to log herself out each time she leaves her desk, but keeps her password on a Post-It note stuck to her monitor. This type of unauthorized access is much more common than invasion by an outside person, though much less exciting and newsworthy.

Theft of Information

Any information stored on a computer is open to the threat of theft. A password file might be stolen to run a cracking program against the file at another computer. Research data could save a rival company years of investment in R&D. A new project or product proposal could be worth millions to a competitor. Any information that could be valuable to someone other than the owner of the information should be considered.

Denial of Service

As anyone who uses a computer knows, it doesn't take long for the computer to become an indispensable tool. If the computer becomes unavailable, it is often impossible to get any work done. Denial of service can come in many forms. A malicious or incorrect program can flood a network with packets and bring it to a standstill as discussed in Chapter 6. A virus can infect a computer system and slow or halt it completely as covered in Chapter 4. The security policy should determine which services are provided by the system to its users and try to predict the effect on the company if these services are disrupted.

Don't forget that electricity is the power behind the whole system. If you find that a certain file server is essential to operations and needs to be available twenty-four hours a day, seven days a week, you might consider an uninterruptable power supply (UPS) for that server.

Policy Issues

If you are designing security for a single-user PC, most of your work is finished when you have defined the assets and threats to the computer. If, instead, you are dealing with a multi-user system, more issues need to be addressed in the security policy, or they should be addressed in a separate Computer Use Policy, as discussed in Chapter Two.

Authorized Users

The security policy should explicitly define who is authorized to use which resources. For example, if a certain file server is to house payroll information, it should be explicitly stated that only those people employed by the payroll department are allowed to access that server or that particular information. The issues of information access rights covered in Chapter 2 also fall under this category.

Acceptable Use

As discussed in Chapter 2, users should also get some guidance as to what is considered appropriate usage of system resources. The following items should be addressed in the security policy or a companion Computer Use Policy:

- Users should not share accounts. Shared accounts make it impossible to use system auditing to assess responsibility for mishaps.
- If file access permissions are in place on the system, users should not assume they have permission to read a file simply because they have permission from the file system to do so, nor should they think that they have the right to modify a file they do not own simply because the operating system permissions allow them to do so. (Just because Steve mistakenly changed the file access permissions on the payroll file to allow anyone to edit the file does not give John the right to give himself a raise.)
- Breaking into accounts should not be tolerated.
- Password cracking should be prohibited. Bill in accounting should not be permitted to run a password cracking program in his spare time to try and get a password for another account. (*Note:* Some site administrators perform legitimate password checking procedures to check the safety of passwords.)
- Users should not be permitted to disrupt service to other users.
- Copyrighted software should not be duplicated.

The more explicit you make the "acceptable use" section of your security policy, the more clear, easier to follow, and easier to enforce it will be.

Responsibilities and Rights of Users

Users should be responsible for understanding and following security measures for the computer system. In addition, the security policy should contain the following:

- Resource consumption guidelines. Let the users know what is considered "excessive use" of resources like disk space, printer paper, or even CPU time.
- Password security guidelines. How cryptic should users make their passwords? How often (if ever) are users required to change their passwords? (See Chapter 2 for a useful set of passwork guidelines.)
- Backups. Does the network administrator maintain backups or are users expected to maintain their own?
- Proprietary Information. Let users know what information the company considers private and what sanctions exist for distributing proprietary information.

Responsibilities and Rights of System Administrators

In most multi-user systems, system administrators need to have unrestricted access to the entire system for maintenance and control. Your security policy should clearly state what limitations should be imposed on this access with respect to the users' rights to privacy. In what situations should a system administrator be allowed to read a user's files?

Sensitive Information

Somewhere in the security policy, a site needs to decide the level of security that will be provided. If security measures will be lax, this must be decided in the early stages and included in the policy so that users do not assume more security than that which exists and store sensitive information on your organization's computer systems. For example, if it is decided that anyone on the Internet should be able to use file transfers to place an order or retrieve a catalog list, and no precautions are going to be taken to protect its internal network from unauthorized file transfers, sensitive patent or research information should not be kept online.

What Happens When Policy Is Violated?

Every rule gets broken. When security policy violations happen, they are dealt with much more quickly and efficiently if the process is planned for in advance. Security violations might be due to user negligence or mistake. Perhaps the policy was not sufficiently explained or understood. If the course of action to be taken in the event of a violation is defined in advance, enforcement can be prompt. There may be legal issues involved in security violations, and a site is in a much better legal position if its security policy is well defined and published before incidents occur.

Sites that are connected to the Internet or other wide area networks must also establish policies to deal with local users causing problems on other systems on the network. What is your company to do when the system administrator gets a call about someone in payroll that has been caught trying to break into the payroll record system of a competitor? There may be legal liability issues that can be cleared up with a carefully formulated security policy. At the other end, what should happen if an intrusion on your local system is detected and traced to another site? Outside organizations like CERT and law enforcement agencies may need to be contacted, and publicity about the problem may or may not be released. In any case, the security policy needs to assign responsibility for making these decisions.

If an intrusion occurs, will the intruder's processes be immediately terminated, or will the intruder be allowed to continue unhampered while the system administrators trace the intruder's identity? These two strategies are called "protect and proceed" and "pursue and prosecute" in RFC 1244 (see Appendix B). Each strategy has its benefits and drawbacks. If the intrusion is immediately eliminated and the security hole that allowed it repaired, the system can be repaired and restored to normal operation more quickly. On the other hand, law enforcement agencies and prosecutors are urging more prosecutions of intruders, even though they cannot offer protection to a site reporting an incident if users initiate lawsuits alleging damage to their systems and data.

RFC 1244 recommends the following checklist to help decide between the two different approaches. A site needs to be able to confirm that all of the following statements are true before it considers trying to pursue and prosecute an intruder:

1. The system assets are well protected so that continued activity by the intruder will do no irreparable damage. Clearly if there is a risk of losing some irreplaceable data or program or having a system damaged or destroyed, then the intrusion should be stopped immediately rather than being allowed to proceed to gather information.
2. Good backups of all system software and data are available that can replace any files damaged by the intruder. If there is a risk that the intrusion could damage or corrupt data that is essential to site operations and the data could not be replaced from backups, the intrusion should not be allowed to continue. Say an intruder is detected attempting to access the data on orders received in the last week. If the file has not been backed up recently, the intruder should be stopped immediately; the intruder could alter the file and you would have no way of getting the original contents back.

3. Protection against future breakins are worth more to the site than risk to the assets from the current intrusion. Your site has had a couple of incidents in the last month or so, and you plan to continue to do business on the networks. It would be worth it in the long run to identify and prosecute the intruder now so that you could proceed with some guarantee that the attacks would stop.
4. The attack is one that occurs frequently. Every Monday morning, you find that someone has attempted to access your system all weekend.
5. The site is a natural attraction to intruders. Sites like large financial and defense institutions or research systems at universities seem to attract a large number of attempted breakins.
6. The site is willing to take the financial (or other) risk involved with letting the intrusion continue.
7. The intruder's access to the system can be controlled.
8. Monitoring tools are in place to gather information necessary to catch the intruder.
9. The system staff is sufficiently knowledgeable about the operating system and utilities to make pursuit worthwhile. Can they outsmart the intruder?
10. Management is willing to prosecute when the intruder is identified. This is often not the case; the publicity could damage a company more than any damage caused by the breakin.
11. There is sufficient legal knowledge about what type of information is needed for a successful prosecution.
12. There is established contact with knowledgeable law enforcement agencies.
13. There is someone at the site who knows the relevant legal issues.
14. The site is prepared for possible legal action from its own users if there is damage caused by the intruder.

The "protect and proceed" philosophy strives to patch the hole that allowed the intrusion without attempting to identify and prosecute the offender. You would want to protect and proceed if any of the following were true:

1. System assets are not well protected. It would be better to stop the intruder immediately, try and figure out the hole that was exploited to admit intrusion, patch it, and go on from there.
2. Continued access by the intruder could lead to great financial risk. Industrial espionage is getting more and more prevalent as companies become connected. If there is a chance that an intruder could cause the site to lose large sums of money, stop the intruder and lock them out in the future.
3. The company is unwilling to prosecute intruders. It is often the case that prosecution and the publicity attached would do more damage to a company's reputation than the security breach itself.
4. The users' work is vulnerable. Much of the work done on computer systems is done by people who know little about the systems themselves. If the users at a site are doing work online that is valuable to other sites, and if the users are not sophisticated computer users, it is better to stop intrusions as soon as they are detected.

Implementing the Information Security Policy

Once the security policy has been formulated in general terms, it is time to outline specific steps that will be taken at the site to put the security policy into action. The prioritized list of assets will be used now to devise mechanisms for the actual security of the site.

Spotting Problems

This list of site vulnerabilities comes from RFC 1244, and as the authors state, it "is by no means complete," but it gives a good starting point for hunting down soft spots in a site's security:

1. Access points

   For a single user PC, the only access point is the keyboard. This system can be secured by securing the keyboard, either by securing the room where the computer is located or by using a keyed power switch. As a system grows, its access points multiply, and each access point presents a potential security problem. Dial-in lines are often provided, allowing intruders access to an entire system. If the system is connected to the Internet and offers services like remote login or file transfer to users outside the site, unauthorized users may gain access by disguising themselves through the use of compromised passwords or spoofed origin addresses.

2. Misconfigured systems

   Some of today's networked operating systems have become so complex that just keeping up with the systems and their included software can become a full-time job. Hardware and software vendors may also ship products with insecure default settings. It is important to understand the default setting and make sure that any new software or hardware is installed to the specifications of the security policy, not left in the default configuration.

3. Software bugs

   No system as complex as today's computer programs can be engineered to be completely bug free. Unfortunately, some bugs can cause significant security holes. System administrators in charge of security must keep up with current security literature and always make sure that the most current versions of software are installed. CERT (The Computer Emergency Response Team) maintains a newsletter that informs people of known security holes in programs only after a work-around has been discovered. The Usenet security newsgroups are also good sources of announcements about holes discovered in programs.

4. Insider threats

   Contrary to what you see on the news, most computer security problems emanate from within a site. A disgruntled employee may vandalize programs or files. A user may inadvertently delete important files. These threats are the hardest to prevent, since measures installed to prevent their occurrence will almost certainly involve inconvenience to normal system users.

Balancing Protection and Cost

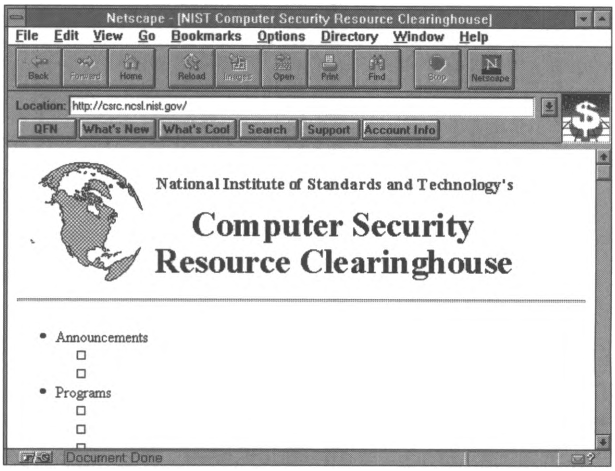
The information gathered in risk assessment will be used to design the actual security measures to be put in place. Don't forget that it makes little sense to place outlandish restrictions on the users and spend vast amounts of money to secure assets against risks deemed slight in the risk analysis phase of the security policy. If it was decided that there is very little risk in the event of power loss, it makes no sense to spend thousands on redundant uninterruptable power supplies.

It is also important to choose your controls correctly. There are ways that users can be authenticated by voice or fingerprint, but these controls are expensive, and if you have decided that the site's major risk was from offsite, they make little sense. Remember that simple controls are just as important as elaborate security systems. A single user with a poor password can negate the most elaborate security system.

Learning More About Information Security Policies

One of the best ways to begin learning about information security policies is to review some. Appendix A of this text includes three sample policy documents: (1) Contra Costa County's *Acceptable Use, Standard Practice and Security Policies*; (2) Hermann Hospital Clinical Information System's *Hermann Hospital Information Security Policy Draft;* and (3) The Arctic Region Supercomputing Center's *User Security Policies.*

The National Institute of Standards and Technology's Web site, called the *Computer Security Resource Clearinghouse,* maintains a list of "Security Policy Documents" at **http://csrc.ncsl.nist.gov/secplcy/**. Through this listing, you can link to, among many other documents, Chapter 10 of the Department of Commerce's *DOC IT Management Handbook,* which contains the information security policies for the Department.



Netscape - [NIST Computer Security Resource Clearinghouse]

Location: http://csrc.ncsl.nist.gov/

National Institute of Standards and Technology's

Computer Security
Resource Clearinghouse

- Announcements
  - □
  - □
- Programs
  - □
  - □

Document Done

Figure 7.1 *Computer Security Resources Clearinghouse Web site of the National Institute of Standards and Technology.*

Stephen L. Arnold, Ph.D. of Arnold Consulting Inc. has posted a Web site version of his "Security Policies for the Internet" presentation delivered at the DECUS US Chapter Symposium in San Francisco in 1995 (**http://www.arnold.com/POLICIES_9512_SLIDES.HTML**). This document contains a lively discussion of security issues and some useful guidelines for distinguishing between policy-level information and specific technical procedures.

In addition to the newsgroups applicable to your system's operating software, such as ***comp.os.ms-windows***, look for discussions of security policy issues in ***comp.security.misc*** and ***comp.security.unix***. The ***comp.admin.policy*** newsgroupgroup carries discussions of computer use and information security policies, as well as other computer administration topics.

Information Security Policy Outline

I. Risk Analysis

   A. Site Assets
   B. Identification of Threats

II. Physical Security (include relevant policy items from Physical Security Planning Worksheet)

III. Viruses (include relevant policy items from Virus Protection Planning Worksheet)

IV. Encryption (include relevant policy items from Encryption Planning Worksheet)

V. Network Security (include relevant policy items from Network Security Planning Worksheet)

VI. Individual Computer Use (you may decide to detach this section and instead create an Computer Use Policy with these items)

   A. Authorized Users

   B. Responsibilities and Rights of Users

      1. Resource consumption guidelines
      2. Acceptable Use
      3. Information Access Rights
      4. Passwords
      5. Personal Information
      6. Netiquette and Corporate Image
      7. Copyrights and Proprietary Information

   C. Responsibilities and Rights of System Administrators

VII. Enforcement

   A. Penalties for Internal Violators

   B. Approach for External Violators

VIII. Security Policy Update Mechanism

Appendix A
Sample Security Policies

Contra Costa County Acceptable Use, Standard Practice & Security Policies

Purpose

To define the criteria for acceptable use and the standard practices that Contra Costa County employees must follow when using County computers and computer data. Use of computer technology has grown rapidly in recent years, reflecting the proliferation of microcomputers and networks. County employees are making extensive use of technology-based systems for to conduct business in a more effective, effecient manner. Furthermore, current and planned developments in County networks promise to make these capabilities even more accessible and powerful. Therefore, it is important to ensure these systems are used appropriately.

Policy

The Contra Costa County Board of Supervisors has established policies governing the use of County computers and computer data. Those policies are presented here for completeness. Those policies are:

- Board Resolution 95/560
- Resolution 95/560 Attachment #1: Employee/Contractor Responsibility Statement
- Resolution 95/560 Attachment #1 Exhibit 1: Do's And Don'ts For Network Users (Passwords, Modem, Security, Good Practices)
- Resolution 95/560 Attachment #1 Exhibit 2: Excerpts From Calif. Penal Code Section 502 On Computer Crime
- Resolution 95/560 Attachment #2: W.A.N. Access Standard
- Computer Security Memorandum Of Agreement (MOA)

Board Resolution 95/560

Upon the recommendation of the County Administrator, the Contra Costa County Board of Supervisors in its capacity as governing board of the County of Contra Costa and of all the Districts and agencies of which it is the ex-officio governing board,

Resolves that:

This resolution supersedes the Board's September 29, 1987 order on personal computer use. The following policies govern the use of Contra Costa County computers and computer data. The County Administrator is authorized to adopt regulations on the implementation of these policies:

1. Employees are to be encouraged to use personal computers in County departments to promote greater staff productivity.

2. The equipment, software, programs and all County data developed and/or entered on County computers and

County data entered on home computers is property of the County.

3. Subject to applicable legal privileges and confidentiality requirements, all County data entered on County computers and County data entered on home computers is not private and is subject to disclosure upon the demand of authorized County officers at any time.

4. County policies on the use of personal computers, software, software licensing and other desktop technology are expressed in attachments one and two hereto.

5. Department heads shall inform county employees of and review, on an ongoing basis, adherence to, the County's policies for the use of personal computers, software, software licensing and other desktop technology.

6. Data Processing Services will annually publish a County-wide policy regarding use and licensing of software on County computers.

7. Subject to prior written Department head approval and to the policies expressed herein, County employees may use County computers for personal matters during non-work hours.

Resolution 95/560 - Attachment #1: Employee/Contractor Responsibility Statement

Purpose Of This Responsibility Statement And User Agreement: Computer security has become an increasing concern for County government as computer access and usage have increased through the availability of networks and personal computers. It is therefore necessary that all employees and contractors using County computers, or processing County data on home computers, acknowledge awareness of good computer security practices and agree to follow these practices. This statement is intended to protect the County and County employees authorized to access and use County data from unauthorized access to the data.

Provisions of This Responsibility Statement:
County employees and contractors shall comply with County standards for computer security and usage, including, but not limited to, the following:

- Good password and modem management (Exhibit 1 attached)
- Good security practices (Exhibit 1 attached)
- Proper log-off from systems and networks
- No introduction of any software or hardware onto County systems or networks without written authorization from your Agency/Department computer systems support staff
- Regular use of virus protection software
- No illegal or unlicensed software usage (one user/license)
- No attempts at unauthorized access to any County systems or data, or for which you have no legitimate business need

- Use of county Internet access only for legitimate County business

- No unauthorized printing of and/or changes to data to which you have access, or giving of access to that data to persons not authorized to view or use that data

- No copying of software from one computer to another without authorization of your Agency/Department computer support staff

- Running only pre-approved processes over networks so as to avoid generating excessive network traffic that might negatively impact other network users

- No masking the identity of an account or machine, including, but not limited to, sending mail anonymously

- No usage of County computers for unlawful or illegal practices; for the personal profit of yourself or others; or for personal activities that have not been pre-approved in writing by Agency/Department management.

- No usage of County computers or network for the creation or dissemination of harassing or demeaning statements about individuals or groups, or of sexually explicit materials

- California Penal Code Section 502 (excerpts attached as Exhibit 2)

All information resources on any County-owned network or system are the property of the County, and are subject to County and Agency/Department policies on computer security and acceptable information resources usage. Any software developed on County time or using county computer resources is the property of the County. There is no presumption of privacy for persons using County computers or County networks. Persons using computers or sending electronic mail should make the same provisions to ensure confidentiality as would be taken for sending hard copy correspondence. All activity on County computer resources is subject to monitoring by Agency/Department and County computer systems support staff as part of their responsibility for ensuring system integrity and compliance with security standards. Such monitoring may include access personal computers without notice to investigate possible security breaches.

Rev. 10/9/95

Resolution 95/560 - Attachment #1 - Exhibit 1: Do's and Don'ts for Network Users

Passwords

Almost 90% of computer network security incidents can be traced to poor or mismanaged passwords. Following several basic rules for passwords is critical in preventing network break-ins.

1. Never share your password with anyone.

2. Don't write your password down, and don't be tempted to give your password to someone over the phone, on electronic mail or via fax.

3. Follow the basic rules for constructing good passwords. A good password is a least 8 characters long and includes at least one number and/or punctuation character. Good passwords are words that are not found in the dictionary!

Don't use your name, your spouse's name or your children's name as a password.

4. Choose a password that you can remember. Combine two meaningful words with punctuation, or select a phrase and use the first letter form each word. If your system accepts long passwords, you may want to use a "passphrase", which is a phrase that your can remember easily but that someone else cannot guess.

5. Don't embed your password in a login script or assign it to a function key.

6. Change your password at least once a year; more often is desirable.

Modem Security

1. Never attach a dial-up modem to a County PC or workstation without coordinating with your Agency/Department computer systems support staff.

2. If you have dial-in access to a county computer, treat the dial-in number as sensitive information.

3. The rules for good password management apply to dial-in modem passwords.

Good Practices

An alert user can help detect or prevent attempted break-ins.

1. Some computers supply a "last login" date when you log in. Pay attention to when the computer thinks you last logged in;' if there is a discrepancy, notify your System

Administrator. Someone else may have logged in from your account!

2. If you are leaving your desk for a period of time, log off from the computer - especially if you are in a public area. If you have a "screen lock" feature, you can use that instead of logging out.

3. Don't let anyone look over your shoulder while you enter your password.

4. If you can set access permission for your files and directories, set them to be as restrictive as possible.

5. Don't install free or "shareware" software on County computers. This software may contain viruses or trapdoors that later allow intruders access. This also applies to software that can be obtained over the Internet.

6. Be conscious of the physical security of your equipment, especially if you work in an area visited often by persons from outside your Department or form the public. Lock doors to offices when not used or during off-hours. Maintain physical security of any portable computer equipment such as laptops or notebooks.

Rev. 8/9/95

Resolution 95/560 - Attachment #1 - Exhibit 2: EXCERPTS FROM CALIF. PENAL CODE SECTION 502 ON COMPUTER CRIME

California Penal Code Section 502 states, in part, that any person is guilty of a public offense who:

1. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system or computer network in order to either A) devise or execute any scheme or artifice to defraud, deceive, or extort, or B) wrongfully control or obtain money, property, or data.

2. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

3. Knowingly accesses and without permission adds, alters, damages, deletes,, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

4. Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

5. Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

Resolution 95/560 - Attachment #2

Contra Costa County
LAN/WAN Committee
Security Sub-Committee
July 20, 1995

To: LAN/WAN Committee Members
From: CCC W.A.N. Security Sub-Committee
Subject: W.A.N. Access Standard

In order to be granted access to the County W.A.N., individual departments must conform to the following minimum standards for security. If the requesting department does not meet these standards, their case will be reviewed by the County W.A.N. committee, and their access may be granted or denied by that committee. Departments that are on the WAN must meet these requirements by June 30, 1996. If they have requirements that they cannot meet, their WAN access must be reviewed by the WAN committee.

Physical Security:

- All servers, hubs, routers, and network switches must be housed in locked or entry restricted rooms.

- All user machines in non-secure work areas must be turned off overnight. Users must be logged off. This does not apply to systems that are in use 24 hours/day.

- All machines with public access must have the floppy (or other user inserted) drives removed or locked.

- At least one copy of systems backup media must be stored off site.

Password Security:

- All network including home machines must be password protected.

- All network user accounts must be password protected.

- Each network user must have a unique user id., or if there are group id's, they must have limited access.
- All passwords must be formulated based on strong password rules.
- All passwords stored on the system must be in encrypted format.
- All passwords must be changed without repetition at least every 3 months.
- All users must be directed to not share their passwords
- All users must be directed to not keep their passwords written down using a non-secure method.

Administrative Procedures:

- Full L.A.N. backups must be performed locally at least every two weeks.
- Incremental L.A.N. backups must be performed locally at least every two days.
- Administrator / Supervisor, Super user access must be limited to a few knowledgeable individuals, who actively engage in administrative activities.
- Regular users must not have file "write" permission in systems directories where executable files are stored unless necessary.

- Users attempting network/system logins must be locked out after three sequential unsuccessful logins.

- Guest, demo, or other anonymous accounts without passwords are not allowed.

- Systems rights and privileges should be conservatively assigned.

- All network servers must have anti-virus software installed and operational at all points of entry if the software is commercially available.

- Inactive user accounts must be disabled after 3 months and removed after 6 months.

- Terminated users must be removed immediately.

Modems:

- All modems must be inventoried.

- All dial-in modems must have call-back, have supervised access, or other approved (by the WAN Committee) security device(s) implemented.

- All modem dial-ins must be restricted to real need users.

- Modem usage must be logged where possible, and usage should be audited and reviewed regularly.

- Modem phone line numbers must be treated as confidential.

New Device Implementation Policies:

Before any new servers, routers, dial-in/out, Async servers, hubs or non-standard devices are attached to the WAN, the department wishing to attach the device(s) must first notify the Network Support Group at county DP, describing what the equipment is, and if it is a server, the server name and network address, and the data and time that the device(s) will be connected to the network. The data and time, and other pertinent information will be made available to all other WAN members via a publicly accessible bulletin board or some other electronic form of communication.

New Process Implementation Policies:

Before any new process is run across the WAN, the department wishing to run this process must first notify the Network Support Group at County DP, describing what the process is, the extent and type of data to be sent across the network, the source server name and network address, and the date and time that the process will be run across the network. The data and time, and other pertinent information will be made available to all other WAN members via publicly accessible bulletin board or some other electronic form of communication, so that the effects on other users can be monitored. Based on monitoring results, the process may be approved for standard operation across the WAN.

County of Contra Costa

Computer Security Memorandum of Agreement (MOA)

Purpose of This MOA:

This MOA signifies that County Agency/Department Heads are cognizant of their responsibilities for the maintenance of strong computer security within their Agencies/Departments.

Importance of Computer Security:
Increasingly, important and sensitive data is processed and stored on County computers. The advent of local area networks (LAN's) and wide area networks (WAN's), and of improved capabilities for all types of computers to communicate with each other, increases the risk that County data can be inappropriately accessed and used. These developments also make one Agency/Department's data vulnerable to security lapses by other agencies/Departments. Adherence to good computer security County-wide reduces these risks.

Essence of This Agreement:
This MOA is an agreement between an Agency/Department Head and the County Administrator whereby the Agency/Department Head agrees to the provisions of this MOA and of other computer security policies developed for the County. In particular, the signing Agency/Department Head agrees that employees and contractors of the Agency/Department who use County computers will be notified of the need for good computer security practices, and have received the County's Employee/Contractor Responsibility Statement (Attachment 1). The Agency/Department Head also agrees to comply with the guidelines expressed in the Contra Costa County WAN Access Standards document (Attachment 2) and to enforce good computer security by applying appropriate sanctions against persons who knowingly breach computer security or who repeatedly create inadvertent security risks.

Agency/Department Computer Security and Disaster Recovery Plans:
Each Agency/Department agrees to develop a computer security plan and a disaster recovery plan, each of which will be reviewed by a group designated by the County-Wide Information Technology Steering Committee (ITSC), and to update these plans

on an annual basis. Any disagreements on compliance with County security policies will be reviewed by the County-Wide Information Technology Steering Committee.

Acceptance:

Agency/Department: ________________________________

Signature: ________________________ Date Signed:_______

Rev. 10/9/95

Hermann Hospital Information Security Policy Draft

I. Purpose

A. To provide guidelines for ensuring that authorized persons have timely and appropriate access to computerized information, while safeguarding the information's confidentiality, security, and integrity.

II. Policy

A. Definitions

1. Security Protection of information resources from unauthorized change, destruction, or disclosure, whether intentional or accidental.
2. Such information resources include, but are not limited to, all Hermann-owned or managed computer and telecommunications : hardware, software, storage media, computer signon codes, information transmitted, stored, printed, and/or processed by a computer system
3. Confidential Information Requires special safeguards due to private nature. Examples Patient care information, including all information regarding a patient's identity, treatment, and diagnosis Personnel information regarding employees' salaries, benefits, performance reviews, and disciplinary action.

B. Development and support of information security processes

1. Hermann will implement processes to ensure sufficient security and confidentiality for its information. These porcesses will address the following issues:
   a. Who has access to information

b. The information to which each individual has access

c. The obligation of the individual who has access to information to keep it confidential

d. The release of information

e. The mechanisms to secure information against loss, destruction, tampering, and unauthorized access or use

2. Hermann will address security issues during the purchase and implementation of new information systems

3. Management staff in each department will develop and maintain information security policies specific to their department, if appropriate, which are consistent with this policy.

4. The orientation program for new employees will address Hermann's information security policies. At the time of orientation, each new employee will sign a confidentiality agreement that summarizes Hermann's information security policies and the individual's responsibilities regarding these policies. This agreement will be filed in the employee's records in Human Resources.

5. Management staff in each department will inform their staff of institutional and departmental information security policies. Management will ensure that these policies are addressed at departmental staff meetings annually.

C. Authorization to Access information resources

1. Only persons who have valid business reasons for accessing Hermann's information resources will be granted access. Individuals will be given access to information resources in keeping with their job requirements. Management in each department is

responsible for determining what information resources its employees need to access in order to complete their job functions Hermann department heads are responsible for determining which information resources will be made accessible to physicians, students, and third parties having business relationships with Hermann

2. No one may access Hermann's information resources or applications without prior written authroization and approval. It is illegal to use a Hermann computer or access inofrmation stored or maintained by a Hermann computer without the consent of Hermann (Texas Penal Code, Section 33.02).
3. All passwords to Hermann's computer systems are confidential and are the property of Hermann Hospital. These include, but are not limited to, passwords to network systems, mainframe systems, PCs, voice mail, and long distance telephone codes. It is a crime, punishable by fine and imprisonment, to reveal passwords to anyone without Hermann's permission (Texas Penal Code, Section 33.02).
4. Computer equipment security
   a. Terminals, network devices, and personal computers in unsecured areas will be secured against theft and use by unauthorized persons.
   b. Personal computers in unsecured areas will be set up to use power-on passwords and keyboard passwords, to prevent unauthorized persons from using the device without providing the appropriate password.
   c. Anyone who signs on to a computer system must sign off and/or physically secure the terminal or PC when leaving it unattended

   d. Where possible, computer systems wil be set up to automatically sign off or password-protect terminals and PCs after a specified period of inactivity
   e. Access to data centers will be secured by means of locked entryways. Only persons authorized to operate or maintain the computer systems will be issued keys, passcards, or other means for unlocking the entryway. Authorized visitors to the Data Center will be escorted by authorized staff.

5. Security of computer-related media
   a. Printed reports containing confidential or sensitive information will be stored in a secure area, inaccessible to unauthorized persons. Confidential reports will be rendered unreadable before being discarded.
   b. Diskettes, tapes, and other media containing confidential information will be labeled "confidential" and will be portected appropriately.
   c. Diskettes, tapes and other medial containing computer files will be stored in areas accessible only to authorized persons.
6. Protection of computerized files
   a. Departments and indivduals must establish regular schedules for making backup copies of data files stored on personal computers, network file servers, and other computer systems.
   b. Backup copies will be stored in a safe location (not exposed to heat or magnetic fields). Backup copies for network file servers and mainframe computer systems will not be stored in the same room as the servers or data storage devices.

c. Virus protection programs will be installed and executed regularly on each PC and computer system.

d. Software will not be copied from public access bulletin boards or other non-Hermann computer systems without first being scanned by a virus protection program.

7. Dial up access to information resources

a. Authorized employees, physicians, and other authorized parties will be permitted to use telephone lines to access Hermann information resources, with proper safeguards.

b. All dial-up connections to Hermann computer systems will be routed through devices that provide for password verification, call-back security, or other similar security features.

c. Modems or personal computers that do not have dial-up access security features will not be connected to direc-inward-dial telephone lines.

8. Violations of information security policy

a. Failure to comply with these information security policies and procedures may result in Level III disciplinary action, termination of access privileges to Hermann inofrmation systems, and civil or crinimal legal penalties, at the discretion of Hermann management.

b. Management staff in each department will monitor and counsel their staff in matters of inofrmation security.

III. Procedure
   A. Security administration
      1. A system security adminstrator will be designated for each network system and each mainframe application
         a. System security administrators will be responsible for issuing signon codes for the system(s) for which they are responsible. System security administrators are responsible for ensuring that all persons who receive signon codes have proper authorization to access the system.
         b. The Information Systems Department will maintain a list of all designated system security administrators and their backups.
   B. Obtaining authorization to access information resources
      1. Requests for access to Hermann's information resources must be submitted in writing to the appropriate system security administrator.
      2. Requests for access to information resources must be approved by the appropriate Hermann management, as follows:
         a. Hermann employees: Authorization by the employee's supervisor.
         b. Physicians: Authorization by a Hermann Chief of Service
         c. University of Texas Health Science Center employees: Authorization by a UTHSC department head and a Hermann department head.
         d. Students: Authorization by the appropriate dean of students and a Hermann department head
         e. Third parties having business relationships with Hermann (such as payers, vendors, consultants,

regulatory agencies, etc.): authorization by a Hermann department head.

3. All persons who request access to computer systems will be required to sign a Confidentiality Agreement that summarizes Hermann's information security policies and the individual's responsibilities regarding these policies.

C. Issuance of computer signon codes

1. Each person authorized to access a Hermann computer system (mainframe, minicomputer, or network) will be issued a unique, individual identification code and password. The person must supply this identification immediately after initial contact with the computer, or further access will be denied.
2. Each authorized user of Herman computer systems will have a unique personal password associated with his or her user identification code. Each person is responsible for changing this password periodially (at least every 90 days) on systems where this can be done.

D. Termination of access to information resources

1. A person's access to Hermann's information resources will be revoked upon termination of employment or contract with Hermann; upon transfer to a different department; or at the request of the person's supervisor or department head.

Author: Alan S. Tonnesen, MD

Last Update: 5/15/95

User Security Policies

Introduction and Enforcement

Every user of ARSC systems can rightfully expect his or her e-mail, programs, data, documents, etc., to be inaccessible to others, secure against arbitrary loss or alteration, and available for appropriate use, at all times.

To help achieve this goal of protecting system security, ARSC system administrators reserve the right to routinely examine certain features of user accounts, such as the permissions set on environment files, the contents of specific environment files, and encrypted passwords. ARSC also reserves the right, in cases of suspected security incidents, to inactivate and examine the general contents of user accounts, without prior notification. ARSC employs several mechanisms to enforce its user security policies, including:

- Contacting the user and asking him or her to correct the problem;
- Changing the permissions on the user's home directory to 700;
- Inactivating the account;
- Resetting the user's password.

By accepting your account at ARSC, you accept these policies.

Policies

1. Security Level
   ARSC operates an unclassified system. Don't do classified work on ARSC systems.

2. Security Awareness
   Report your suspicions. For instance, if a file in your directory seems to have changed, but you don't remember having changed it, contact User Services (phone: 907-474-5102 or e-mail: consult@arsc.edu).

3. Passwords
   You must maintain a secure, unbreakable password. Please read our password protection policy for hints on choosing and remembering passwords.

   To enforce this policy, ARSC analysts periodically run password cracking programs, and if your password is cracked, we will attempt to contact you to change it. If you are unreachable, we will reset it and/or inactivate your account. This protects your account as well as ARSC systems.

   When ARSC resets your password, it uses your "default" password. At any time, if you feel that your default password letter (which was either issued with your new account or, if you were an early ARSC account holder, mailed to you in January, 1997) may have been compromised or misplaced, contact us immediately and we will issue you a new one. ARSC will not communicate passwords via phone or email.

   On its Cray platforms, ARSC runs a program which "locks" an account if five consecutive attempts to log on fail. Thus, if you mistype your password five times, your account will be locked, and, even if you type correctly the sixth time, you will not be able to log in (contact us to have the lock removed). The purpose of this measure is to prevent others from making multiple guesses of your password.

4. Account Sharing
   You may not share your account with anyone under any circumstances.

   This requirement makes every user solely accountable for all actions extending from his or her account. Two ways to share your account are listed here, either one is considered a violation:

   - Password sharing–Don't give anyone your password.
   - .rhosts file–Don't give anyone, other than yourself, rlogin permissions via your .rhosts file. (Please review the .rhosts files policies for details.)

5. Home Directory Permissions
   Your home directory must never be group-writeable or world-writeable.

	Recommended Permissions
Home Directory	700, 710, or 750

6. Environment (or "Dot") Files
   Your environment files must never be group-writeable or world-writeable. Additional restrictions apply to .netrc, .rhosts, and .Xauthority files, as described in detail.

Environment files are executed automatically as a consequence of some normal, frequent activity on your part (like logging on) and thus, they are a prime target for anyone trying to compromise your account.

Dot File	Description	Recommended Permissions
.cshrc	csh file, executed only on login	400, 440, 600, or 640
.forward	mail forwarding file	400, 440, 600, or 640
.kshrc	ksh file, executed each time ksh is executed	400, 440, 600, or 640
.login	csh file, executed each time csh is executed	400, 440, 600, or 640
.netrc	file with configuration information for ftp access to a remote machine.	400, 440, 600, or 640
.profile	ksh file, executed only on login	400, 440, 600, or 640
.rhosts	file of remote hosts and account names	400 or 440
.Xauthority	contains xauth magic cookie	600 only
.xinitrc, .xsession, .Xdefaults, .Xresources	X Window System environment files	400, 440, 600, or 640
Other Environment Files	files used by less common shells and programs	400, 440, 600, or 640

netrc_policy

.netrc files contain login information and configuration data for ftp access to remote machines. When ftp is opening a connection to a specified remote machine, it checks for this file in the user's home directory on the machine initiating the file transfer.

ARSC policies on .netrc files are:

1. no passwords are permitted in .netrc files unless the username is "ftp" or "anonymous."
2. users may not maintain passwords for ARSC systems in .netrc files stored on other computers

rhosts_policy

.rhosts files specify a list of trusted remote hosts and account names. The .rhosts file allows a user to log in to the account free of the normal user validation. Hence if present it must be between two or more secure systems.

ARSC can only ensure a secure system among ARSC machines and cannot enforce its security policies on other remote hosts. As a result, use of the .rhosts file between ARSC computers and remote hosts presents a security risk for all ARSC users.

ARSC policies on .rhosts files are:

1. rhosts files may give access only between ARSC systems. However, the host, fosters.arsc.edu (the ARSC www/ftp server), is an exception to this policy, and may not appear in a .rhosts file.
2. Host names must be fully qualified domain names, e.g., "onyx3.arsc.edu"
3. The userid in the .rhosts file must match the login id of the home directory that contains the .rhosts file.

4. rhosts files must not be writeable by anyone: not even the owner.

Xauthority_policy
An .Xauthority file contain a key (magic cookie) used by xauth to authenticate X Window System requests to initiate processes on remote systems. If someone could read this file, they could obtain the key and circumvent the security provided by xauth.

ARSC policies on .Xauthority files are:

1. The file permission for the .Xauthority file MUST be 600 only

7. Java and Related Languages
Background

Java and JavaScript enable web page developers to include within a web page snippets of code (e.g., Java 'applets') which, when executed by the web browser, dynamically generate content for that web page. As more web pages make use of this feature, more web browsers appear with the ability to accomodate them. Netscape 3.0S, the version of Netscape provided by ARSC under IRIX 6.2, handles both Java and JavaScript.

With these options enabled, when you download a web page containing such code, that code is automatically executed by your browser, and it is not in general possible to know in advance the presence or purpose of such code. The dangers involved in this automatic execution of unknown code downloaded from the Internet are such that these languages and their interpreters were carefully designed to disallow certain types of actions, such as the modification or deletion of files.

Nevertheless, reports regularly reach ARSC of newly discovered exploitable security holes and bugs found in both Java and JavaScript. Some of these security holes enable hostile applets to execute arbitrary commands that can modify or delete important system or user files.

Java and related languages are relatively new and are undergoing rapid development. It is to be hoped that as they mature these security holes will be firmly plugged, and ARSC is monitoring their development.

ARSC Policies Concerning Java and Related Languages

Due to the security considerations discussed above, and until further notice, ARSC is disallowing the execution of Java and related code downloaded from the Internet. Such code includes:

- Java applets
- standalone Java applications
- web pages containing JavaScript

With respect to the system copy of Netscape 3.0S, the associated Java interpreter has had world execute permissions removed. Use of JavaScript, however, cannot be globally disabled, and since it is not possible to know in advance whether a requested web page contains JavaScript, when using Netscape you are required to disable JavaScript locally:

- select 'options' from the menu bar
- select 'network preferences' from the options
- select 'languages' from the network preferences
- uncheck the 'Enable JavaScript' box

Use of other Java-enabled browsers for the viewing of downloaded Java related code is similarly disallowed.

With respect to the system copy of appletviewer, world execute permissions have also been removed.

If you wish to use Netscape and/or appletviewer to view locally developed code, you may apply to be added to the SGI 'java' group, which has execute permissions for the system copies of the Netscape Java interpreter and appletviewer. To apply for admission to this group, you will need to complete a brief application form.

8. Tampering

Don't try to break passwords, tamper with system files, look into anyone else's directories, or otherwise abuse the trust implicit in your account. Your privileges do not extend beyond the directories, files, and volumes which you rightfully own or to which you have been given permission.

9. Sabbaticals

You may not let your account sit idle for extended periods of time. At the minimum, please log on every two weeks, and do basic user maintenance, particularly, changing your password and checking for suspicious activity.

ARSC enforces this policy by inactivating all accounts after six months without user activity, and disabling them after six more months without user activity.

An inactive account is unchanged except that the owner will not be able to access it. When you try to log onto an inactive account, you will be given a message to contact User Services and will then be logged out. To reactivate your account, contact ARSC User Services (phone: 907-474-5102 or e-mail: consult@arsc.edu). A disabled account is actually removed, and the disk space it occupied is returned to the system.

Appendix B InterNIC Site Security Handbook RFC 1244, FYI 8

Status of this Memo

This handbook is the product of the Site Security Policy Handbook Working Group (SSPHWG), a combined effort of the Security Area and User Services Area of the Internet Engineering Task Force (IETF). This FYI RFC provides information for the Internet community. It does not specify an Internet standard. Distribution of this memo is unlimited.

Contributing Authors

The following are the authors of the Site Security Handbook. Without their dedication, this handbook would not have been possible.

Dave Curry (Purdue University), Sean Kirkpatrick (Unisys), Tom Longstaff (LLNL), Greg Hollingsworth (Johns Hopkins University), Jeffrey Carpenter (University of Pittsburgh), Barbara Fraser (CERT), Fred Ostapik (SRI NISC), Allen Sturtevant (LLNL), Dan Long (BBN), Jim Duncan (Pennsylvania State University), and Frank Byrum (DEC).

Editors' Note

This FYI RFC is a first attempt at providing Internet users guidance on how to deal with security issues in the Internet. As such, this document is necessarily incomplete. There are some clear shortfalls; for example, this document focuses mostly on resources available in the United States. In the spirit of the Internet's "Request for Comments" series of notes, we encourage feedback from users of this handbook. In particular, those who utilize this document to craft their own policies and procedures.

This handbook is meant to be a starting place for further research and should be viewed as a useful resource, but not the final authority. Different organizations and jurisdictions will have different resources and rules. Talk to your local organizations, consult an informed lawyer, or consult with local and national law enforcement. These groups can help fill in the gaps that this document cannot hope to cover.

Finally, we intend for this FYI RFC to grow and evolve. Please send comments and suggestions to: ssphwg@cert.sei.cmu.edu.

1. Introduction

1.1 Purpose of this Work

This handbook is a guide to setting computer security policies and procedures for sites that have systems on the Internet. This guide lists issues and factors that a site must consider when setting their own policies. It makes some recommendations and gives discussions of relevant areas.

This guide is only a framework for setting security policies and procedures. In order to have an effective set of policies and procedures, a site will have to make many decisions, gain agreement, and then communicate and implement the policies.

1.2 Audience

The audience for this work are system administrators and decision makers (who are more traditionally called "administrators" or "middle management") at sites. This document is not directed at programmers or those trying to create secure programs or systems. The focus of this document is on the policies and procedures that need to be in place to support any technical security features that a site may be implementing.

The primary audience for this work are sites that are members of the Internet community. However, this document should be useful to any site that allows communication with other sites. As a general guide to security policies, this document may also be useful to sites with isolated systems.

1.3 Definitions

For the purposes of this guide, a "site" is any organization that owns computers or network-related resources. These resources may include host computers that users use, routers, terminal servers, PC's or other devices that have access to the Internet. A site may be a end user of Internet services or a service provider such as a regional network. However, most of the focus of this guide is on those end users of Internet services. We assume that the site has the ability to set policies and procedures for itself with the concurrence and support from those who actually own the resources.

The "Internet" is those set of networks and machines that use the TCP/IP protocol suite, connected through gateways, and sharing a common name and address spaces [1].

The term "system administrator" is used to cover all those who are responsible for the day-to-day operation of resources. This may be a number of individuals or an organization.

The term "decision maker" refers to those people at a site who set or approve policy. These are often (but not always) the people who own the resources.

1.4 Related Work

The IETF Security Policy Working Group (SPWG) is working on a set of recommended security policy guidelines for the Internet [23]. These guidelines may be adopted as policy by regional networks or owners of other resources. This handbook should be a useful tool to help sites implement those policies as desired or required. However, even implementing the proposed policies isn't enough to secure a site. The proposed Internet policies deal only with network access security. It says nothing about how sites should deal with local security issues.

1.5 Scope

This document covers issues about what a computer security policy should contain, what kinds of procedures are need to enforce security, and some recommendations about how to deal with the problem. When developing a security policy, close attention should be made not only on the security needs and requirements of the local network, but also the security needs and requirements of the other interconnected networks.

This is not a cookbook for computer security. Each site has different needs; the security needs of a corporation might well be different than the security needs of an academic institution. Any security plan has to conform to the needs and culture of the site.

This handbook does not cover details of how to do risk assessment, contingency planning, or physical security. These things are essential in setting and implementing effective security policy, but this document leaves treatment of those issues to other documents. We will try to provide some pointers in that direction.

This document also doesn't talk about how to design or implement secure systems or programs.

1.6 Why Do We Need Security Policies and Procedures?

For most sites, the interest in computer security is proportional to the perception of risk and threats.

The world of computers has changed dramatically over the past twenty-five years. Twenty-five years ago, most computers were centralized and managed by data centers. Computers were kept in locked rooms and staffs of people made sure they were carefully managed and physically secured. Links outside a site were unusual. Computer security threats were rare, and were basically concerned with insiders: authorized users misusing accounts, theft and vandalism, and so forth. These threats were well understood and dealt with using standard techniques: computers behind locked doors, and accounting for all resources.

Computing in the 1990's is radically different. Many systems are in private offices and labs, often managed by individuals or persons employed outside a computer center. Many systems are connected into the Internet, and from there around the world: the United States, Europe, Asia, and Australia are all connected together.

Security threats are different today. The time honored advice says "don't write your password down and put it in your desk" lest someone find it. With world-wide Internet connections, someone could get into your system from the other side of the world and steal your password in the middle of the night when your building is locked up. Viruses and worms can be passed from machine to machine. The Internet allows the electronic equivalent of the thief who looks for open windows and doors; now a person can check hundreds of machines for vulnerabilities in a few hours.

System administrators and decision makers have to understand the security threats that exist, what the risk and cost of a problem would be, and what kind of action they want to take (if any) to prevent and respond to security threats.

As an illustration of some of the issues that need to be dealt with in security problems, consider the following scenarios (thanks to Russell Brand [2, BRAND] for these):

- A system programmer gets a call reporting that a major underground cracker newsletter is being distributed from the administrative machine at his center to five thousand sites in the US and Western Europe.

  Eight weeks later, the authorities call to inform you the information in one of these newsletters was used to disable "911" in a major city for five hours.

- A user calls in to report that he can't login to his account at 3 o'clock in the morning on a Saturday. The system staffer can't login either. After rebooting to single user mode, he finds that password file is empty. By Monday morning, your staff determines that a number of privileged file transfers took place between this machine and a local university.

  Tuesday morning a copy of the deleted password file is found on the university machine along with password files for a dozen other machines.

A week later you find that your system initialization files had been altered in a hostile fashion.

- You receive a call saying that a breakin to a government lab occurred from one of your center's machines. You are requested to provide accounting files to help trackdown the attacker.

  A week later you are given a list of machines at your site that have been broken into.

- A reporter calls up asking about the breakin at your center. You haven't heard of any such breakin.

  Three days later, you learn that there was a breakin. The center director had his wife's name as a password.

- A change in system binaries is detected.

  The day that it is corrected, they again are changed. This repeats itself for some weeks.

- If an intruder is found on your system, should you leave the system open to monitor the situation or should you close down the holes and open them up again later?

- If an intruder is using your site, should you call law enforcement? Who makes that decision? If law enforcement asks you to leave your site open, who makes that decision?

- What steps should be taken if another site calls you and says they see activity coming from an account on your system? What if the account is owned by a local manager?

1.7 Basic Approach

Setting security policies and procedures really means developing a plan for how to deal with computer security. One way to approach this task is suggested by Fites, et. al. [3, FITES]:

- Look at what you are trying to protect.
- Look at what you need to protect it from.
- Determine how likely the threats are.
- Implement measures which will protect your assets in a cost-effective manner.
- Review the process continuously, and improve things every time a weakness is found.

This handbook will concentrate mostly on the last two steps, but the first three are critically important to making effective decisions about security. One old truism in security is that the cost of protecting yourself against a threat should be less than the cost recovering if the threat were to strike you. Without reasonable knowledge of what you are protecting and what the likely threats are, following this rule could be difficult.

1.8 Organization of this Document

This document is organized into seven parts in addition to this introduction.

The basic form of each section is to discuss issues that a site might want to consider in creating a computer security policy and setting procedures to implement that policy. In some cases, possible options are discussed along with the some of the ramifications of those choices. As far as possible, this document tries not to dictate thechoices a site should make, since these depend on localcircumstances. Some of the issues brought up may not apply to all sites. Nonetheless, all sites should at least consider the issues brought up here to ensure that they do not miss some important area.

The overall flow of the document is to discuss policy issues followed by the issues that come up in creating procedures to implement the policies.

Section 2 discusses setting official site policies for access to computing resources. It also goes into the issue of what happens when the policy is violated. The policies will drive the procedures that need to be created, so decision makers will need to make choices about policies before many of the procedural issues in following sections can be dealt with. A key part of creating policies is doing some kind of risk assessment to decide what really needs to be protected and the level of resources that should be applied to protect them.

Once policies are in place, procedures to prevent future security problems should be established. Section 3 defines and suggests actions to take when unauthorized activity is suspected. Resources to prevent secruity breaches are also discussed.

Section 4 discusses types of procedures to prevent security problems. Prevention is a key to security; as an example, the

Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie-Mellon University (CMU) estimates that 80% or more of the problems they see have to do with poorly chosen passwords.

Section 5 discusses incident handling: what kinds of issues does a site face when someone violates the security policy. Many decisions will have to made on the spot as the incident occurs, but many of the options and issues can be discussed in advance. At very least, responsibilities and methods of communication can be established before an incident. Again, the choices here are influenced by the policies discussed in section 2.

Section 6 deals with what happens after a security violation has been dealt with. Security planning is an on-going cycle; just after an incident has occurred is an excellent opportunity to improve policies and procedures.

The rest of the document provides references and an annotated bibliography.

2. Establishing Official Site Policy on Computer Security

2.1 Brief Overview

2.1.1 Organization Issues

The goal in developing an official site policy on computer security is to define the organization's expectations of proper computer and network use and to define procedures to prevent and respond to security incidents. In order to do this, aspects of the particular organization must be considered.

First, the goals and direction of the organization should be considered. For example, a military base may have very different security concerns from a those of a university.

Second, the site security policy developed must conform to existing policies, rules, regulations and laws that the organization is subject to. Therefore it will be necessary to identify these and take them into consideration while developing the policy.

Third, unless the local network is completely isolated and standalone, it is necessary to consider security implications in a more global context. The policy should address the issues when local security problems develop as a result of a remote site as well as when problems occur on remote systems as a result of a local host or user.

2.1.2 Who Makes the Policy?

Policy creation must be a joint effort by technical personnel, who understand the full ramifications of the proposed policy and the implementation of the policy, and by decision makers who have the power to enforce the policy. A policy which is neither implementable nor enforceable is useless.

Since a computer security policy can affect everyone in an organization, it is worth taking some care to make sure you have the right level of authority in on the policy decisions. Though a particular group (such as a campus information services group) may have responsibility for enforcing a policy, an even higher group may have to support and approve the policy.

2.1.3 Who is Involved?

Establishing a site policy has the potential for involving every computer user at the site in a variety of ways. Computer users may be responsible for personal password administration. Systems managers are obligated to fix security holes and to oversee the system.

It is critical to get the right set of people involved at the start of the process. There may already be groups concerned with security who would consider a computer security policy to be their area. Some of the types of groups that might be involved include auditing/control, organizations that deal with physical security, campus information systems groups, and so forth. Asking these types of groups to "buy in" from the start can help facilitate the acceptance of the policy.

2.1.4 Responsibilities

A key element of a computer security policy is making sure everyone knows their own responsibility for maintaining security. A computer security policy cannot anticipate all possibilities; however, it can ensure that each kind of problem does have someone assigned to deal with it.

There may be levels of responsibility associated with a policy on computer security. At one level, each user of a computing resource may have a responsibility to protect his account. A user who allows his account to be compromised increases the chances of compromising other accounts or resources.

System managers may form another responsibility level: they must help to ensure the security of the computer system. Network managers may reside at yet another level.

2.2 Risk Assessment

2.2.1 General Discussion

One of the most important reasons for creating a computer security policy is to ensure that efforts spent on security yield cost effective benefits. Although this may seem obvious, it is possible to be mislead about where the effort is needed. As an example, there is a great deal of publicity about intruders on computers systems; yet most surveys of computer security show that for most organizations, the actual loss from "insiders" is much greater.

Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. Is is the process of examining all of your risks, and ranking those risks by level of severity. This process involves making cost-effective decisions on what you want to protect. The old security adage says that you should not spend more to protect something than it is actually worth.

A full treatment of risk analysis is outside the scope of this document. [3, FITES] and [16, PFLEEGER] provide introductions to this topic. However, there are two elements of a risk analysis that will be briefly covered in the next two sections:

1. Identifying the assets
2. Identifying the threats

For each asset, the basic goals of security are availability, confidentiality, and integrity. Each threat should be examined with an eye to how the threat could affect these areas.

2.2.2 Identifying the Assets

One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious, like all the various pieces of hardware, but some are overlooked, such as the people who actually use the systems. The essential point is to list all things that could be affected by a security problem.

One list of categories is suggested by Pfleeger [16, PFLEEGER, page 459]; this list is adapted from that source:

1. Hardware: cpus, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers.
2. Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.
3. Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
4. People: users, people needed to run systems.
5. Documentation: on programs, hardware, systems, local administrative procedures.
6. Supplies: paper, forms, ribbons, magnetic media.

2.2.3 Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assests. The threats can then be examined to determine what potential for loss exists. It helps to consider from what threats you are trying to protect your assets.

The following sections describe a few of the possible threats.

2.2.3.1 Unauthorized Access

A common threat that concerns many sites is unauthorized access to computing facilities. Unauthorized access takes many forms. One means of unauthorized access is the use of another user's account to gain access to a system. The use of any computer resource without prior permission may be considered unauthorized access to computing facilities.

The seriousness of an unauthorized access will vary from site to site. For some sites, the mere act of granting access to an unauthorized user may cause irreparable harm by negative media coverage. For other sites, an unauthorized access opens the door to other security threats. In addition, some sites may be more frequent targets than others; hence the risk from unauthorized access will vary from site to site. The Computer Emergency Response Team (CERT - see section 3.9.7.3.1) has observed that well-known universities, government sites, and military sites seem to attract more intruders.

2.2.3.2 Disclosure of Information

Another common threat is disclosure of information. Determine the value or sensitivity of the information stored on your computers. Disclosure of a password file might allow for future unauthorized accesses. A glimpse of a proposal may give a competitor an unfair advantage. A technical paper may contain years of valuable research.

2.2.3.3 Denial of Service

Computers and networks provide valuable services to their users. Many people rely on these services in order to perform their jobs efficiently. When these services are not available when called upon, a loss in productivity results.

Denial of service comes in many forms and might affect users in a number of ways. A network may be rendered unusable by a rogue packet, jamming, or by a disabled network component. A virus might slow down or cripple a computer system. Each site should determine which services are essential, and for each of these services determine the affect to the site if that service were to become disabled.

2.3 Policy Issues

There are a number of issues that must be addressed when developing a security policy. These are:

1. Who is allowed to use the resources?
2. What is the proper use of the resources?
3. Who is authorized to grant access and approve usage?
4. Who may have system administration privileges?
5. What are the user's rights and responsibilities?
6. What are the rights and responsibilities of the system administrator vs. those of the user?
7. What do you do with sensitive information?

These issues will be discussed below. In addition you may wish to include a section in your policy concerning ethical use of computing resources. Parker, Swope and Baker [17, PARKER90] and Forester and Morrison [18, FORESTER] are two useful references that address ethical issues.

2.3.1 Who is Allowed to use the Resources?

One step you must take in developing your security policy is defining who is allowed to use your system and services. The policy should explicitly state who is authorized to use what resources.

2.3.2 What is the Proper Use of the Resources?

After determining who is allowed access to system resources it is necessary to provide guidelines for the acceptable use of the resources. You may have different guidelines for different types of users (i.e., students, faculty, external users). The policy should state what is acceptable use as well as unacceptable use. It should also include types of use that may be restricted.

Define limits to access and authority. You will need to consider the level of access various users will have and what resources will be available or restricted to various groups of people.

Your acceptable use policy should clearly state that individual users are responsible for their actions. Their responsibility exists regardless of the security mechanisms that are in place. It should be clearly stated that breaking into accounts or bypassing security is not permitted.

The following points should be covered when developing an acceptable use policy:

- Is breaking into accounts permitted? o Is cracking passwords permitted? o Is disrupting service permitted?
- Should users assume that a file being world-readable grants them the authorization to read it?
- Should users be permitted to modify files that are not their own even if they happen to have write permission?
- Should users share accounts?

The answer to most of these questions will be "no".

You may wish to incorporate a statement in your policies concerning copyrighted and licensed software. Licensing agreements with vendors may require some sort of effort on your part to ensure that the license is not violated. In addition, you may wish to inform users that the copying of copyrighted software may be a violation of the copyright laws, and is not permitted.

Specifically concerning copyrighted and/or licensed software, you may wish to include the following information:

- Copyrighted and licensed software may not be duplicated unless it is explicitly stated that you may do so.
- Methods of conveying information on the copyright/licensed status of software.
- When in doubt, DON'T COPY.

Your acceptable use policy is very important. A policy which does not clearly state what is not permitted may leave you unable to prove that a user violated policy.

There are exception cases like tiger teams and users or administrators wishing for "licenses to hack" — you may face the situation where users will want to "hack" on your services for security research purposes. You should develop a policy that will determine whether you will permit this type of research on your services and if so, what your guidelines for such research will be.

Points you may wish to cover in this area:

- Whether it is permitted at all. o What type of activity is permitted: breaking in, releasing worms, releasing viruses, etc..

- What type of controls must be in place to ensure that it does not get out of control (e.g., separate a segment of your network for these tests).
- How you will protect other users from being victims of these activities, including external users and networks.
- The process for obtaining permission to conduct these tests.

In cases where you do permit these activities, you should isolate the portions of the network that are being tested from your main network. Worms and viruses should never be released on a live network.

You may also wish to employ, contract, or otherwise solicit one or more people or organizations to evaluate the security of your services, of which may include "hacking". You may wish to provide for this in your policy.

2.3.3 Who Is Authorized to Grant Access and Approve Usage?

Your policy should state who is authorized to grant access to your services. Further, it must be determined what type of access they are permitted to give. If you do not have control over who is granted access to your system, you will not have control over who is using your system. Controlling who has the authorization to grant access will also enable you to know who was or was not granting access if problems develop later.

There are many schemes that can be developed to control the distribution of access to your services. The following are the factors that you must consider when determining who will distribute access to your services:

- Will you be distributing access from a centralized point or at various points?

You can have a centralized distribution point to a distributed system where various sites or departments independently authorize access. The trade off is between security and convenience. The more centralized, the easier to secure.

- What methods will you use for creating accounts and terminating access?

From a security standpoint, you need to examine the mechanism that you will be using to create accounts. In the least restrictive case, the people who are authorized to grant access would be able to go into the system directly and create an account by hand or through vendor supplied mechanisms. Generally, these mechanisms place a great deal of trust in the person running them, and the person running them usually has a large amount of privileges. If this is the choice you make, you need to select someone who is trustworthy to perform this task. The opposite solution is to have an integrated system that the people authorized to create accounts run, or the users themselves may actually run. Be aware that even in the restrictive case of having a mechanized facility to create accounts does not remove the potential for abuse.

You should have specific procedures developed for the creation of accounts. These procedures should be well documented to prevent confusion and reduce mistakes. A security vulnerability in the account authorization process is not only possible through abuse, but is also possible if a mistake is made. Having clear and well documented procedure will help ensure that these mistakes won't happen.

You should also be sure that the people who will be following these procedures understand them.

The granting of access to users is one of the most vulnerable of times. You should ensure that the selection of an initial password cannot be easily guessed. You should avoid using an initial password that is a function of the username, is part of the user's name, or some algorithmically generated password that can easily be guessed. In addition, you should not permit users to continue to use the initial password indefinitely. If possible, you should force users to change the initial password the first time they login. Consider that some users may never even login, leaving their password vulnerable indefinitely. Some sites choose to disable accounts that have never been accessed, and force the owner to reauthorize opening the account.

2.3.4 Who May Have System Administration Privileges?

One security decision that needs to be made very carefully is who will have access to system administrator privileges and passwords for your services. Obviously, the system administrators will need access, but inevitably other users will request special privileges. The policy should address this issue. Restricting privileges is one way to deal with threats from local users. The challenge is to balance restricting access to these to protect security with giving people who need these privileges access so that they can perform their tasks. One approach that can be taken is to grant only enough privilege to accomplish the necessary tasks.

Additionally, people holding special privileges should be accountable to some authority and this should also be identified within the site's security policy. If the people you grant privileges to are not accountable, you run the risk of losing control of your system and will have difficulty managing a compromise in security.

2.3.5 What Are The Users' Rights and Responsibilities?

The policy should incorporate a statement on the users' rights and responsibilities concerning the use of the site's computer systems and services. It should be clearly stated that users are responsible for understanding and respecting the security rules of the systems they are using. The following is a list of topics that you may wish to cover in this area of the policy:

- What guidelines you have regarding resource consumption (whether users are restricted, and if so, what the restrictions are).
- What might constitute abuse in terms of system performance.
- Whether users are permitted to share accounts or let others use their accounts.
- How "secret" users should keep their passwords.
- How often users should change their passwords and any other password restrictions or requirements.
- Whether you provide backups or expect the users to create their own.
- Disclosure of information that may be proprietary.
- Statement on Electronic Mail Privacy (Electronic Communications Privacy Act).
- Your policy concerning controversial mail or postings to mailing lists or discussion groups (obscenity, harassment, etc.).
- Policy on electronic communications: mail forging, etc.

The Electronic Mail Association sponsored a white paper on the privacy of electronic mail in companies [4]. Their basic recommendation is that every site should have a policy on the protection of employee privacy. They also recommend that organizations establish privacy policies that deal with all media, rather than singling out electronic mail.

They suggest five criteria for evaluating any policy:

1. Does the policy comply with law and with duties to third parties?
2. Does the policy unnecessarily compromise the interest of the employee, the employer or third parties?
3. Is the policy workable as a practical matter and likely to be enforced?
4. Does the policy deal appropriately with all different forms of communications and record keeping with the office?
5. Has the policy been announced in advance and agreed to by all concerned?

2.3.6 What Are The Rights and Responsibilities of System Administrators Versus Rights of Users

There is a tradeoff between a user's right to absolute privacy and the need of system administrators to gather sufficient information to diagnose problems. There is also a distinction between a system administrator's need to gather information to diagnose problems and investigating security violations. The policy should specify to what degree system administrators can examine user files to diagnose problems or for other purposes, and what rights you grant to the users. You may also wish to make a statement concerning system administrators' obligation to maintaining the privacy of information viewed under these circumstances. A few questions that should be answered are:

- Can an administrator monitor or read a user's files for any reason?
- What are the liabilities?
- Do network administrators have the right to examine network or host traffic?

2.3.7 What To Do With Sensitive Information

Before granting users access to your services, you need to determine at what level you will provide for the security of data on your systems. By determining this, you are determining the level of sensitivity of data that users should store on your systems. You do not want users to store very sensitive information on a system that you are not going to secure very well. You need to tell users who might store sensitive information what services, if any, are appropriate for the storage of sensitive information. This part should include storing of data in different ways (disk, magnetic tape, file servers, etc.). Your policy in this area needs to be coordinated with the policy concerning the rights of system administrators versus users (see section 2.3.6).

2.4 What Happens When the Policy is Violated

It is obvious that when any type of official policy is defined, be it related to computer security or not, it will eventually be broken. The violation may occur due to an individual's negligence, accidental mistake, having not been properly informed of the current policy, or not understanding the current policy. It is equally possible that an individual (or group of individuals) may knowingly perform an act that is in direct violation of the defined policy.

When a policy violation has been detected, the immediate course of action should be pre-defined to ensure prompt and proper enforcement. An investigation should be performed to determine how and why the violation occurred. Then the appropriate corrective action should be executed. The type and severity of action taken varies depending on the type of violation that occurred.

2.4.1 Determining the Response to Policy Violations

Violations to policy may be committed by a wide variety of users. Some may be local users and others may be from outside the local environment. Sites may find it helpful to define what it considers "insiders" and "outsiders" based upon administrative, legal or political boundaries. These boundaries imply what type of action must be taken to correct the offending party; from a written reprimand to pressing legal charges. So, not only do you need to define actions based on the type of violation, you also need to have a clearly defined series of actions based on the kind of user violating your computer security policy. This all seems rather complicated, but should be addressed long before it becomes necessary as the result of a violation.

One point to remember about your policy is that proper education is your best defense. For the outsiders who are using your computer legally, it is your responsibility to verify that these individuals are aware of the policies that you have set forth. Having this proof may assist you in the future if legal action becomes necessary.

As for users who are using your computer illegally, the problem is basically the same. What type of user violated the policy and how and why did they do it? Depending on the results of your investigation, you may just prefer to "plug" the hole in your computer security and chalk it up to experience. Or if a significant amount of loss was incurred, you may wish to take more drastic action.

2.4.2 What to do When Local Users Violate the Policy of a Remote Site

In the event that a local user violates the security policy of a remote site, the local site should have a clearly defined set of administrative actions to take concerning that local user. The site should also be prepared to protect itself against possible actions by the remote site. These situations involve legal issues which should be addressed when forming the security policy.

2.4.3 Defining Contacts and Responsibilities to Outside Organizations

The local security policy should include procedures for interaction with outside organizations. These include law enforcement agencies, other sites, external response team organizations (e.g., the CERT, CIAC) and various press agencies. The procedure should state who is authorized to make such contact and how it should be handled. Some questions to be answered include:

- Who may talk to the press?
- When do you contact law enforcement and investigative agencies?
- If a connection is made from a remote site, is the system manager authorized to contact that site?
- Can data be released? What kind?

Detailed contact information should be readily available along with clearly defined procedures to follow.

2.4.4 What are the Responsibilities to our Neighbors and Other Internet Sites?

The Security Policy Working Group within the IETF is working on a document entitled, "Policy Guidelines for the

Secure Operation of the Internet" [23]. It addresses the issue that the Internet is a cooperative venture and that sites are expected to provide mutual security assistance. This should be addressed when developing a site's policy. The major issue to be determined is how much information should be released. This will vary from site to site according to the type of site (e.g., military, education, commercial) as well as the type of security violation that occurred.

2.4.5 Issues for Incident Handling Procedures

Along with statements of policy, the document being prepared should include procedures for incident handling. This is covered in detail in the next chapter. There should be procedures available that cover all facets of policy violation.

2.5 Locking In or Out

Whenever a site suffers an incident which may compromise computer security, the strategies for reacting may be influenced by two opposing pressures.

If management fears that the site is sufficiently vulnerable, it may choose a "Protect and Proceed" strategy. This approach will have as its primary goal the protection and preservation of the site facilities and to provide for normalcy for its users as quickly as possible. Attempts will be made to actively interfere with the intruder's processes, prevent further access and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruder is identified directly, they may come back into the site via a different path, or may attack another site.

The alternate approach, "Pursue and Prosecute", adopts the opposite philosophy and goals. The primary goal is to allow intruders to continue their activities at the site until the site can identify the responsible persons. This approach is endorsed by law enforcement agencies and prosecutors. The drawback is that the agencies cannot exempt a site from possible user lawsuits if damage is done to their systems and data.

Prosecution is not the only outcome possible if the intruder is identified. If the culprit is an employee or a student, the organization may choose to take disciplinary actions. The computer security policy needs to spell out the choices and how they will be selected if an intruder is caught.

Careful consideration must be made by site management regarding their approach to this issue before the problem occurs. The strategy adopted might depend upon each circumstance. Or there may be a global policy which mandates one approach in all circumstances. The pros and cons must be examined thoroughly and the users of the facilities must be made aware of the policy so that they understand their vulnerabilities no matter which approach is taken.

The following are checklists to help a site determine which strategy to adopt: "Protect and Proceed" or "Pursue and Prosecute".

Protect and Proceed

1. If assets are not well protected.
2. If continued penetration could result in great financial risk.

3. If the possibility or willingness to prosecute is not present.
4. If user base is unknown.
5. If users are unsophisticated and their work is vulnerable.
6. If the site is vulnerable to lawsuits from users, e.g., if their resources are undermined.

Pursue and Prosecute

1. If assets and systems are well protected.
2. If good backups are available.
3. If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.
4. If this is a concentrated attack occurring with great frequency and intensity.
5. If the site has a natural attraction to intruders, and consequently regularly attracts intruders.
6. If the site is willing to incur the financial (or other) risk to assets by allowing the penetrator continue.
7. If intruder access can be controlled.
8. If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.
9. If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.
10. If there is willingness on the part of management to prosecute.
11. If the system adminitrators know in general what kind of evidence would lead to prosecution.
12. If there is established contact with knowledgeable law enforcement.

13. If there is a site representative versed in the relevant legal issues.
14. If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit.

2.6 Interpreting the Policy

It is important to define who will interpret the policy. This could be an individual or a committee. No matter how well written, the policy will require interpretation from time to time and this body would serve to review, interpret, and revise the policy as needed.

2.7 Publicizing the Policy

Once the site security policy has been written and established, a vigorous process should be engaged to ensure that the policy statement is widely and thoroughly disseminated and discussed. A mailing of the policy should not be considered sufficient. A period for comments should be allowed before the policy becomes effective to ensure that all affected users have a chance to state their reactions and discuss any unforeseen ramifications. Ideally, the policy should strike a balance between protection and productivity.

Meetings should be held to elicit these comments, and also to ensure that the policy is correctly understood. (Policy promulgators are not necessarily noted for their skill with the language.) These meetings should involve higher management as well as line employees. Security is a collective effort.

In addition to the initial efforts to publicize the policy, it is essential for the site to maintain a continual awareness of its computer security policy. Current users may need periodic reminders New users should have the policy included as part of their site introduction packet. As a condition for using the site facilities, it may be advisable to have them sign a statement that they have read and understood the policy. Should any of these users require legal action for serious policy violations, this signed statement might prove to be a valuable aid.

3. Establishing Procedures to Prevent Security Problems

The security policy defines what needs to be protected. This section discusses security procedures which specify what steps will be used to carry out the security policy.

3.1 Security Policy Defines What Needs to be Protected

The security policy defines the WHAT's: what needs to be protected, what is most important, what the priorities are, and what the general approach to dealing with security problems should be.

The security policy by itself doesn't say HOW things are protected. That is the role of security procedures, which this section discusses. The security policy should be a high level document, giving general strategy. The security procedures need to set out, in detail, the precise steps your site will take to protect itself.

The security policy should include a general risk assessment of the types of threats a site is mostly likely to face and the consequences of those threats (see section 2.2). Part of doing a risk assessment will include creating a general list of assets that should be protected (section 2.2.2). This information is critical in devising cost-effective procedures.

It is often tempting to start creating security procedures by deciding on different mechanisms first: "our site should have logging on all hosts, call-back modems, and smart cards for all users." This approach could lead to some areas that have too much protection for the risk they face, and other areas that aren't protected enough. Starting with the security policy and the risks it outlines should ensure that the procedures provide the right level of protect for all assets.

3.2 Identifing Possible Problems

To determine risk, vulnerabilities must be identified. Part of the purpose of the policy is to aid in shoring up the vulnerabilities and thus to decrease the risk in as many areas as possible. Several of the more popular problem areas are presented in sections below. This list is by no means complete. In addition, each site is likely to have a few unique vulnerabilities.

3.2.1 Access Points

Access points are typically used for entry by unauthorized users. Having many access points increases the risk of access to an organization's computer and network facilities.

Network links to networks outside the organization allow access into the organization for all others connected to that external network. A network link typically provides access to a large number of network services, and each service has a potential to be compromised.

Dialup lines, depending on their configuration, may provide access merely to a login port of a single system. If connected to a terminal server, the dialup line may give access to the entire network.

Terminal servers themselves can be a source of problem. Many terminal servers do not require any kind of authentication. Intruders often use terminal servers to disguise their actions, dialing in on a local phone and then using the terminal server to go out to the local network. Some terminal servers are configured so that intruders can TELNET [19] in from outside the network, and then TELNET back out again, again serving to make it difficult to trace them.

3.2.2 Misconfigured Systems

Misconfigured systems form a large percentage of security holes. Today's operating systems and their associated software have become so complex that understanding how the system works has become a full-time job. Often, systems managers will be non- specialists chosen from the current organization's staff.

Vendors are also partly responsible for misconfigured systems. To make the system installation process easier, vendors occasionally choose initial configurations that are not secure in all environments.

3.2.3 Software Bugs

Software will never be bug free. Publicly known security bugs are common methods of unauthorized entry. Part of the solution to this problem is to be aware of the security problems and to update the software when problems are detected. When bugs are found, they should be reported to the vendor so that a solution to the problem can be implemented and distributed.

3.2.4 "Insider" Threats

An insider to the organization may be a considerable threat to the security of the computer systems. Insiders often have direct access to the computer and network hardware components. The ability to access the components of a system makes most systems easier to compromise. Most desktop workstations can be easily manipulated so that they grant privileged access. Access to a local area network provides the ability to view possibly sensitive data traversing the network.

3.3 Choose Controls to Protect Assets in a Cost-Effective Way

After establishing what is to be protected, and assessing the risks these assets face, it is necessary to decide how to implement the controls which protect these assets. The controls and protection mechanisms should be selected in a way so as to adequately counter the threats found during risk assessment, and to implement those controls in a cost effective manner. It makes little sense to spend an exorbitant sum of money and overly constrict the user base if the risk of exposure is very small.

3.3.1 Choose the Right Set of Controls

The controls that are selected represent the physical embodiment of your security policy. They are the first and primary line of defense in the protection of your assets. It is therefore most important to ensure that the controls that you select are the right set of controls. If the major threat to your system is outside penetrators, it probably doesn't make much sense to use biometric devices to authenticate your regular system users. On the other hand, if the major threat is unauthorized use of computing resources by regular system users, you'll probably want to establish very rigorous automated accounting procedures.

3.3.2 Use Common Sense

Common sense is the most appropriate tool that can be used to establish your security policy. Elaborate security schemes and mechanisms are impressive, and they do have their place, yet there is little point in investing money and time on an elaborate implementation scheme if the simple controls are forgotten. For example, no matter how elaborate a system you put into place on top of existing security controls, a single user with a poor password can still leave your system open to attack.

3.4 Use Multiple Strategies to Protect Assets

Another method of protecting assets is to use multiple strategies. In this way, if one strategy fails or is circumvented, another strategy comes into play to continue protecting the asset. By using several simpler strategies, a system can often be made more secure than if one very sophisticated method were used in its place. For example, dial-back modems can be used in conjunction with traditional logon mechanisms. Many similar approaches could be devised that provide several levels of protection for assets. However, it's very easy to go overboard with extra mechanisms. One must keep in mind exactly what it is that needs to be protected.

3.5 Physical Security

It is a given in computer security if the system itself is not physically secure, nothing else about the system can be considered secure. With physical access to a machine, an intruder can halt the machine, bring it back up in privileged mode, replace or alter the disk, plant Trojan horse programs (see section 2.13.9.2), or take any number of other undesirable (and hard to prevent) actions.

Critical communications links, important servers, and other key machines should be located in physically secure areas. Some security systems (such as Kerberos) require that the machine be physically secure.

If you cannot physically secure machines, care should be taken about trusting those machines. Sites should consider limiting access from non-secure machines to more secure machines. In particular, allowing trusted access (e.g., the BSD Unix remote commands such as rsh) from these kinds of hosts is particularly risky.

For machines that seem or are intended to be physically secure, care should be taken about who has access to the machines. Remember that custodial and maintenance staff often have keys to rooms.

3.6 Procedures to Recognize Unauthorized Activity

Several simple procedures can be used to detect most unauthorized uses of a computer system. These procedures use tools provided with the operating system by the vendor, or tools publicly available from other sources.

3.6.1 Monitoring System Use

System monitoring can be done either by a system administrator, or by software written for the purpose. Monitoring a system involves looking at several parts of the system and searching for anything unusual. Some of the easier ways to do this are described in this section.

The most important thing about monitoring system use is that it be done on a regular basis. Picking one day out of the month to monitor the system is pointless, since a security breach can be isolated to a matter of hours. Only by maintaining a constant vigil can you expect to detect security violations in time to react to them.

3.6.2 Tools for Monitoring the System

This section describes tools and methods for monitoring a system against unauthorized access and use.

3.6.2.1 Logging

Most operating systems store numerous bits of information in log files. Examination of these log files on a regular basis is often the first line of defense in detecting unauthorized use of the system.

- Compare lists of currently logged in users and past login histories. Most users typically log in and out at roughly the same time each day. An account logged in outside the "normal" time for the account may be in use by an intruder.

- Many systems maintain accounting records for billing purposes. These records can also be used to determine usage patterns for the system; unusual accounting records may indicate unauthorized use of the system.

- System logging facilities, such as the UNIX "syslog" utility, should be checked for unusual error messages from system software. For example, a large number of failed login attempts in a short period of time may indicate someone trying to guess passwords.

- Operating system commands which list currently executing processes can be used to detect users running programs they are not authorized to use, as well as to detect unauthorized programs which have been started by an intruder.

3.6.2.2 Monitoring Software

Other monitoring tools can easily be constructed using standard operating system software, by using several, often unrelated, programs together. For example, checklists of file ownerships and permission settings can be constructed (for example, with "ls" and "find" on UNIX) and stored off-line. These lists can then be reconstructed periodically and compared against the master checklist (on UNIX, by using the "diff" utility). Differences may indicate that unauthorized modifications have been made to the system.

Still other tools are available from third-party vendors and public software distribution sites. Section 3.9.9 lists several sources from which you can learn what tools are available and how to get them.

3.6.2.3 Other Tools

Other tools can also be used to monitor systems for security violations, although this is not their primary purpose. For example, network monitors can be used to detect and log connections from unknown sites.

3.6.3 Vary the Monitoring Schedule

The task of system monitoring is not as daunting as it may seem. System administrators can execute many of the commands used for monitoring periodically throughout the day during idle moments (e.g., while talking on the telephone), rather than spending fixed periods of each day monitoring the system. By executing the commands frequently, you will rapidly become used to seeing "normal" output, and will easily spot things which are out of the ordinary. In addition, by running various monitoring commands at different times throughout the day, you make it hard for an intruder to predict your actions. For example, if an intruder knows that each day at 5:00 p.m. the system is checked to see that everyone has logged off, he will simply wait until after the check has completed before logging in. But the intruder cannot guess when a system administrator might type a command to display all logged-in users, and thus he runs a much greater risk of detection.

Despite the advantages that regular system monitoring provides, some intruders will be aware of the standard logging mechanisms in use on systems they are attacking. They will actively pursue and attempt to disable monitoring mechanisms. Regular monitoring therefore is useful in detecting intruders, but does not provide any guarantee that your system is secure, nor should monitoring be considered an infallible method of detecting unauthorized use.

3.7 Define Actions to Take When Unauthorized Activity is Suspected

Sections 2.4 and 2.5 discussed the course of action a site should take when it suspects its systems are being abused. The computer security policy should state the general approach towards dealing with these problems.

The procedures for dealing with these types of problems should be written down. Who has authority to decide what actions will be taken? Should law enforcement be involved? Should your organization cooperate with other sites in trying to track down an intruder? Answers to all the questions in section 2.4 should be part of the incident handling procedures.

Whether you decide to lock out or pursue intruders, you should have tools and procedures ready to apply. It is best to work up these tools and procedures before you need them. Don't wait until an intruder is on your system to figure out how to track the intruder's actions; you will be busy enough if an intruder strikes.

3.8 Communicating Security Policy

Security policies, in order to be effective, must be communicated to both the users of the system and the system maintainers. This section describes what these people should be told, and how to tell them.

3.8.1 Educating the Users

Users should be made aware of how the computer systems are expected to be used, and how to protect themselves from unauthorized users.

3.8.1.1 Proper Account/Workstation Use

All users should be informed about what is considered the "proper" use of their account or workstation ("proper" use is discussed in section 2.3.2). This can most easily be done at the time a user receives their account, by giving them a policy statement. Proper use policies typically dictate things such as whether or not the account or workstation may be used for personal activities (such as checkbook balancing or letter writing), whether profit-making activities are allowed, whether game playing is permitted, and so on. These policy statements may also be used to summarize how the computer facility is licensed and what software licenses are held by the institution; for example, many universities have educational licenses which explicitly prohibit commercial uses of the system. A more complete list of items to consider when writing a policy statement is given in section 2.3.

3.8.1.2 Account/Workstation Management Procedures

Each user should be told how to properly manage their account and workstation. This includes explaining how to protect files stored on the system, how to log out or lock the terminal or workstation, and so on. Much of this information is typically covered in the "beginning user" documentation provided by the operating system vendor, although many sites elect to supplement this material with local information.

If your site offers dial-up modem access to the computer systems, special care must be taken to inform users of the security problems inherent in providing this access. Issues such as making sure to log out before hanging up the modem should be covered when the user is initially given dial-up access.

Likewise, access to the systems via local and wide-area networks presents its own set of security problems which users should be made aware of. Files which grant "trusted host" or "trusted user" status to remote systems and users should be carefully explained.

3.8.1.3 Determining Account Misuse

Users should be told how to detect unauthorized access to their account. If the system prints the last login time when a user logs in, he or she should be told to check that time and note whether or not it agrees with the last time he or she actually logged in.

Command interpreters on some systems (e.g., the UNIX C shell) maintain histories of the last several commands executed. Users should check these histories to be sure someone has not executed other commands with their account.

3.8.1.4 Problem Reporting Procedures

A procedure should be developed to enable users to report suspected misuse of their accounts or other misuse they may have noticed. This can be done either by providing the name and telephone number of a system administrator who manages security of the computer system, or by creating an electronic mail address (e.g., "security") to which users can address their problems.

3.8.2 Educating the Host Administrators

In many organizations, computer systems are administered by a wide variety of people. These administrators must know how to protect their own systems from attack and unauthorized use, as well as how to communicate successful penetration of their systems to other administrators as a warning.

3.8.2.1 Account Management Procedures

Care must be taken when installing accounts on the system in order to make them secure. When installing a system from distribution media, the password file should be examined for "standard" accounts provided by the vendor. Many vendors provide accounts for use by system services or field service personnel. These accounts typically have either no password or one which is common knowledge. These accounts should be given new passwords if they are needed, or disabled or deleted from the system if they are not.

Accounts without passwords are generally very dangerous since they allow anyone to access the system. Even accounts which do not execute a command interpreter (e.g., accounts which exist only to see who is logged in to the system) can be compromised if set up incorrectly. A related concept, that of "anonymous" file transfer (FTP) [20], allows users from all over the network to access your system to retrieve files from (usually) a protected disk area. You should carefully weigh the benefits that an account without a password provides against the security risks of providing such access to your system.

If the operating system provides a "shadow" password facility which stores passwords in a separate file accessible only to privileged users, this facility should be used. System V UNIX, SunOS 4.0 and above, and versions of Berkeley UNIX after 4.3BSD Tahoe, as well as others, provide this feature. It protects passwords by hiding their encrypted values from unprivileged users. This prevents an attacker from copying your password file to his or her machine and then attempting to break the passwords at his or her leisure.

Keep track of who has access to privileged user accounts (e.g., "root" on UNIX or "MAINT" on VMS). Whenever a privileged user leaves the organization or no longer has need of the privileged account, the passwords on all privileged accounts should be changed.

3.8.2.2 Configuration Management Procedures

When installing a system from the distribution media or when installing third-party software, it is important to check the installation carefully. Many installation procedures assume a "trusted" site, and hence will install files with world write permission enabled, or otherwise compromise the security of files.

Network services should also be examined carefully when first installed. Many vendors provide default network permission files which imply that all outside hosts are to be "trusted", which is rarely the case when connected to wide-area networks such as the Internet.

Many intruders collect information on the vulnerabilities of particular system versions. The older a system, the more likely it is that there are security problems in that version which have since been fixed by the vendor in a later release. For this reason, it is important to weigh the risks of not upgrading to a new operating system release (thus leaving security holes unplugged) against the cost of upgrading to the new software (possibly breaking third-party software, etc.). Bug fixes from the vendor should be weighed in a similar fashion, with the added note that "security" fixes from a vendor usually address fairly serious security problems.

Other bug fixes, received via network mailing lists and the like, should usually be installed, but not without careful examination. Never install a bug fix unless you're sure you know what the consequences of the fix are - there's always the possibility that an intruder has suggested a "fix" which actually gives him or her access to your system.

3.8.2.3 Recovery Procedures - Backups

It is impossible to overemphasize the need for a good backup strategy. File system backups not only protect you in the event of hardware failure or accidental deletions, but they also protect you against unauthorized changes made by an intruder. Without a copy of your data the way it's "supposed" to be, it can be difficult to undo something an attacker has done.

Backups, especially if run daily, can also be useful in providing a history of an intruder's activities. Looking through old backups can establish when your system was first penetrated. Intruders may leave files around which, although deleted later, are captured on the backup tapes. Backups can also be used to document an intruder's activities to law enforcement agencies if necessary.

A good backup strategy will dump the entire system to tape at least once a month. Partial (or "incremental") dumps should be done at least twice a week, and ideally they should be done daily. Commands specifically designed for performing file system backups (e.g., UNIX "dump" or VMS "BACKUP") should be used in preference to other file copying commands, since these tools are designed with the express intent of restoring a system to a known state.

3.8.2.4 Problem Reporting Procedures

As with users, system administrators should have a defined procedure for reporting security problems. In large installations, this is often done by creating an electronic mail alias which contains the names of all system administrators in the organization. Other methods include setting up some sort of response team similar to the CERT, or establishing a "hotline" serviced by an existing support group.

3.9 Resources to Prevent Security Breaches

This section discusses software, hardware, and procedural resources that can be used to support your site security policy.

3.9.1 Network Connections and Firewalls

A "firewall" is put in place in a building to provide a point of resistance to the entry of flames into another area. Similarly, a secretary's desk and reception area provides a point of controlling access to other office spaces. This same technique can be applied to a computer site, particularly as it pertains to network connections.

Some sites will be connected only to other sites within the same organization and will not have the ability to connect to other networks. Sites such as these are less susceptible to threats from outside their own organization, although intrusions may still occur via paths such as dial-up modems. On the other hand, many other organizations will be connected to other sites via much larger networks, such as the Internet. These sites are susceptible to the entire range of threats associated with a networked environment.

The risks of connecting to outside networks must be weighed against the benefits. It may be desirable to limit connection to outside networks to those hosts which do not store sensitive material, keeping "vital" machines (such as those which maintain company payroll or inventory systems) isolated. If there is a need to participate in a Wide Area Network (WAN), consider restricting all access to your local network through a single system. That is, all access to or from your own local network must be made through a single host computer that acts as a firewall between you and the outside world. This firewall system should be rigorously controlled and password protected, and external users accessing it should also be constrained by restricting the functionality available to remote users. By using this approach, your site could relax some of the internal security controls on your local net, but still be afforded the protection of a rigorously controlled host front end.

Note that even with a firewall system, compromise of the firewall could result in compromise of the network behind the firewall. Work has been done in some areas to construct a firewall which even when compromised, still protects the local network [6, CHESWICK].

3.9.2 Confidentiality

Confidentiality, the act of keeping things hidden or secret, is one of the primary goals of computer security practitioners. Several mechanisms are provided by most modern operating systems to enable users to control the dissemination of information. Depending upon where you work, you may have a site where everything is protected, or a site where all information is usually regarded as public, or something in-between. Most sites lean toward the in-between, at least until some penetration has occurred.

Generally, there are three instances in which information is vulnerable to disclosure: when the information is stored on a computer system, when the information is in transit to another system (on the network), and when the information is stored on backup tapes.

The first of these cases is controlled by file permissions, access control lists, and other similar mechanisms. The last can be controlled by restricting access to the backup tapes (by locking them in a safe, for example). All three cases can be helped by using encryption mechanisms.

3.9.2.1 Encryption (hardware and software)

Encryption is the process of taking information that exists in some readable form and converting it into a non-readable form. There are several types of commercially available encryption packages in both hardware and software forms. Hardware encryption engines have the advantage that they are much faster than the software equivalent, yet because they are faster, they are of greater potential benefit to an attacker who wants to execute a brute-force attack on your encrypted information.

The advantage of using encryption is that, even if other access control mechanisms (passwords, file permissions, etc.) are compromised by an intruder, the data is still unusable. Naturally, encryption keys and the like should be protected at least as well as account passwords.

Information in transit (over a network) may be vulnerable to interception as well. Several solutions to this exist, ranging from simply encrypting files before transferring them (end-to-end encryption) to special network hardware which encrypts everything it sends without user intervention (secure links). The Internet as a whole does not use secure links, thus end-to-end encryption must be used if encryption is desired across the Internet.

3.9.2.1.1 Data Encryption Standard (DES)

DES is perhaps the most widely used data encryption mechanism today. Many hardware and software implementations exist, and some commercial computers are provided with a software version. DES transforms plain text information into encrypted data (or ciphertext) by means of a special algorithm and "seed" value called a key. So long as the key is retained (or remembered) by the original user, the ciphertext can be restored to the original plain text.

One of the pitfalls of all encryption systems is the need to remember the key under which a thing was encrypted (this is not unlike the password problem discussed elsewhere in this document). If the key is written down, it becomes less secure. If forgotten, there is little (if any) hope of recovering the original data.

Most UNIX systems provide a DES command that enables a user to encrypt data using the DES algorithm.

3.9.2.1.2 Crypt

Similar to the DES command, the UNIX "crypt" command allows a user to encrypt data. Unfortunately, the algorithm used by "crypt" is very insecure (based on the World War II "Enigma" device), and files encrypted with this command can be decrypted easily in a matter of a few hours. Generally, use of the "crypt" command should be avoided for any but the most trivial encryption tasks.

3.9.2.2 Privacy Enhanced Mail

Electronic mail normally transits the network in the clear (i.e., anyone can read it). This is obviously not the optimal solution. Privacy enhanced mail provides a means to automatically encrypt electronic mail messages so that a person eavesdropping at a mail distribution node is not (easily) capable of reading them. Several privacy enhanced mail packages are currently being developed and deployed on the Internet.

The Internet Activities Board Privacy Task Force has defined a draft standard, elective protocol for use in implementing privacy enhanced mail. This protocol is defined in RFCs 1113, 1114, and 1115 [7,8,9]. Please refer to the current edition of the "IAB Official Protocol Standards" (currently, RFC 1200 [21]) for the standardization state and status of these protocols.

3.9.3 Origin Authentication

We mostly take it on faith that the header of an electronic mail message truly indicates the originator of a message. However, it iseasy to "spoof", or forge the source of a mail message. Origin authentication provides a means to be certain of the originator of a message or other object in the same way that a Notary Public assures a signature on a legal document. This is done by means of a "Public Key" cryptosystem.

A public key cryptosystem differs from a private key cryptosystem in several ways. First, a public key system uses two keys, a Public Key that anyone can use (hence the name) and a Private Key that only the originator of a message uses. The originator uses the private key to encrypt the message (as in DES). The receiver, who has obtained the public key for the originator, may then decrypt the message.

In this scheme, the public key is used to authenticate the originator's use of his or her private key, and hence the identity of the originator is more rigorously proven. The most widely known implementation of a public key cryptosystem is the RSA system [26]. The Internet standard for privacy enhanced mail makes use of the RSA system.

3.9.4 Information Integrity

Information integrity refers to the state of information such that it is complete, correct, and unchanged from the last time in which it was verified to be in an "integral" state. The value of information integrity to a site will vary. For example, it is more important for military and government installations to prevent the "disclosure" of classified information, whether it is right or wrong. A bank, on the other hand, is far more concerned with whether the account information maintained for its customers is complete and accurate.

Numerous computer system mechanisms, as well as procedural controls, have an influence on the integrity of system information. Traditional access control mechanisms maintain controls over who can access system information. These mechanisms alone are not sufficient in some cases to provide the degree of integrity required. Some other mechanisms are briefly discussed below.

It should be noted that there are other aspects to maintaining system integrity besides these mechanisms, such as two-person controls, and integrity validation procedures. These are beyond the scope of this document.

3.9.4.1 Checksums

Easily the simplest mechanism, a simple checksum routine can compute a value for a system file and compare it with the last known value. If the two are equal, the file is probably unchanged. If not, the file has been changed by some unknown means.

Though it is the easiest to implement, the checksum scheme suffers from a serious failing in that it is not very sophisticated and a determined attacker could easily add enough characters to the file to eventually obtain the correct value.

A specific type of checksum, called a CRC checksum, is considerably more robust than a simple checksum. It is only slightly more difficult to implement and provides a better degree of catching errors. It too, however, suffers from the possibility of compromise by an attacker.

Checksums may be used to detect the altering of information. However, they do not actively guard against changes being made. For this, other mechanisms such as access controls and encryption should be used.

3.9.4.2 Cryptographic Checksums

Cryptographic checksums (also called cryptosealing) involve breaking a file up into smaller chunks, calculating a (CRC) checksum for each chunk, and adding the CRCs together. Depending upon the exact algorithm used, this can result in a nearly unbreakable method of determining whether a file has been changed. This mechanism suffers from the fact that it is sometimes computationally intensive and may be prohibitive except in cases where the utmost integrity protection is desired.

Another related mechanism, called a one-way hash function (or a Manipulation Detection Code (MDC)) can also be used to uniquely identify a file. The idea behind these functions is that no two inputs can produce the same output, thus a modified file will not have the same hash value. One-way hash functions can be implemented efficiently on a wide variety of systems, making unbreakable integrity checks possible. (Snefru, a one-way hash function available via USENET as well as the Internet is just one example of an efficient one-way hash function.) [10]

3.9.5 Limiting Network Access

The dominant network protocols in use on the Internet, IP (RFC 791) [11], TCP (RFC 793) [12], and UDP (RFC 768) [13], carry certain control information which can be used to restrict access to certain hosts or networks within an organization.

The IP packet header contains the network addresses of both the sender and recipient of the packet. Further, the TCP and UDP protocols provide the notion of a "port", which identifies the endpoint (usually a network server) of a communications path. In some instances, it may be desirable to deny access to a specific TCP or UDP port, or even to certain hosts and networks altogether.

3.9.5.1 Gateway Routing Tables

One of the simplest approaches to preventing unwanted network connections is to simply remove certain networks from a gateway's routing tables. This makes it "impossible" for a host to send packets to these networks. (Most protocols require bidirectional packet flow even for unidirectional data flow, thus breaking one side of the route is usually sufficient.)

This approach is commonly taken in "firewall" systems by preventing the firewall from advertising local routes to the outside world. The approach is deficient in that it often prevents "too much" (e.g., in order to prevent access to one system on the network, access to all systems on the network is disabled).

3.9.5.2 Router Packet Filtering

Many commercially available gateway systems (more correctly called routers) provide the ability to filter packets based not only on sources or destinations, but also on source-destination combinations. This mechanism can be used to deny access to a specific host, network, or subnet from any other host, network, or subnet.

Gateway systems from some vendors (e.g., cisco Systems) support an even more complex scheme, allowing finer control over source and destination addresses. Via the use of address masks, one can deny access to all but one host on a particular network. The cisco Systems also allow packet screening based on IP protocol type and TCP or UDP port numbers [14].

This can also be circumvented by "source routing" packets destined for the "secret" network. Source routed packets may be filtered out by gateways, but this may restrict other legitimate activities, such as diagnosing routing problems.

3.9.6 Authentication Systems

Authentication refers to the process of proving a claimed identity to the satisfaction of some permission-granting authority. Authentication systems are hardware, software, or procedural mechanisms that enable a user to obtain access to computing resources. At the simplest level, the system administrator who adds new user accounts to the system is part of the system authentication mechanism. At the other end of the spectrum, fingerprint readers or retinal scanners provide a very high-tech solution to establishing a potential user's identity. Without establishing and proving a user's identity prior to establishing a session, your site's computers are vulnerable to any sort of attack.

Typically, a user authenticates himself or herself to the system by entering a password in response to a prompt. Challenge/Response mechanisms improve upon passwords by prompting the user for some piece of information shared by both the computer and the user (such as mother's maiden name, etc.).

3.9.6.1 Kerberos

Kerberos, named after the dog who in mythology is said to stand at the gates of Hades, is a collection of software used in a large network to establish a user's claimed identity. Developed at the Massachusetts Institute of Technology (MIT), it uses a combination of encryption and distributed databases so that a user at a campus facility can login and start a session from any computer located on the campus. This has clear advantages in certain environments where there are a large number of potential users who may establish a connection from any one of a large number of workstations. Some vendors are now incorporating Kerberos into their systems.

It should be noted that while Kerberos makes several advances in the area of authentication, some security weaknesses in the protocol still remain [15].

3.9.6.2 Smart Cards

Several systems use "smart cards" (a small calculator-like device) to help authenticate users. These systems depend on the user having an object in their possession. One such system involves a new password procedure that require a user to enter a value obtained from a "smart card" when asked for a password by the computer. Typically, the host machine will give the user some piece of information that is entered into the keyboard of the smart card. The smart card will display a response which must then be entered into the computer before the session will be established. Another such system involves a smart card which displays a number which changes over time, but which is synchronized with the authentication software on the computer.

This is a better way of dealing with authentication than with the traditional password approach. On the other hand, some say it's inconvenient to carry the smart card. Start-up costs are likely to be high as well.

3.9.7 Books, Lists, and Informational Sources

There are many good sources for information regarding computer security. The annotated bibliography at the end of this document can provide you with a good start. In addition, information can be obtained from a variety of other sources, some of which are described in this section.

3.9.7.1 Security Mailing Lists

The UNIX Security mailing list exists to notify system administrators of security problems before they become common knowledge, and to provide security enhancement information. It is a restricted-access list, open only to people who can be verified as being principal systems people at a site. Requests to join the list must be sent by either the site contact listed in the Defense Data Network's Network Information Center's (DDN NIC) WHOIS database, or from the "root" account on one of the major site machines. You must include the destination address you want on the list, an indication of whether you want to be on the mail reflector list or receive weekly digests, the electronic mail address and voice telephone number of the site contact if it isn't you, and the name, address, and telephone number of your organization. This information should be sent to SECURITY-REQUEST@CPD.COM.

The RISKS digest is a component of the ACM Committee on Computers and Public Policy, moderated by Peter G. Neumann. It is a discussion forum on risks to the public in computers and related systems, and along with discussing computer security and privacy issues, has discussed such subjects as the Stark incident, the shooting down of the Iranian airliner in the Persian Gulf (as it relates to the computerized weapons systems), problems in air and railroad traffic control systems, software engineering, and so on. To join the mailing list, send a message to RISKS-REQUEST@CSL.SRI.COM. This list is also available in the USENET newsgroup "comp.risks".

The VIRUS-L list is a forum for the discussion of computer virus experiences, protection software, and related topics. The list is open to the public, and is implemented as a moderated digest. Most of the information is related to personal computers, although some of it may be applicable to larger systems. To subscribe, send the line:

```
SUB VIRUS-L your full name
```

to the address LISTSERV%LEHIIBM1.BITNET@MITVMA.MIT.EDU. This list is also available via the USENET newsgroup "comp.virus".

The Computer Underground Digest "is an open forum dedicated to sharing information among computerists and to the presentation and debate of diverse views." While not directly a security list, it does contain discussions about privacy and other security related topics. The list can be read on USENET as alt.society.cu-digest, or to join the mailing list, send mail to Gordon Myer (TK0JUT2%NIU.bitnet@mitvma.mit.edu). Submissions may be mailed to: cud@chinacat.unicom.com.

3.9.7.2 Networking Mailing Lists

The TCP-IP mailing list is intended to act as a discussion forum for developers and maintainers of implementations of the TCP/IP protocol suite. It also discusses network-related security problems when they involve programs providing network services, such as "Sendmail". To join the TCP-IP list, send a message to TCP-IP-REQUEST@NISC.SRI.COM. This list is also available in the USENET newsgroup "comp.protocols.tcp-ip".

SUN-NETS is a discussion list for items pertaining to networking on Sun systems. Much of the discussion is related to NFS, NIS (formally Yellow Pages), and name servers. To subscribe, send a message to SUN-NETS-REQUEST@UMIACS.UMD.EDU.

The USENET groups misc.security and alt.security also discuss security issues. misc.security is a moderated group and also includes discussions of physical security and locks. alt.security is unmoderated.

3.9.7.3 Response Teams

Several organizations have formed special groups of people to deal with computer security problems. These teams collect information about possible security holes and disseminate it to the proper people, track intruders, and assist in recovery from security violations. The teams typically have both electronic mail distribution lists as well as a special telephone number which can be called for information or to report a problem. Many of these teams are members of the CERT System, which is coordinated by the National Institute of Standards and Technology (NIST), and exists to facilitate the exchange of information between the various teams.

3.9.7.3.1 DARPA Computer Emergency Response Team

The Computer Emergency Response Team/Coordination Center (CERT/CC) was established in December 1988 by the Defense Advanced Research Projects Agency (DARPA) to address computer security concerns of research users of the Internet. It is operated by the Software Engineering Institute (SEI) at Carnegie-Mellon University (CMU). The CERT can immediately confer with experts to diagnose and solve security problems, and also establish and maintain communications with the affected computer users and government authorities as appropriate.

The CERT/CC serves as a clearing house for the identification and repair of security vulnerabilities, informal assessments of existing systems, improvement of emergency response capability, and both vendor and user security awareness. In addition, the team works with vendors of various systems in order to coordinate the fixes for security problems.

The CERT/CC sends out security advisories to the CERT-ADVISORY mailing list whenever appropriate. They also operate a 24-hour hotline that can be called to report security problems (e.g., someone breaking into your system), as well as to obtain current (and accurate) information about rumored security problems.

To join the CERT-ADVISORY mailing list, send a message to CERT@CERT.SEI.CMU.EDU and ask to be added to the mailing list. The material sent to this list also appears in the

USENET newsgroup "comp.security.announce". Past advisories are available for anonymous FTP from the host CERT.SEI.CMU.EDU. The 24-hour hotline number is (412) 268- 7090.

The CERT/CC also maintains a CERT-TOOLS list to encourage the exchange of information on tools and techniques that increase the secure operation of Internet systems. The CERT/CC does not review or endorse the tools described on the list. To subscribe, send a message to CERT-TOOLS-REQUEST@CERT.SEI.CMU.EDU and ask to be added to the mailing list.

The CERT/CC maintains other generally useful security information for anonymous FTP from CERT.SEI.CMU.EDU. Get the README file for a list of what is available.

For more information, contact:

CERT Software Engineering Institute Carnegie Mellon
University Pittsburgh, PA 15213-3890
(412) 268-7090 cert@cert.sei.cmu.edu.

3.9.7.3.2 DDN Security Coordination Center

For DDN users, the Security Coordination Center (SCC) serves a function similar to CERT. The SCC is the DDN's clearing- house for host/user security problems and fixes, and works with the DDN Network Security Officer. The SCC also distributes the DDN Security Bulletin, which communicates information on network and host security exposures, fixes, and concerns to security and management personnel at DDN facilities. It is available online, via kermit or anonymous FTP, from the host NIC.DDN.MIL, in SCC:DDN-SECURITY-yy-nn.TXT (where "yy" is the year and "nn" is the bulletin number). The SCC provides immediate assistance with DDN-related host security problems; call (800) 235-3155 (6:00 a.m. to 5:00 p.m. Pacific Time) or send email to SCC@NIC.DDN.MIL. For 24 hour coverage, call the MILNET Trouble Desk (800) 451-7413 or AUTOVON 231-1713.

3.9.7.3.3 NIST Computer Security Resource and Response Center

The National Institute of Standards and Technology (NIST) has responsibility within the U.S. Federal Government for computer science and technology activities. NIST has played a strong role in organizing the CERT System and is now serving as the CERT System Secretariat. NIST also operates a Computer Security Resource and Response Center (CSRC) to provide help and information regarding computer security events and incidents, as well as to raise awareness about computer security vulnerabilities.

The CSRC team operates a 24-hour hotline, at (301) 975-5200. For individuals with access to the Internet, on-line publications and computer security information can be obtained via anonymous FTP from the host CSRC.NCSL.NIST.GOV (129.6.48.87). NIST also operates a personal computer bulletin board that contains information regarding computer viruses as well as other aspects of computer security. To access this board, set your modem to 300/1200/2400 BPS, 1 stop bit, no parity, and 8-bit characters, and call (301) 948-5717. All users are given full access to the board immediately upon registering.

NIST has produced several special publications related to computer security and computer viruses in particular; some of these publications are downloadable. For further information, contact NIST at the following address:

Computer Security Resource and Response Center A-216
Technology Gaithersburg, MD 20899 Telephone: (301)
975-3359 Electronic Mail: CSRC@nist.gov

3.9.7.3.4 DOE Computer Incident Advisory Capability (CIAC)
CIAC is the Department of Energy's (DOE's) Computer Incident Advisory Capability. CIAC is a four-person team of computer scientists from Lawrence Livermore National Laboratory (LLNL) charged with the primary responsibility of assisting DOE sites faced with computer security incidents (e.g., intruder attacks, virus infections, worm attacks, etc.). This capability is available to DOE sites on a 24-hour-a-day basis.

CIAC was formed to provide a centralized response capability (including technical assistance), to keep sites informed of current events, to deal proactively with computer security issues, and to maintain liaisons with other response teams and agencies. CIAC's charter is to assist sites (through direct technical assistance, providing information, or referring inquiries to other technical experts), serve as a clearinghouse for information about threats/known incidents/vulnerabilities, develop guidelines for incident handling, develop software for responding to events/incidents, analyze events and trends, conduct training and awareness activities, and alert and advise sites about vulnerabilities and potential attacks.

CIAC's business hours phone number is (415) 422-8193 or FTS 532-8193. CIAC's e-mail address is CIAC@TIGER.LLNL.GOV.

3.9.7.3.5 NASA Ames Computer Network Security Response Team

The Computer Network Security Response Team (CNSRT) is NASA Ames Research Center's local version of the DARPA CERT. Formed in August of 1989, the team has a constituency that is primarily Ames users, but it is also involved in assisting other NASA Centers and federal agencies. CNSRT maintains liaisons with the DOE's CIAC team and the DARPA CERT. It is also a charter member of the CERT System. The team may be reached by 24 hour pager at (415) 694-0571, or by electronic mail to CNSRT@AMES.ARC.NASA.GOV.

3.9.7.4 DDN Management Bulletins

The DDN Management Bulletin is distributed electronically by the DDN NIC under contract to the Defense Communications Agency (DCA). It is a means of communicating official policy, procedures, and other information of concern to management personnel at DDN facilities.

The DDN Security Bulletin is distributed electronically by the DDN SCC, also under contract to DCA, as a means of communicating information on network and host security exposures, fixes, and concerns to security and management personnel at DDN facilities.

Anyone may join the mailing lists for these two bulletins by sending a message to NIC@NIC.DDN.MIL and asking to be placed on the mailing lists. These messages are also posted to the USENET newsgroup "ddn.mgt-bulletin". For additional information, see section 8.7.

3.9.7.5 System Administration List

The SYSADM-LIST is a list pertaining exclusively to UNIX system administration. Mail requests to be added to the list to SYSADM-LIST-REQUEST@SYSADMIN.COM.

3.9.7.6 Vendor Specific System Lists

The SUN-SPOTS and SUN-MANAGERS lists are discussion groups for users and administrators of systems supplied by Sun Microsystems. SUN-SPOTS is a fairly general list, discussing everything from hardware configurations to simple UNIX questions. To subscribe, send a message to SUN-SPOTS- REQUEST@RICE.EDU. This list is also available in the USENET newsgroup "comp.sys.sun". SUN-MANAGERS is a discussion list for Sun system administrators and covers all aspects of Sun system administration. To subscribe, send a message to SUN- MANAGERS-REQUEST@EECS.NWU.EDU.

The APOLLO list discusses the HP/Apollo system and its software. To subscribe, send a message to APOLLO-REQUEST@UMIX.CC.UMICH.EDU. APOLLO-L is a similar list which can be subscribed to by sending

```
SUB APOLLO-L your full name
```

to LISTSERV%UMRVMB.BITNET@VM1.NODAK.EDU.

HPMINI-L pertains to the Hewlett-Packard 9000 series and HP/UX operating system. To subscribe, send

```
SUB HPMINI-L your full name
```

to LISTSERV%UAFSYSB.BITNET@VM1.NODAK.EDU.

INFO-IBMPC discusses IBM PCs and compatibles, as well as MS- DOS. To subscribe, send a note to INFO-IBMPC-REQUEST@WSMR- SIMTEL20.ARMY.MIL.

There are numerous other mailing lists for nearly every popular computer or workstation in use today. For a complete list, obtain the file "netinfo/interest-groups" via anonymous FTP from the host FTP.NISC.SRI.COM.

3.9.7.7 Professional Societies and Journals

The IEEE Technical Committee on Security & Privacy publishes a quarterly magazine, "CIPHER".

IEEE Computer Society, 1730 Massachusetts Ave. N.W.
Washington, DC 2036-1903

The ACM SigSAC (Special Interest Group on Security, Audit, and Controls) publishes a quarterly magazine, "SIGSAC Review".

Association for Computing Machinery 11 West 42nd St. New York, N.Y. 10036

The Information Systems Security Association publishes a quarterly magazine called "ISSA Access".

Information Systems Security Association P.O. Box 9457
Newport Beach, CA 92658

"Computers and Security" is an "international journal for the professional involved with computer security, audit and control, and data integrity."
$266/year, 8 issues (1990)

Elsevier Advanced Technology Journal Information Center
655 Avenue of the Americas New York, NY 10010

The "Data Security Letter" is published "to help data security professionals by providing inside information and knowledgable analysis of developments in computer and communications security."
$690/year, 9 issues (1990)

Data Security Letter P.O. Box 1593 Palo Alto, CA 94302

3.9.8 Problem Reporting Tools

3.9.8.1 Auditing

Auditing is an important tool that can be used to enhance the security of your installation. Not only does it give you a means of identifying who has accessed your system (and may have done something to it) but it also gives you an indication of how your system is being used (or abused) by authorized users and attackers alike. In addition, the audit trail traditionally kept by computer systems can become an invaluable piece of evidence should your system be penetrated.

3.9.8.1.1 Verify Security

An audit trail shows how the system is being used from day to day. Depending upon how your site audit log is configured, your log files should show a range of access attempts that can show what normal system usage should look like. Deviation from that normal usage could be the result of penetration from an outside source using an old or stale user account. Observing a deviation in logins, for example, could be your first indication that something unusual is happening.

3.9.8.1.2 Verify Software Configurations

One of the ruses used by attackers to gain access to a system is by the insertion of a so-called Trojan Horse program. A Trojan Horse program can be a program that does something useful, or merely something interesting. It always does something unexpected, like steal passwords or copy files without your knowledge [25]. Imagine a Trojan login program that prompts for username and password in the usual way, but also writes that information to a special file that the attacker can come back and read at will. Imagine a Trojan Editor program that, despite the file permissions you have given your files, makes copies of everything in your directory space without you knowing about it.

This points out the need for configuration management of the software that runs on a system, not as it is being developed, but as it is in actual operation. Techniques for doing this range from checking each command every time it is executed against some criterion (such as a cryptoseal, described above) or merely checking the date and time stamp of the executable. Another technique might be to check each command in batch mode at midnight.

3.9.8.2 Tools

COPS is a security tool for system administrators that checks for numerous common security problems on UNIX systems [27]. COPS is a collection of shell scripts and C programs that can easily be run on almost any UNIX variant. Among other things, it checks the following items and sends the results to the system administrator:

- Checks "/dev/kmem" and other devices for world read/writability.

- Checks special or important files and directories for "bad" modes (world writable, etc.).

- Checks for easily-guessed passwords.
- Checks for duplicate user ids, invalid fields in the password file, etc..
- Checks for duplicate group ids, invalid fields in the group file, etc..
- Checks all users' home directories and their ".cshrc", ".login", ".profile", and ".rhosts" files for security problems.
- Checks all commands in the "/etc/rc" files and "cron" files for world writability.
- Checks for bad "root" paths, NFS file systems exported to the world, etc..
- Includes an expert system that checks to see if a given user (usually "root") can be compromised, given that certain rules are true.
- Checks for changes in the setuid status of programs on the system.

The COPS package is available from the "comp.sources.unix" archive on "ftp.uu.net", and also from the UNIX-SW repository on the MILNET host "wsmr-simtel20.army.mil".

3.9.9 Communication Among Administrators

3.9.9.1 Secure Operating Systems

The following list of products and vendors is adapted from the National Computer Security Center's (NCSC) Evaluated Products List. They represent those companies who have either received an evaluation from the NCSC or are in the process of a product evaluation. This list is not complete, but it is representative of those operating systems and add on components available in the commercial marketplace.

For a more detailed listing of the current products appearing in the NCSC EPL, contact the NCSC at:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000
(301) 859-4458

Evaluated Product	Vendor	Version Evaluated	Evaluation Class
Secure Communications Processor (SCOMP)	Honeywell Information Systems, Inc.	2.1	A1
Multics	Honeywell Information Systems, Inc.	MR11.0	B2
System V/MLS 1.1.2 on UNIX System V 3.1.1 on AT&T 3B2/500 and 3B2/600	AT&T	1.1.2	B1
OS 1100	Unisys Corp.	Security Release 1	B1
MPE V/E	Hewlett-Packard Computer Systems Division	G.03.04	C2
AOS/VS on MV/ECLIPSE series	Data General Corp.	7.60	C2
VM/SP or VM/SP HPO with CMS, RACF, DIRMAINT, VMTAPE-MS, ISPF	IBM Corp.	5	C2
MVS/XA with RACF	IBM Corp.	2.2,2.3	C2
AX/VMS	Digital Equipment Corp.	4.3	C2
NOS	Control Data Corp.	NOS Security Eval Product	C2
TOP SECRET	CGA Software Products Group, Inc.	3.0/163	C2
Access Control Facility 2	SKK, Inc.	3.1.3	C2
UTX/32S	Gould, Inc. Computer Systems Division	1.0	C2
A Series MCP/AS with InfoGuard Security Enhancements	Unisys Corp.	3.7	C2
Primos	Prime Computer, Inc.	21.0.1DODC2A	C2
Resource Access Control Facility (RACF)	IBM Corp.	1.5	C1

Candidate Product	Vendor	Version Evaluated	Candidate Class
Boeing MLS LAN	Boeing Aerospace		A1 M1
Trusted XENIX	Trusted Information Systems, Inc.		B2
VSLAN	VERDIX Corp.		B2
System V/MLS	AT&T		B1
VM/SP with RACF	IBM Corp.	5/1.8.2	C2
Wang SVS/OS with CAP	Wang Laboratories, Inc.	1.0	C2

3.9.9.2 Obtaining Fixes for Known Problems

It goes without saying that computer systems have bugs. Even operating systems, upon which we depend for protection of our data, have bugs. And since there are bugs, things can be broken, both maliciously and accidentally. It is important that whenever bugs are discovered, a should fix be identified and implemented as soon as possible. This should minimize any exposure caused by the bug in the first place.

A corollary to the bug problem is: from whom do I obtain the fixes? Most systems have some support from the manufacturer or supplier. Fixes coming from that source tend to be implemented quickly after receipt. Fixes for some problems are often posted on the network and are left to the system administrators to incorporate as they can. The problem is that one wants to have faith that the fix will close the hole and not introduce any others. We will tend to trust that the manufacturer's fixes are better than those that are posted on the net.

3.9.9.3 Sun Customer Warning System

Sun Microsystems has established a Customer Warning System (CWS) for handling security incidents. This is a formal process which includes:

- Having a well advertised point of contact in Sun for reporting security problems.
- Pro-actively alerting customers of worms, viruses, or other security holes that could affect their systems.
- Distributing the patch (or work-around) as quickly as possible.

They have created an electronic mail address, SECURITY-ALERT@SUN.COM, which will enable customers to report security problems. A voice-mail backup is available at (415) 688-9081. A "Security Contact" can be designated by each customer site; this person will be contacted by Sun in case of any new security problems. For more information, contact your Sun representative.

3.9.9.4 Trusted Archive Servers

Several sites on the Internet maintain large repositories of public-domain and freely distributable software, and make this material available for anonymous FTP. This section describes some of the larger repositories. Note that none of these servers implements secure checksums or anything else guaranteeing the integrity of their data. Thus, the notion of "trust" should be taken as a somewhat limited definition.

3.9.9.4.1 Sun Fixes on UUNET

Sun Microsystems has contracted with UUNET Communications Services, Inc., to make fixes for bugs in Sun software available via anonymous FTP. You can access these fixes by using the "ftp" command to connect to the host FTP.UU.NET. Then change into the directory "sun-dist/security", and obtain a directory listing. The file "README" contains a brief description of what each file in this directory contains, and what is required to install the fix.

3.9.9.4.2 Berkeley Fixes

The University of California at Berkeley also makes fixes available via anonymous FTP; these fixes pertain primarily to the current release of BSD UNIX (currently, release 4.3). However, even if you are not running their software, these fixes are still important, since many vendors (Sun, DEC, Sequent, etc.) base their software on the Berkeley releases.

The Berkeley fixes are available for anonymous FTP from the host UCBARPA.BERKELEY.EDU in the directory "4.3/ucb-fixes". The file "INDEX" in this directory describes what each file contains. They are also available from UUNET (see section 3.9.9.4.3).

Berkeley also distributes new versions of "sendmail" and "named" from this machine. New versions of these commands are stored in the "4.3" directory, usually in the files "sendmail.tar.Z" and "bind.tar.Z", respectively.

3.9.9.4.3 Simtel-20 and UUNET

The two largest general-purpose software repositories on the Internet are the hosts WSMR-SIMTEL20.ARMY.MIL and FTP.UU.NET.

WSMR-SIMTEL20.ARMY.MIL is a TOPS-20 machine operated by the U.S. Army at White Sands Missile Range (WSMR), New Mexico. The directory "pd2:<unix-c>" contains a large amount of UNIX software, primarily taken from the "comp.sources" newsgroups. The directories "pd1:<msdos>" and "pd2:<msdos2>" contains software for IBM PC systems, and "pd3:<macintosh>" contains software for the Apple Macintosh.

FTP.UU.NET is operated by UUNET Communications Services, Inc. in Falls Church, Virginia. This company sells Internet and USENET access to sites all over the country (and internationally). The software posted to the following USENET source newsgroups is stored here, in directories of the same name:

comp.sources.games
comp.sources.misc
comp.sources.sun
comp.sources.unix
comp.sources.x

Numerous other distributions, such as all the freely distributable Berkeley UNIX source code, Internet Request for Comments (RFCs), and so on are also stored on this system.

3.9.9.4.4 Vendors

Many vendors make fixes for bugs in their software available electronically, either via mailing lists or via anonymous FTP. You should contact your vendor to find out if they offer this service, and if so, how to access it. Some vendors that offer these services include Sun Microsystems (see above), Digital Equipment Corporation (DEC), the University of California at Berkeley (see above), and Apple Computer [5, CURRY].

4. Types of Security Procedures

4.1 System Security Audits

Most businesses undergo some sort of annual financial auditing as a regular part of their business life. Security audits are an important part of running any computing environment. Part of the security audit should be a review of any policies that concern system security, as well as the mechanisms that are put in place to enforce them.

4.1.1 Organize Scheduled Drills

Although not something that would be done each day or week, scheduled drills may be conducted to determine if the procedures defined are adequate for the threat to be countered. If your major threat is one of natural disaster, then a drill would be conducted to verify your backup and recovery mechanisms. On the other hand, if your greatest threat is from external intruders attempting to penetrate your system, a drill might be conducted to actually try a penetration to observe the effect of the policies.

Drills are a valuable way to test that your policies and procedures are effective. On the other hand, drills can be time- consuming and disruptive to normal operations. It is important to weigh the benefits of the drills against the possible time loss which may be associated with them.

4.1.2 Test Procedures

If the choice is made to not to use scheduled drills to examine your entire security procedure at one time, it is important to test individual procedures frequently. Examine your backup procedure to make sure you can recover data from the tapes. Check log files to be sure that information which is supposed to be logged to them is being logged to them, etc..

When a security audit is mandated, great care should be used in devising tests of the security policy. It is important to clearly identify what is being tested, how the test will be conducted, and results expected from the test. This should all be documented and included in or as an adjunct to the security policy document itself.

It is important to test all aspects of the security policy, both procedural and automated, with a particular emphasis on the automated mechanisms used to enforce the policy. Tests should be defined to ensure a comprehensive examination of policy features, that is, if a test is defined to examine the user logon process, it should be explicitly stated that both valid and invalid user names and passwords will be used to demonstrate proper operation of the logon program.

Keep in mind that there is a limit to the reasonableness of tests. The purpose of testing is to ensure confidence that the security policy is being correctly enforced, and not to "prove" the absoluteness of the system or policy. The goal should be to obtain some assurance that the reasonable and credible controls imposed by your security policy are adequate.

4.2 Account Management Procedures

Procedures to manage accounts are important in preventing unauthorized access to your system. It is necessary to decide several things: Who may have an account on the system? How long may someone have an account without renewing his or her request? How do old accounts get removed from the system? The answers to all these questions should be explicitly set out in the policy.

In addition to deciding who may use a system, it may be important to determine what each user may use the system for (is personal use allowed, for example). If you are connected to an outside network, your site or the network management may have rules about what the network may be used for. Therefore, it is important for any security policy to define an adequate account management procedure for both administrators and users. Typically, the system administrator would be responsible for creating and deleting user accounts and generally maintaining overall control of system use. To some degree, account management is also the responsibility of each system user in the sense that the user should observe any system messages and events that may be indicative of a policy violation. For example, a message at logon that indicates the date and time of the last logon should be reported by the user if it indicates an unreasonable time of last logon.

4.3 Password Management Procedures

A policy on password management may be important if your site wishes to enforce secure passwords. These procedures may range from asking or forcing users to change their passwords occasionally to actively attempting to break users' passwords and then informing the user of how easy it was to do. Another part of password management policy covers who may distribute passwords - can users give their passwords to other users?

Section 2.3 discusses some of the policy issues that need to be decided for proper password management. Regardless of the policies, password management procedures need to be carefully setup to avoid disclosing passwords. The choice of initial passwords for accounts is critical. In some cases, users may never login to activate an account; thus, the choice of the initial password should not be easily guessed. Default passwords should never be assigned to accounts: always create new passwords for each user. If there are any printed lists of passwords, these should be kept off-line in secure locations; better yet, don't list passwords.

4.3.1 Password Selection

Perhaps the most vulnerable part of any computer system is the account password. Any computer system, no matter how secure it is from network or dial-up attack, Trojan horse programs, and so on, can be fully exploited by an intruder if he or she can gain access via a poorly chosen password. It is important to define a good set of rules for password selection, and distribute these rules to all users. If possible, the software which sets user passwords should be modified to enforce as many of the rules as possible.

A sample set of guidelines for password selection is shown below:

- DON'T use your login name in any form (as-is, reversed, capitalized, doubled, etc.).

- DON'T use your first, middle, or last name in any form.

- DON'T use your spouse's or child's name.

- DON'T use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc..

- DON'T use a password of all digits, or all the same letter.

- DON'T use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.

- DON'T use a password shorter than six characters.

- DO use a password with mixed-case alphabetics.

- DO use a password with non-alphabetic characters (digits or punctuation).

- DO use a password that is easy to remember, so you don't have to write it down.

- DO use a password that you can type quickly, without having to look at the keyboard.

Methods of selecting a password which adheres to these guidelines include:

- Choose a line or two from a song or poem, and use the first letter of each word.

- Alternate between one consonant and one or two vowels, up to seven or eight characters. This provides nonsense words which are usually pronounceable, and thus easily remembered.

- Choose two short words and concatenate them together with a punctuation character between them.

Users should also be told to change their password periodically, usually every three to six months. This makes sure that an intruder who has guessed a password will eventually lose access, as well as invalidating any list of passwords he/she may have obtained. Many systems enable the system administrator to force users to change their passwords after an expiration period; this software should be enabled if your system supports it [5, CURRY].

Some systems provide software which forces users to change their passwords on a regular basis. Many of these systems also include password generators which provide the user with a set of passwords to choose from. The user is not permitted to make up his or her own password. There are arguments both for and against systems such as these. On the one hand, by using generated passwords, users are prevented from selecting insecure passwords. On the other hand, unless the generator is good at making up easy to remember passwords, users will begin writing them down in order to remember them.

4.3.2 Procedures for Changing Passwords

How password changes are handled is important to keeping passwords secure. Ideally, users should be able to change their own passwords on-line. (Note that password changing programs are a favorite target of intruders. See section 4.4 on configuration management for further information.)

However, there are exception cases which must be handled carefully. Users may forget passwords and not be able to get onto the system. The standard procedure is to assign the user a new password. Care should be taken to make sure that the real person is requesting the change and gets the new password. One common trick used by intruders is to call or message to a system administrator and request a new password. Some external form of verification should be used before the password is assigned. At some sites, users are required to show up in person with ID.

There may also be times when many passwords need to be changed. If a system is compromised by an intruder, the intruder may be able to steal a password file and take it off the system. Under these circumstances, one course of action is to change all passwords on the system. Your site should have procedures for how this can be done quickly and efficiently. What course you choose may depend on the urgency of the problem. In the case of a known attack with damage, you may choose to forcibly disable all accounts and assign users new passwords before they come back onto the system. In some places, users are sent a message telling them that they should change their passwords, perhaps within a certain time period. If the password isn't changed before the time period expires, the account is locked.

Users should be aware of what the standard procedure is for passwords when a security event has occurred. One well-known spoof reported by the Computer Emergency Response Team (CERT) involved messages sent to users, supposedly from local system administrators, requesting them to immediately change their password to a new value provided in the message [24]. These messages were not from the administrators, but from intruders trying to steal accounts. Users should be warned to immediately report any suspicious requests such as this to site administrators.

4.4 Configuration Management Procedures

Configuration management is generally applied to the software development process. However, it is certainly applicable in a operational sense as well. Consider that the since many of the system level programs are intended to enforce the security policy, it is important that these be "known" as correct. That is, one should not allow system level programs (such as the operating system, etc.) to be changed arbitrarily. At very least, the procedures should state who is authorized to make changes to systems, under what circumstances, and how the changes should be documented.

In some environments, configuration management is also desirable as applied to physical configuration of equipment. Maintaining valid and authorized hardware configuration should be given due consideration in your security policy.

4.4.1 Non-Standard Configurations

Occasionally, it may be beneficial to have a slightly non-standard configuration in order to thwart the "standard" attacks used by some intruders. The non-standard parts of the configuration might include different password encryption algorithms, different configuration file locations, and rewritten or functionally limited system commands.

Non-standard configurations, however, also have their drawbacks. By changing the "standard" system, these modifications make software maintenance more difficult by requiring extra documentation to be written, software modification after operating system upgrades, and, usually, someone with special knowledge of the changes.

Because of the drawbacks of non-standard configurations, they are often only used in environments with a "firewall" machine (see section 3.9.1). The firewall machine is modified in non-standard ways since it is susceptible to attack, while internal systems behind the firewall are left in their standard configurations.

5. Incident Handling

5.1 Overview

This section of the document will supply some guidance to be applied when a computer security event is in progress on a machine, network, site, or multi-site environment. The operative philosophy in the event of a breach of computer security, whether it be an external intruder attack or a disgruntled employee, is to plan for adverse events in advance. There is no substitute for creating contingency plans for the types of events described above.

Traditional computer security, while quite important in the overall site security plan, usually falls heavily on protecting systems from attack, and perhaps monitoring systems to detect attacks. Little attention is usually paid for how to actually handle the attack when it occurs. The result is that when an attack is in progress, many decisions are made in haste and can be damaging to tracking down the source of the incident, collecting evidence to be used in prosecution efforts, preparing for the recovery of the system, and protecting the valuable data contained on the system.

5.1.1 Have a Plan to Follow in Case of an Incident

Part of handling an incident is being prepared to respond before the incident occurs. This includes establishing a suitable level of protections, so that if the incident becomes severe, the damage which can occur is limited. Protection includes preparing incident handling guidelines or a contingency response plan for your organization or site. Having written plans eliminates much of the ambiguity which occurs during an incident, and will lead to a more appropriate and thorough set of responses. Second, part of protection is preparing a method of notification, so you will know who to call and the relevant phone numbers. It is important, for example, to conduct "dry runs," in which your computer security personnel, system administrators, and managers simulate handling an incident.

Learning to respond efficiently to an incident is important for numerous reasons. The most important benefit is directly to human beings—preventing loss of human life. Some computing systems are life critical systems, systems on which human life depends (e.g., by controlling some aspect of life-support in a hospital or assisting air traffic controllers).

An important but often overlooked benefit is an economic one. Having both technical and managerial personnel respond to an incident requires considerable resources, resources which could be utilized more profitably if an incident did not require their services. If these personnel are trained to handle an incident efficiently, less of their time is required to deal with that incident.

A third benefit is protecting classified, sensitive, or proprietary information. One of the major dangers of a computer security incident is that information may be irrecoverable. Efficient incident handling minimizes this danger. When classified information is involved, other government regulations may apply and must be integrated into any plan for incident handling.

A fourth benefit is related to public relations. News about computer security incidents tends to be damaging to an organization's stature among current or potential clients. Efficient incident handling minimizes the potential for negative exposure.

A final benefit of efficient incident handling is related to legal issues. It is possible that in the near future organizations may be sued because one of their nodes was used to launch a network attack. In a similar vein, people who develop patches or workarounds may be sued if the patches or workarounds are ineffective, resulting in damage to systems, or if the patches or workarounds themselves damage systems. Knowing about operating system vulnerabilities and patterns of attacks and then taking appropriate measures is critical to circumventing possible legal problems.

5.1.2 Order of Discussion in this Session Suggests an Order for a Plan

This chapter is arranged such that a list may be generated from the Table of Contents to provide a starting point for creating a policy for handling ongoing incidents. The main points to be included in a policy for handling incidents are:

- Overview (what are the goals and objectives in handling the incident).
- Evaluation (how serious is the incident).
- Notification (who should be notified about the incident).
- Response (what should the response to the incident be).

- Legal/Investigative (what are the legal and prosecutorial implications of the incident).
- Documentation Logs (what records should be kept from before, during, and after the incident).

Each of these points is important in an overall plan for handling incidents. The remainder of this chapter will detail the issues involved in each of these topics, and provide some guidance as to what should be included in a site policy for handling incidents.

5.1.3 Possible Goals and Incentives for Efficient Incident Handling

As in any set of pre-planned procedures, attention must be placed on a set of goals to be obtained in handling an incident. These goals will be placed in order of importance depending on the site, but one such set of goals might be:

Assure integrity of (life) critical systems. Maintain and restore data. Maintain and restore service. Figure out how it happened. Avoid escalation and further incidents. Avoid negative publicity. Find out who did it. Punish the attackers.

It is important to prioritize actions to be taken during an incident well in advance of the time an incident occurs. Sometimes an incident may be so complex that it is impossible to do everything at once to respond to it; priorities are essential. Although priorities will vary from institution-to-institution, the following suggested priorities serve as a starting point for defining an organization's response:

- Priority one — protect human life and people's safety; human life always has precedence over all other considerations.

- Priority two — protect classified and/or sensitive data (as regulated by your site or by government regulations).
- Priority three — protect other data, includingproprietary, scientific, managerial and other data, because loss of data is costly in terms of resources.
- Priority four — prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.); damage to systems can result in costly down time and recovery.
- Priority five — minimize disruption of computing resources; it is better in many cases to shut a system down or disconnect from a network than to risk damage to data or systems.

An important implication for defining priorities is that once human life and national security considerations have been addressed, it is generally more important to save data than system software and hardware. Although it is undesirable to have any damage or loss during an incident, systems can be replaced; the loss or compromise of data (especially classified data), however, is usually not an acceptable outcome under any circumstances.

Part of handling an incident is being prepared to respond before the incident occurs. This includes establishing a suitable level of protections so that if the incident becomes severe, the damage which can occur is limited. Protection includes preparing incident handling guidelines or a contingency response plan for your organization or site. Written plans eliminate much of the ambiguity which occurs during an incident, and will lead to a more appropriate and thorough set of responses. Second, part of protection is preparing a method of notification so you will know who to call and how to contact them. For example, every member of the Department of Energy's CIAC Team carries a card with every other team member's work and home phone numbers, as well as pager numbers. Third, your organization or site should establish backup procedures for every machine and system. Having backups eliminates much of the threat of even a severe incident, since backups preclude serious data loss. Fourth, you should set up secure systems. This involves eliminating vulnerabilities, establishing an effective password policy, and other procedures, all of which will be explained later in this document. Finally, conducting training activities is part of protection. It is important, for example, to conduct "dry runs," in which your computer security personnel, system administrators, and managers simulate handling an incident.

5.1.4 Local Policies and Regulations Providing Guidance

Any plan for responding to security incidents should be guided by local policies and regulations. Government and private sites that deal with classified material have specific rules that they must follow.

The policies your site makes about how it responds to incidents (as discussed in sections 2.4 and 2.5) will shape your response. For example, it may make little sense to create mechanisms to monitor and trace intruders if your site does not plan to take action against the intruders if they are caught. Other organizations may have policies that affect your plans. Telephone companies often release information about telephone traces only to law enforcement agencies.

Section 5.5 also notes that if any legal action is planned, there are specific guidelines that must be followed to make sure that any information collected can be used as evidence.

5.2 Evaluation

5.2.1 Is It Real?

This stage involves determining the exact problem. Of course many, if not most, signs often associated with virus infections, system intrusions, etc., are simply anomalies such as hardware failures. To assist in identifying whether there really is an incident, it is usually helpful to obtain and use any detection software which may be available. For example, widely available software packages can greatly assist someone who thinks there may be a virus in a Macintosh computer. Audit information is also extremely useful, especially in determining whether there is a network attack. It is extremely important to obtain a system snapshot as soon as one suspects that something is wrong. Many incidents cause a dynamic chain of events to occur, and an initial system snapshot may do more good in identifying the problem and any source of attack than most other actions which can be taken at this stage. Finally, it is important to start a log book. Recording system events, telephone conversations, time stamps, etc., can lead to a more rapid and systematic identification of the problem, and is the basis for subsequent stages of incident handling.

There are certain indications or "symptoms" of an incident which deserve special attention:

- System crashes.
- New user accounts (e.g., the account RUMPLESTILTSKIN has unexplainedly been created),

or high activity on an account that has had virtually no activity for months.

- New files (usually with novel or strange file names, such as data.xx or k).
- Accounting discrepancies (e.g., in a UNIX system you might notice that the accounting file called /usr/admin/lastlog has shrunk, something that should make you very suspicious that there may be an intruder).
- Changes in file lengths or dates (e.g., a user should be suspicious if he/she observes that the .EXE files in an MS DOS computer have unexplainedly grown by over 1800 bytes).
- Attempts to write to system (e.g., a system manager notices that a privileged user in a VMS system is attempting to alter RIGHTSLIST.DAT).
- Data modification or deletion (e.g., files start to disappear).
- Denial of service (e.g., a system manager and all other users become locked out of a UNIX system, which has been changed to single user mode).
- Unexplained, poor system performance (e.g., system response time becomes unusually slow).
- Anomalies (e.g., "GOTCHA" is displayed on a display terminal or there are frequent unexplained "beeps").
- Suspicious probes (e.g., there are numerous unsuccessful login attempts from another node).
- Suspicious browsing (e.g., someone becomes a root user on a UNIX system and accesses file after file in one user's account, then another's).

None of these indications is absolute "proof" that an incident is occurring, nor are all of these indications normally observed when an incident occurs. If you observe any of these indications, however, it is important to suspect that an incident might be occurring, and act accordingly. There is no formula for determining with 100 percent accuracy that an incident is occurring (possible exception: when a virus detection package indicates that your machine has the nVIR virus and you confirm this by examining contents of the nVIR resource in your Macintosh computer, you can be very certain that your machine is infected). It is best at this point to collaborate with other technical and computer security personnel to make a decision as a group about whether an incident is occurring.

5.2.2 Scope

Along with the identification of the incident is the evaluation of the scope and impact of the problem. It is important to correctly identify the boundaries of the incident in order to effectively deal with it. In addition, the impact of an incident will determine its priority in allocating resources to deal with the event. Without an indication of the scope and impact of the event, it is difficult to determine a correct response.

In order to identify the scope and impact, a set of criteria should be defined which is appropriate to the site and to the type of connections available. Some of the issues are:

- Is this a multi-site incident?
- Are many computers at your site effected by this incident?
- Is sensitive information involved?
- What is the entry point of the incident (network, phone line, local terminal, etc.)?
- Is the press involved?
- What is the potential damage of the incident?

- What is the estimated time to close out the incident?
- What resources could be required to handle the incident?

5.3 Possible Types of Notification

When you have confirmed that an incident is occurring, the appropriate personnel must be notified. Who and how this notification is achieved is very important in keeping the event under control both from a technical and emotional standpoint.

5.3.1 Explicit

First of all, any notification to either local or off-site personnel must be explicit. This requires that any statement (be it an electronic mail message, phone call, or fax) provides information about the incident that is clear, concise, and fully qualified. When you are notifying others that will help you to handle an event, a "smoke screen" will only divide the effort and create confusion. If a division of labor is suggested, it is helpful to provide information to each section about what is being accomplished in other efforts. This will not only reduce duplication of effort, but allow people working on parts of the problem to know where to obtain other information that would help them resolve a part of the incident.

5.3.2 Factual

Another important consideration when communicating about the incident is to be factual. Attempting to hide aspects of the incident by providing false or incomplete information may not only prevent a successful resolution to the incident, but may even worsen the situation. This is especially true when the press is involved. When an incident severe enough to gain press attention is ongoing, it is likely that any false information you provide will not be substantiated by other sources. This will reflect badly on the site and may create enough ill-will between the site and the press to damage the site's public relations.

5.3.3 Choice of Language

The choice of language used when notifying people about the incident can have a profound effect on the way that information is received. When you use emotional or inflammatory terms, you raise the expectations of damage and negative outcomes of the incident. It is important to remain calm both in written and spoken notifications.

Another issue associated with the choice of language is the notification to non-technical or off-site personnel. It is important to accurately describe the incident without undue alarm or confusing messages. While it is more difficult to describe the incident to a non-technical audience, it is often more important. A non-technical description may be required for upper-level management, the press, or law enforcement liaisons. The importance of these notifications cannot be underestimated and may make the difference between handling the incident properly and escalating to some higher level of damage.

5.3.4 Notification of Individuals

- Point of Contact (POC) people (Technical, Administrative, Response Teams, Investigative, Legal, Vendors, Service providers), and which POCs are visible to whom.
- Wider community (users).
- Other sites that might be affected.

Finally, there is the question of who should be notified during and after the incident. There are several classes of individuals that need to be considered for notification. These are the technical personnel, administration, appropriate response teams (such as CERT or CIAC), law enforcement, vendors, and other service providers. These issues are important for the central point of contact, since that is the person responsible for the actual notification of others (see section 5.3.6 for further information). A list of people in each of these categories is an important time saver for the POC during an incident. It is much more difficult to find an appropriate person during an incident when many urgent events are ongoing.

In addition to the people responsible for handling part of the incident, there may be other sites affected by the incident (or perhaps simply at risk from the incident). A wider community of users may also benefit from knowledge of the incident. Often, a report of the incident once it is closed out is appropriate for publication to the wider user community.

5.3.5 Public Relations - Press Releases

One of the most important issues to consider is when, who, and how much to release to the general public through the press. There are many issues to consider when deciding this particular issue. First and foremost, if a public relations office exists for the site, it is important to use this office as liaison to the press. The public relations office is trained in the type and wording of information released, and will help to assure that the image of the site is protected during and after the incident (if possible). A public relations office has the advantage that you can communicate candidly with them, and provide a buffer between the constant press attention and the need of the POC to maintain control over the incident.

If a public relations office is not available, the information released to the press must be carefully considered. If the information is sensitive, it may be advantageous to provide only minimal or overview information to the press. It is quite possible that any information provided to the press will be quickly reviewed by the perpetrator of the incident. As a contrast to this consideration, it was discussed above that misleading the press can often backfire and cause more damage than releasing sensitive information.

While it is difficult to determine in advance what level of detail to provide to the press, some guidelines to keep in mind are:

- Keep the technical level of detail low. Detailed information about the incident may provide enough information for copy-cat events or even damage the site's ability to prosecute once the event is over.
- Keep the speculation out of press statements. Speculation of who is causing the incident or the motives are very likely to be in error and may cause an inflamed view of the incident.
- Work with law enforcement professionals to assure that evidence is protected. If prosecution is involved, assure that the evidence collected is not divulged to the press.
- Try not to be forced into a press interview before you are prepared. The popular press is famous for the "2am" interview, where the hope is to catch the interviewee off guard and obtain information otherwise not available.

- Do not allow the press attention to detract from the handling of the event. Always remember that the successful closure of an incident is of primary importance.

5.3.6 Who Needs to Get Involved?

There now exists a number of incident response teams (IRTs) such as the CERT and the CIAC. (See sections 3.9.7.3.1 and 3.9.7.3.4.) Teams exists for many major government agencies and large corporations. If such a team is available for your site, the notification of this team should be of primary importance during the early stages of an incident. These teams are responsible for coordinating computer security incidents over a range of sites and larger entities. Even if the incident is believed to be contained to a single site, it is possible that the information available through a response team could help in closing out the incident.

In setting up a site policy for incident handling, it may be desirable to create an incident handling team (IHT), much like those teams that already exist, that will be responsible for handling computer security incidents for the site (or organization). If such a team is created, it is essential that communication lines be opened between this team and other IHTs. Once an incident is under way, it is difficult to open a trusted dialogue between other IHTs if none has existed before.

5.4 Response

A major topic still untouched here is how to actually respond to an event. The response to an event will fall into the general categories of containment, eradication, recovery, and follow-up.

Containment

The purpose of containment is to limit the extent of an attack. For example, it is important to limit the spread of a worm attack on a network as quickly as possible. An essential part of containment is decision making (i.e., determining whether to shut a system down, to disconnect from a network, to monitor system or network activity, to set traps, to disable functions such as remote file transfer on a UNIX system, etc.). Sometimes this decision is trivial; shut the system down if the system is classified or sensitive, or if proprietary information is at risk! In other cases, it is worthwhile to risk having some damage to the system if keeping the system up might enable you to identify an intruder.

The third stage, containment, should involve carrying out predetermined procedures. Your organization or site should, for example, define acceptable risks in dealing with an incident, and should prescribe specific actions and strategies accordingly. Finally, notification of cognizant authorities should occur during this stage.

Eradication

Once an incident has been detected, it is important to first think about containing the incident. Once the incident has been contained, it is now time to eradicate the cause. Software may be available to help you in this effort. For example, eradication software is available to eliminate most viruses which infect small systems. If any bogus files have been created, it is time to delete them at this point. In the case of virus infections, it is important to clean and reformat any disks containing infected files. Finally, ensure that all backups are clean. Many systems infected with viruses become periodically reinfected simply because people do not systematically eradicate the virus from backups.

Recovery

Once the cause of an incident has been eradicated, the recovery phase defines the next stage of action. The goal of recovery is to return the system to normal. In the case of a network-based attack, it is important to install patches for any operating system vulnerability which was exploited.

Follow-up

One of the most important stages of responding to incidents is also the most often omitted—the follow-up stage. This stage is important because it helps those involved in handling the incident develop a set of "lessons learned" (see section 6.3) to improve future performance in such situations. This stage also provides information which justifies an organization's computer security effort to management, and yields information which may be essential in legal proceedings.

The most important element of the follow-up stage is performing a postmortem analysis. Exactly what happened, and at what times? How well did the staff involved with the incident perform? What kind of information did the staff need quickly, and how could they have gotten that information as soon as possible? What would the staff do differently next time? A follow-up report is valuable because it provides a reference to be used in case of other similar incidents. Creating a formal chronology of events (including time stamps) is also important for legal reasons. Similarly, it is also important to as quickly obtain a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth. This estimate may become the basis for subsequent prosecution activity by the FBI, the U.S. Attorney General's Office, etc..

5.4.1 What Will You Do?

- Restore control.
- Relation to policy.
- Which level of service is needed?
- Monitor activity.
- Constrain or shut down system.

5.4.2 Consider Designating a "Single Point of Contact"

When an incident is under way, a major issue is deciding who is in charge of coordinating the activity of the multitude of players. A major mistake that can be made is to have a number of "points of contact" (POC) that are not pulling their efforts together. This will only add to the confusion of the event, and will probably lead to additional confusion and wasted or ineffective effort.

The single point of contact may or may not be the person "in charge" of the incident. There are two distinct rolls to fill when deciding who shall be the point of contact and the person in charge of the incident. The person in charge will make decisions as to the interpretation of policy applied to the event. The responsibility for the handling of the event falls onto this person. In contrast, the point of contact must coordinate the effort of all the parties involved with handling the event.

The point of contact must be a person with the technical expertise to successfully coordinate the effort of the system managers and users involved in monitoring and reacting to the attack. Often the management structure of a site is such that the administrator of a set of resources is not a technically competent person with regard to handling the details of the operations of the computers, but is ultimately responsible for the use of these resources.

Another important function of the POC is to maintain contact with law enforcement and other external agencies (such as the CIA, DoD, U.S. Army, or others) to assure that multi-agency involvement occurs.

Finally, if legal action in the form of prosecution is involved, the POC may be able to speak for the site in court. The alternative is to have multiple witnesses that will be hard to coordinate in a legal sense, and will weaken any case against the attackers. A single POC may also be the single person in charge of evidence collected, which will keep the number of people accounting for evidence to a minimum. As a rule of thumb, the more people that touch a potential piece of evidence, the greater the possibility that it will be inadmissible in court. The section below (Legal/Investigative) will provide more details for consideration on this topic.

5.5 Legal/Investigative

5.5.1 Establishing Contacts with Investigative Agencies

It is important to establish contacts with personnel from investigative agencies such as the FBI and Secret Service as soon as possible, for several reasons. Local law enforcement and local security offices or campus police organizations should also be informed when appropriate. A primary reason is that once a major attack is in progress, there is little time to call various personnel in these agencies to determine exactly who the correct point of contact is. Another reason is that it is important to cooperate with these agencies in a manner that will foster a good working relationship, and that will be in accordance with the working procedures of these agencies. Knowing the working procedures in advance and the expectations of your point of contact is a big step in this direction. For example, it is important to gather evidence that will be admissible in a court of law. If you don't know in advance how to gather admissible evidence, your efforts to collect evidence during an incident are likely to be of no value to the investigative agency with which you deal. A final reason for establishing contacts as soon as possible is that it is impossible to know the particular agency that will assume jurisdiction in any given incident. Making contacts and finding the proper channels early will make responding to an incident go considerably more smoothly.

If your organization or site has a legal counsel, you need to notify this office soon after you learn that an incident is in progress. At a minimum, your legal counsel needs to be involved to protect the legal and financial interests of your site or organization. There are many legal and practical issues, a few of which are:

1. Whether your site or organization is willing to risk negative publicity or exposure to cooperate with legal prosecution efforts.
2. Downstream liability—if you leave a compromised system as is so it can be monitored and another computer is damaged because the attack originated from your system, your site or organization may be liable for damages incurred.
3. Distribution of information—if your site or organization distributes information about an attack in which another site or organization may be involved or the vulnerability in a product that may affect ability to market that product, your site or

organization may again be liable for any damages (including damage of reputation).

4. Liabilities due to monitoring—your site or organization may be sued if users at your site or elsewhere discover that your site is monitoring account activity without informing users.

Unfortunately, there are no clear precedents yet on the liabilities or responsibilities of organizations involved in a security incident or who might be involved in supporting an investigative effort. Investigators will often encourage organizations to help trace and monitor intruders — indeed, most investigators cannot pursue computer intrusions without extensive support from the organizations involved. However, investigators cannot provide protection from liability claims, and these kinds of efforts may drag out for months and may take lots of effort.

On the other side, an organization's legal council may advise extreme caution and suggest that tracing activities be halted and an intruder shut out of the system. This in itself may not provide protection from liability, and may prevent investigators from identifying anyone.

The balance between supporting investigative activity and limiting liability is tricky; you'll need to consider the advice of your council and the damage the intruder is causing (if any) in making your decision about what to do during any particular incident.

Your legal counsel should also be involved in any decision to contact investigative agencies when an incident occurs at your site. The decision to coordinate efforts with investigative agencies is most properly that of your site or organization.

Involving your legal counsel will also foster the multi-level coordination between your site and the particular investigative agency involved which in turn results in an efficient division of labor. Another result is that you are likely to obtain guidance that will help you avoid future legal mistakes.

Finally, your legal counsel should evaluate your site's written procedures for responding to incidents. It is essential to obtain a "clean bill of health" from a legal perspective before you actually carry out these procedures.

5.5.2 Formal and Informal Legal Procedures

One of the most important considerations in dealing with investigative agencies is verifying that the person who calls asking for information is a legitimate representative from the agency in question. Unfortunately, many well intentioned people have unknowingly leaked sensitive information about incidents, allowed unauthorized people into their systems, etc., because a caller has masqueraded as an FBI or Secret Service agent. A similar consideration is using a secure means of communication. Because many network attackers can easily reroute electronic mail, avoid using electronic mail to communicate with other agencies (as well as others dealing with the incident at hand). Non-secured phone lines (e.g., the phones normally used in the business world) are also frequent targets for tapping by network intruders, so be careful!

There is no established set of rules for responding to an incident when the U.S. Federal Government becomes involved. Except by court order, no agency can force you to monitor, to disconnect from the network, to avoid telephone contact with the suspected attackers, etc.. As discussed in section 5.5.1, you should consult the matter with your legal counsel, especially before taking an action that your organization has never taken. The particular agency involved may ask you to leave an attacked machine on and to monitor activity on this machine, for example. Your complying with this request will ensure continued cooperation of the agency—usually the best route towards finding the source of the network attacks and, ultimately, terminating these attacks. Additionally, you may need some information or a favor from the agency involved in the incident. You are likely to get what you need only if you have been cooperative. Of particular importance is avoiding unnecessary or unauthorized disclosure of information about the incident, including any information furnished by the agency involved. The trust between your site and the agency hinges upon your ability to avoid compromising the case the agency will build; keeping "tight lipped" is imperative.

Sometimes your needs and the needs of an investigative agency will differ. Your site may want to get back to normal business by closing an attack route, but the investigative agency may want you to keep this route open. Similarly, your site may want to close a compromised system down to avoid the possibility of negative publicity, but again the investigative agency may want you to continue monitoring. When there is such a conflict, there may be a complex set of tradeoffs (e.g., interests of your site's management, amount of resources you can devote to the problem, jurisdictional boundaries, etc.). An important guiding principle is related to what might be called "Internet citizenship" [22, IAB89, 23] and its responsibilities. Your site can shut a system down, and this will relieve you of the stress, resource demands, and danger of negative exposure. The attacker, however, is likely to simply move on to another system, temporarily leaving others blind to the attacker's intention and actions until another path of attack can be detected. Providing that there is no damage to your systems and others, the most responsible course of action is to cooperate with the participating agency by leaving your compromised system on. This will allow monitoring (and, ultimately, the possibility of terminating the source of the threat to systems just like yours). On the other hand, if there is damage to computers illegally accessed through your system, the choice is more complicated: shutting down the intruder may prevent further damage to systems, but might make it impossible to track down the intruder. If there has been damage, the decision about whether it is important to leave systems up to catch the intruder should involve all the organizations effected. Further complicating the issue of network responsibility is the consideration that if you do not cooperate with the agency involved, you will be less likely to receive help from that agency in the future.

5.6 Documentation Logs

When you respond to an incident, document all details related to the incident. This will provide valuable information to yourself and others as you try to unravel the course of events. Documenting all details will ultimately save you time. If you don't document every relevant phone call, for example, you are likely to forget a good portion of information you obtain, requiring you to contact the source of information once again. This wastes yours and others' time, something you can ill afford. At the same time, recording details will provide evidence for prosecution efforts, providing the case moves in this direction. Documenting an incident also will help you perform a final assessment of damage (something your management as well as law enforcement officers will want to know), and will provide the basis for a follow-up analysis in which you can engage in a valuable "lessons learned" exercise.

During the initial stages of an incident, it is often infeasible to determine whether prosecution is viable, so you should document as if you are gathering evidence for a court case. At a minimum, you should record:

- All system events (audit records).
- All actions you take (time tagged).
- All phone conversations (including the person with whom you talked, the date and time, and the content of the conversation).

The most straightforward way to maintain documentation is keeping a log book. This allows you to go to a centralized, chronological source of information when you need it, instead of requiring you to page through individual sheets of paper. Much of this information is potential evidence in a court of law. Thus, when you initially suspect that an incident will result in prosecution or when an investigative agency becomes involved, you need to regularly (e.g., every day) turn in photocopied, signed copies of your logbook (as well as media you use to record system events) to a document custodian who can store these copied pages in a secure place (e.g., a safe). When you submit information for storage, you should in return receive a signed, dated receipt from the document custodian. Failure to observe these procedures can result in invalidation of any evidence you obtain in a court of law.

6. Establishing Post-Incident Procedures

6.1 Overview

In the wake of an incident, several actions should take place. These actions can be summarized as follows:

1. An inventory should be taken of the systems' assets, i.e., a careful examination should determine how the system was affected by the incident,
2. The lessons learned as a result of the incident should be included in revised security plan to prevent the incident from re-occurring,
3. A new risk analysis should be developed in light of the incident,
4. An investigation and prosecution of the individuals who caused the incident should commence, if it is deemed desirable.

All four steps should provide feedback to the site security policy committee, leading to prompt re-evaluation and amendment of the current policy.

6.2 Removing Vulnerabilities

Removing all vulnerabilities once an incident has occurred is difficult. The key to removing vulnerabilities is knowledge and understanding of the breach. In some cases, it is prudent to remove all access or functionality as soon as possible, and then restore normal operation in limited stages. Bear in mind that removing all access while an incident is in progress will obviously notify all users, including the alleged problem users, that the administrators are aware of a problem; this may have a deleterious effect on an investigation. However, allowing an incident to continue may also open the likelihood of greater damage, loss, aggravation, or liability (civil or criminal).

If it is determined that the breach occurred due to a flaw in the systems' hardware or software, the vendor (or supplier) and the CERT should be notified as soon as possible. Including relevant telephone numbers (also electronic mail addresses and fax numbers) in the site security policy is strongly recommended. To aid prompt acknowledgment and understanding of the problem, the flaw should be described in as much detail as possible, including details about how to exploit the flaw.

As soon as the breach has occurred, the entire system and all its components should be considered suspect. System software is the most probable target. Preparation is key to recovering from a possibly tainted system. This includes checksumming all tapes from the vendor using a checksum algorithm which (hopefully) is resistant to tampering [10]. (See sections 3.9.4.1, 3.9.4.2.) Assuming original vendor distribution tapes are available, an analysis of all system files should commence, and any irregularities should be noted and referred to all parties involved in handling the incident. It can be very difficult, in some cases, to decide which backup tapes to recover from; consider that the incident may have continued for months or years before discovery, and that the suspect may be an employee of the site, or otherwise have intimate knowledge or access to the systems. In all cases, the pre-incident preparation will determine what recovery is possible. At worst-case, restoration from the original manufactures' media and a re-installation of the systems will be the most prudent solution.

Review the lessons learned from the incident and always update the policy and procedures to reflect changes necessitated by the incident.

6.2.1 Assessing Damage

Before cleanup can begin, the actual system damage must be discerned. This can be quite time consuming, but should lead into some of the insight as to the nature of the incident, and aid investigation and prosecution. It is best to compare previous backups or original tapes when possible; advance preparation is the key. If the system supports centralized logging (most do), go back over the logs and look for abnormalities. If process accounting and connect time accounting is enabled, look for patterns of system usage. To a lesser extent, disk usage may shed light on the incident. Accounting can provide much helpful information in an analysis of an incident and subsequent prosecution.

6.2.2 Cleanup

Once the damage has been assessed, it is necessary to develop a plan for system cleanup. In general, bringing up services in the order of demand to allow a minimum of user inconvenience is the best practice. Understand that the proper recovery procedures for the system are extremely important and should be specific to the site.

It may be necessary to go back to the original distributed tapes and recustomize the system. To facilitate this worst case scenario, a record of the original systems setup and each customization change should be kept current with each change to the system.

6.2.3 Follow up

Once you believe that a system has been restored to a "safe" state, it is still possible that holes and even traps could be lurking in the system. In the follow-up stage, the system should be monitored for items that may have been missed during the cleanup stage. It would be prudent to utilize some of the tools mentioned in section 3.9.8.2 (e.g., COPS) as a start. Remember, these tools don't replace continual system monitoring and good systems administration procedures.

6.2.4 Keep a Security Log

As discussed in section 5.6, a security log can be most valuable during this phase of removing vulnerabilities. There are two considerations here; the first is to keep logs of the procedures that have been used to make the system secure again. This should include command procedures (e.g., shell scripts) that can be run on a periodic basis to recheck the security. Second, keep logs of important system events. These can be referenced when trying to determine the extent of the damage of a given incident.

6.3 Capturing Lessons Learned

6.3.1 Understand the Lesson

After an incident, it is prudent to write a report describing the incident, method of discovery, correction procedure, monitoring procedure, and a summary of lesson learned. This will aid in the clear understanding of the problem. Remember, it is difficult to learn from an incident if you don't understand the source.

6.3.2 Resources

6.3.2.1 Other Security Devices, Methods

Security is a dynamic, not static process. Sites are dependent on the nature of security available at each site, and the array of devices and methods that will help promote security. Keeping up with the security area of the computer industry and their methods will assure a security manager of taking advantage of the latest technology.

6.3.2.2 Repository of Books, Lists, Information Sources

Keep an on site collection of books, lists, information sources, etc., as guides and references for securing the system. Keep this collection up to date. Remember, as systems change, so do security methods and problems.

6.3.2.3 Form a Subgroup

Form a subgroup of system administration personnel that will be the core security staff. This will allow discussions of security problems and multiple views of the site's security issues. This subgroup can also act to develop the site security policy and make suggested changes as necessary to ensure site security.

6.4 Upgrading Policies and Procedures

6.4.1 Establish Mechanisms for Updating Policies, Procedures, and Tools

If an incident is based on poor policy, and unless the policy is changed, then one is doomed to repeat the past. Once a site has recovered from and incident, site policy and procedures should be reviewed to encompass changes to prevent similar incidents. Even without an incident, it would be prudent to review policies and procedures on a regular basis. Reviews are imperative due to today's changing computing environments.

6.4.2 Problem Reporting Procedures

A problem reporting procedure should be implemented to describe, in detail, the incident and the solutions to the incident. Each incident should be reviewed by the site security subgroup to allow understanding of the incident with possible suggestions to the site policy and procedures.

7. References

[1] Quarterman, J., "The Matrix: Computer Networks and Conferencing Systems Worldwide", Pg. 278, Digital Press, Bedford, MA, 1990.

[2] Brand, R., "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery", R. Brand, available on-line from: cert.sei.cmu.edu:/pub/info/
primer, 8 June 1990.

[3] Fites, M., Kratz, P. and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.

[4] Johnson, D., and J. Podesta, "Formulating a Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems", Available from: The Electronic Mail Association (EMA) 1555 Wilson Blvd, Suite 555, Arlington VA 22209, (703) 522-7111, 22 October 1990.

[5] Curry, D., "Improving the Security of Your UNIX System", SRI International Report ITSTD-721-FR-90-21, April 1990.

[6] Cheswick, B., "The Design of a Secure Internet Gateway", Proceedings of the Summer Usenix Conference, Anaheim, CA, June 1990.

[7] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures", RFC 1113, IAB Privacy Task Force, August 1989.

[8] Kent, S., and J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part II — Certificate-Based Key Management", RFC 1114, IAB Privacy Task Force, August 1989.

[9] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part III — Algorithms, Modes, and Identifiers", RFC 1115, IAB Privacy Task Force, August 1989.

[10] Merkle, R., "A Fast Software One Way Hash Function", Journal of Cryptology, Vol. 3, No. 1.

[11] Postel, J., "Internet Protocol - DARPA Internet Program Protocol Specification", RFC 791, DARPA, September 1981.

[12] Postel, J., "Transmission Control Protocol - DARPA Internet Program Protocol Specification", RFC 793, DARPA, September 1981.

[13] Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, 28 August 1980.

[14] Mogul, J., "Simple and Flexible Datagram Access Controls for UNIX-based Gateways", Digital Western Research Laboratory Research Report 89/4, March 1989.

[15] Bellovin, S., and M. Merritt, "Limitations of the Kerberos Authentication System", Computer Communications Review, October 1990.

[16] Pfleeger, C., "Security in Computing", Prentice-Hall, Englewood Cliffs, N.J., 1989.

[17] Parker, D., Swope, S., and B. Baker, "Ethical Conflicts: Information and Computer Science, Technology and Business", QED Information Sciences, Inc., Wellesley, MA.

[18] Forester, T., and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990.

[19] Postel, J., and J. Reynolds, "Telnet Protocol Specification", RFC 854, USC/Information Sciences Institute, May 1983.

[20] Postel, J., and J. Reynolds, "File Transfer Protocol", RFC 959, USC/Information Sciences Institute, October 1985.

[21] Postel, J., Editor, "IAB Official Protocol Standards", RFC 1200, IAB, April 1991.

[22] Internet Activities Board, "Ethics and the Internet", RFC 1087, Internet Activities Board, January 1989.

[23] Pethia, R., Crocker, S., and B. Fraser, "Policy Guidelines for the Secure Operation of the Internet", CERT, TIS, CERT, RFC in preparation.

[24] Computer Emergency Response Team (CERT/CC), "Unauthorized Password Change Requests", CERT Advisory CA-91:03, April 1991.

[25] Computer Emergency Response Team (CERT/CC), "TELNET Breakin Warning", CERT Advisory CA-89:03, August 1989.

[26] CCITT, Recommendation X.509, "The Directory: Authentication Framework", Annex C.

[27] Farmer, D., and E. Spafford, "The COPS Security Checker System", Proceedings of the Summer 1990 USENIX Conference, Anaheim, CA, Pgs. 165-170, June 1990.

8. Annotated Bibliography

(Editors Note: This section has been deleted in this reprint due to outdatedness.)

9. Acknowledgments

Thanks to the SSPHWG's illustrious "Outline Squad", who assembled at USC/Information Sciences Institute on 12-June-90: Ray Bates (ISI), Frank Byrum (DEC), Michael A. Contino (PSU), Dave Dalva (Trusted Information Systems, Inc.), Jim Duncan (Penn State Math Department), Bruce Hamilton (Xerox), Sean Kirkpatrick (Unisys), Tom Longstaff (CIAC/LLNL), Fred Ostapik (SRI/NIC), Keith Pilotti (SAIC), and Bjorn Satdeva (/sys/admin, inc.).

Many thanks to Rich Pethia and the Computer Emergency Response Team (CERT); much of the work by Paul Holbrook was done while he was working for CERT. Rich also provided a very thorough review of this document. Thanks also to Jon Postel and USC/Information Sciences Institute for contributing facilities and moral support to this effort.
Last, but NOT least, we would like to thank members of the SSPHWG and Friends for their additional contributions: Vint Cerf (CNRI), Dave Grisham (UNM), Nancy Lee Kirkpatrick (Typist Extraordinaire), Chris McDonald (WSMR), H. Craig McKee (Mitre), Gene Spafford (Purdue), and Aileen Yuan (Mitre).

10.Security Considerations

If security considerations had not been so widely ignored in the Internet, this memo would not have been possible.

11. Authors' Addresses

J. Paul Holbrook CICNet, Inc.
2901 Hubbard
Ann Arbor, MI 48105
Phone: (313) 998-7680
EMail: holbrook@cic.net

Joyce K. Reynolds University of Southern California
Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292
Phone: (213) 822-1511
EMail: JKREY@ISI.EDU

0

Information Security Resources

Accounting

Academy of Accounting Historians

Site of a non-profit organization dedicated to the history of accounting and auditing and its relation to past and current business practices. Provides links to other accounting and business history sites.

URL http://weatherhead.cwru.edu/Accounting/

ACCHANGE

Subscription mailing list for public accountants, industry professionals, and academics on accounting education and curriculum.

Subscribe through: listserv@mcmuse.mc.maricopa.edu

Accountant's Home Page

A collection of links to sites of interest to professionals in the fields of accounting, finance, and business. Among the links provided are Thomas, Internal Revenue Service, and Small Business Administration.

URL http://www.computercpa.com/

Accounting, Auditing & Accountability (journal)

URL http://www.mcb.co.uk/liblink/aaaj/jourhome.htm

Accounting Firms

- Robert C. Alario, CPA
  - URL http://www.cyber-cpa.com/ma01.html
- Alder, Green & Hansson
  - URL http://www.aghcpa.com/
- C.W. Amos & Company, LLC
  - URL http://www.cwamos.com
- Arthur Andersen & Co., SC
  - URL http://www.arthurandersen.com/
- Andersen Consulting
  - URL http://www.ac.com/
- Michael M. Arons, CPA
  - URL http://www.olac.com/arons/
- Aronson, Fetridge & Weigle, CPAs
  - URL http://www.afwcpa.com
- Karen Hope Bachman, CPA
  - URL http://www.summitmedia.com/cpa/
- Patricia Bagley, CPA, PC
  - URL http://www.digex.net/herndon/biz/bagley.html
- Charles Bailly & Company, P.L.L.P.
  - URL http://www.cbailly.com
- Baker Newman & Noyes
  - URL http://www.bnncpa.com/
- Barnes, Welding, Cook & O'Connor, Inc., CPAs
  - URL http://www.multiverse.com/bwco/
- Gregory Barsanti, CPA
  - URL http://www.sover.net/%7Epjarvis/barsanti.html
- BDO Dunwoody (Canada)
  - URL http://www.bdo.ca/
- Al Beane, CPA
  - URL http://community.net/community/solano/business/albeane.html
- Berenson & Co.
  - URL http://www.berenson.com

Klaus Beyer

URL http://www.beyer-steuerberater.de/english.html

David M. Bialick, CPA

URL http://www.earthlink.net/dbialick

Big Apple CPA and Consulting Firm-Glickman, Rubin & Gaft

URL http://www.dewittplaza.com/Apple/main.htm

Blackman Kallick & Bartelstein, LLP

URL http://www.bkbcpa.com

Blanchet CPA

URL http://pbn.net:80/pbn/referalls/accountants/blanchet.htm

Joshua A. Blau, CPA

URL http://www.tagsys.com/Ads/Accountant/accountant.html

Fred Blauer and Associates, CPAs (Canada)

URL http://www.cam.org/%7Efblauer/serv_bus.htm

Bober, Markey & Company

URL http://www.bobermarkey.com

James Bones & Associates

URL http://calproptax.com/

Bonham & Co., CPAs

URL http://www.ice.net/private/bonham/bonham.html

Brief, Rotfarb, Wynbarg, Cappe

URL http://www.brwc.com

Karen Stevenson Brown, CPA

URL http://www.ice.net/~kstevens/

Jack D. Burson, CPA

URL http://www.olac.com/

John Butler, CPA

URL http://www.aros.net/~jbutler/

Paul Bryne & Co. (Ireland)

URL http://gate1.internet-eireann.ie/proll/byrne

Burkhardt & Co.

URL http://www.cinti.net/burkhardt

Caldwell & Bodenheimer
URL http://www.covesoft.com/caldwell/
Chapski & Chapski, CPAs, LLP
URL http://www.umich.edu/%7Echapski/
Checkers, Simon & Rosner
URL http://www.checkers-llp.com/
Choquette & Co. (Canada)
URL http://www.income.com/
Clark, Schaefer, Hackett & Co.
URL http://www.cshco.com
Paul Clough, CPA
URL http://www.turbosales.com/~turbos/paulc/
Eric E. Cohen, CPA, CPIM
URL http://www.servtech.com/re/acct.html
Cohen & Co.
URL http://www.cohencpa.com/
Cohen, Greenstein and Company
URL http://world.std.com/~harvey
Coopers & Lybrand
URL http://www.CoLybrand.com/
Coopers & Lybrand (United Kingdom)
URL http://www.coopers.co.uk/welcome.html
Coughlin & Gomola, CPAs
URL http://www.connix.com/~garyg/
Kathy K. Cregan, CPA
URL http://www.av.qnet.com/%7Ekkc/
Hillary L. Crosby, CPA
URL http://www.hlca.com/hlca/
Dworetsky & Co., CPAs
URL http://www.vvmi.com/dworetsky.html
DeLellis & Co., CPA
URL http://www.vcnet.com/DeLellis/
Deloitte & Touche
URL http://www.dttus.com/

Deloitte & Touche (Bermuda)
URL http://turnpike.net//emporium/D/dtpage1/index.html
Elder & Associates
URL http://www.elder-assoc-cpa.com
English Miller & Co.
URL http://ourworld.compuserve.com/homepages/
EnglishMiller
Ernst & Young
URL http://www.ey.com/
R.A. Fischler & Co.
URL http://www.rafcpa.com
Howard Fisherman, CPA
URL http://www.specdata.com/hfcpa/
Forsyth Financial Services, Management Accountants
URL http://www.sentex.net/~ffs/
Freed Maxick Sachs & Murphy, PC
URL http://www.fmsmpc.com
Friedman & Fuller, PC, CPAs
URL http://www.ffgroup.com/
Friedman Kannenberg & Associates, CPAs
URL http://www.csi-infinet.com/friedman.htm
GBQ/Nesser Consulting Group, Ltd.
URL http://www.iwaynet.net/~nesser
Paula Gilles Maurano & Com, CPAs
URL http://www.maurano.com/
Roxanne Goldberg, CPA
URL http://www.telesphere.com/ts/rgcpa/index.html
Goldstein Golub Kessler & Company, PC
URL http://www.ggk.com/
Grant Thornton LLP
URL http://www.gt-us.com/
Dan Gray, CPA
URL http://www.netquest.net/gary.adams

Grobstein, Horwath and Company, LLP
URL http://www.horwathcal.com

Sallie A. Hagen, CPA, PC
URL http://www.netcpa.com

Earl Hall, CPA
URL http://www.wolfe.net/~earl/

Craig L. Hardison, CPA
URL http://www.iadfw.net/craig/index.html

Hargrave & Hargrave, CPA
URL http://taxwizard.com/

John K. Haslock, CPA
URL http://www.cyberzine.org/html/CPA/cpapage.html

Haugen, Springer & Co.
URL http://www.hsco.com

Hayes & Associates, CPAs
URL http://www.hayescpa.com

Hayes, Debeck, Stewart & Little, CAs (Canada)
URL http://www.islandnet.com/~hdsl/hdsl.html

Hungerford, Alrin, Nichols & Carter, P.C.
URL http://www.hanc.com

Integrated Business Services, Ltd.
URL http://www.geocities.com/WallStreet/5895

Johnson and Scarborough, CPAs
URL http://www.jscpa.com/

Roger A. Kahan, CPA
URL http://www.rak-1.com/

Katz Cassidy, CPAs
URL http://www.primenet.com/~laig/proserve/cpa/cpa0001b.htm

Kidsons Impey (United Kingdom)
URL http://www.kidsons.co.uk/kidsons/hlb.html

Patrick Kissane, CA
URL http://www.taunet.net.au/pat/

Kostin, Ruffkess & Company, LLC
URL http://www.kostin.com/
KPMG Peat Marwick
URL http://hp.rad.kpmg.com/WWW/SSC/home.html
KPMG Peat Marwick (Canada)
URL http://www.kpmg.ca/
Kurtz & Kurtz, CPAs
URL http://www.mcny.com/kurzkurz/
Kushner, La Graize, and Moore, CPAs
URL http://www.communique.net/~klmcpa/
LaFollette, Jansa, Brandt & Co., LLP
URL http://www.ljbco.com
Barbara L. Leary, CPA
URL http://www1.magnus1.com/cta/b11/b11_home.html
Lindgren, Callihan, Van Osdol and Co., Ltd.
URL http://www.essex1.com/people/kappy/lcv.htm
Philip K. Lippincott, CPA
URL http://www.pkl-profit.com
Sherman L. Lubin, CPA
URL http://www.netrunner.net/~rhomer/sll.htm
V F Mather & Co.
URL http://www.personal.u-net.com/~mather/
Mathis, West, Huffines & Co., P.C.
URL http://www.mwhpc.com
Matthews, Reich, Perna & Rootermond, P.C.
URL http://www.mrpr.com
Ronnie C. McClure, CPA
URL http://rampages.onramp.net/~rmphdcpa/
McConnell Galloway Botteselle, CGAs (Canada)
URL http://www.helinet.com/MGB/
McGladrey & Pullen - Renaissance Consulting Division
URL http://www.mcgladrey.com
McNulty & Co., CPAs
URL http://www.review.net/cpa/

Raymond Miner, CPA
URL http://www.onramp.net/%7Efneworld/networking.html
Anne Mitchell, CPA
URL http://slv.net/taxprep/cpa1/mitchell.htm
Mithcell, Emert & Hill, P.C. (Knoxville, TN)
URL http://www.mehcpa.com
Alan Moore, CPA
URL http://www.infi.net/moore/
Moore Stephens North America, LLC
URL http://www.msnainc.com/
Morrison Brown Argiz & Company
URL http://www.shadow.net/mba/
Murphy Green & Co.
URL http://www.mcn.org/A/MGCO/
Arthur Naman, CPA
URL http://www.ccsi.com/~anaman/
Jerry Newman, CPA
URL http://www.5010geary.com/frisco/frisco.htm
Peter Norton, CPA
URL http://www.corpinfohub.com/norton.htm
Ormsby & Mackan (Toronto)
URL http://www.io.org/%7Efmackan/
Obara, Kidwell & Company
URL http://users.aol.com/okc250/homepage.htm
Charles J. Ozeck, CPA
URL http://www.dprint.com/cocpa/
Parks, Palmer, Turner & Yemenidjian, CPA
URL http://www.laig.com/proserve/ppty/
People-Friendly Business Solutions
(Penelope BM Hedges, CA, CSV) (Canada)
URL http://mindlink.net/Penelope_Hedges/pfbs-1.htm
Pester & Co.
URL http://www.taxcpa.com

Pielech & Pielech, CPAs
URL http://www.pielech.com
Presnell Gage Accounting & Consulting
URL http://www.presnellgage.com
Price Waterhouse
URL http://www.pw.com/
Price Waterhouse - Montreal (French language)
URL http://services.bunyip.com:7101/default.html
Read & Bose, CPAs
URL http://www.oregontrail.net/readbose/peer.html
Richman Associates, CPAs
URL http://www.websys.com/richman/home.html
Peter Jason Riley, CPA
URL http://www.pjrcpa.com
Rogers & Co., CPAs, PC
URL http://www.exempt5.com
Micheal A. Ross, CPA
URL http://rampages.onramp.net/~bizplan/
Rowrotham & Company, Inc., CPAs
URL http://www.slip.net/~cpas/
Edward Ryan and Co, CAs (England)
URL http://www.edward-ryan.co.uk
Andrew Sadowski, CPA
URL http://business.poland.net/sadowski/
Sareen & Associates
URL http://www.sareen-assoc.com
Hugo Schouten, CPA (Australia)
URL http://www.ozemail.com.au/~dutch/
Walter C. Schmidt, CPA
URL http://www.dorsai.org/%7Ewalts/index.html
Seager, Seager, Webb, Inc.
URL http://www.sswinc.com/
Carolyn Sechler, CPA
URL http://www.indirect.com/www/carolyn/

Second Shift, Inc.
URL http://www.accounting.com/%7Ercahill/ssftcpa.htm
BDO Seidman, LLP (US member firm)
URL http://www.bdo.com
Simpson & Osborne, CPAs
URL http://www.sandocpas.com/
Bradford L. Smith, CPA
URL http://worldmall.com/msti/bsmith.htm
Donald A. Smith, CPA
URL http://ids.net/%7Edsmith/mtb.html
David Somers & Associates, CPAs
URL http://web2.airmail.com/%7Edsacpa/mainpage.htm
Spaeth & Batterberry, Ltd.
URL http://sabltd.com
Swarts & Co., CPA
URL http://www.internex.com/multipresence/swarts.html
Schwartz, Cohen & Co.
URL http://www.azcpa.com/
Tax Advice, Inc. - Virgil E. Knedlik, CPA
URL http://www.theworld.com/money/taxes/ta/ta.htm
The PC CPA (tm)
URL http://pages.prodigy.com/apc_cpa/
Thomas, Doll & Co., CPAs
URL http://www.ispot.com/TDC/
Thomas & Walters, CPAs
URL http://slv.net/taxprep/cpa1/thomas.htm
Thompson, Greenspon & Co.
URL http://www.tgccpa.com
Urbach Kahn & Werlin PC, CPAs
URL http://www.ukw.com
Varney, Mills, Rogers, Burnett & Associates
URL http://www.varney.com/
Kathleen Villard, CPA
URL http://www.teknetix.com/v.html

Virchow, Krause, & Company, LLP
URL http://www.virchowkrause.com
James A. Volz, CPA
URL http://home.sprynet.com/sprynet/volzcpa
White & Associates, CPAs
URL http://www.whiteassoc.com/%7Eleewhite/homepage.html
Wiener, Strickler & Perez, PC
URL http://members.aol.com/wsandp/

Accounting News Network

A databank for accountants and tax practitioners. Features include the "Accountant's Calendar," a listing of industry events and tax deadlines; "Issue of the Week," and "Accountant's Productivity Tools," which offers demos of new technologies. The site is a joint venture of Microsoft and Faulkner & Gray.

URL http://www.microsoft.com/smallbiz/ann

AI/ES Section of AAA (Artificial Intelligence/Expert Systems Section of the American Accounting Association)

Provides links to scholarly research in the accounting field including teaching materials and the International Journal of Intelligent Systems in Accounting, Finance and Management.

URL http://www.bus.orst.edu:80/faculty/brownc/aies/aieshome.htm

American Accounting Association Home Page

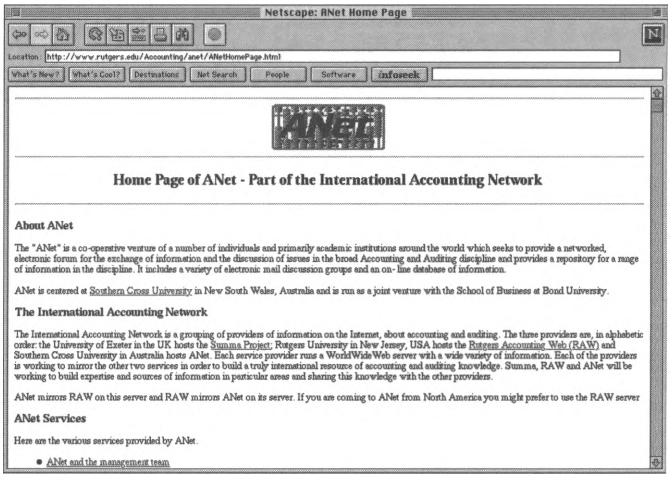
Provides general information about the Association as well as useful links to Yahoo and other resources of particular interest to accounting professionals.

URL http://www.rutgers.edu:80/Accounting/raw/aaa/aaa.htm

ANet

One of three complementary sites of the International Accounting Network, which includes the Summa Project and Rutgers University sites. Hosted by Southern Cross University, ANet contains information on accounting and auditing software and new technology, a bibliography of online publications, and a listing of conferences.

URL http://www.rutgers.edu/Accounting/anet/



Home Page of ANet - Part of the International Accounting Network

About ANet

The "ANet" is a co-operative venture of a number of individuals and primarily academic institutions around the world which seeks to provide a networked, electronic forum for the exchange of information and the discussion of issues in the broad Accounting and Auditing discipline and provides a repository for a range of information in the discipline. It includes a variety of electronic mail discussion groups and an on- line database of information.

ANet is centered at Southern Cross University in New South Wales, Australia and is run as a joint venture with the School of Business at Bond University.

The International Accounting Network

The International Accounting Network is a grouping of providers of information on the Internet, about accounting and auditing. The three providers are, in alphabetic order: the University of Exeter in the UK hosts the Summa Project; Rutgers University in New Jersey, USA hosts the Rutgers Accounting Web (RAW) and Southern Cross University in Australia hosts ANet. Each service provider runs a WorldWideWeb server with a wide variety of information. Each of the providers is working to mirror the other two services in order to build a truly international resource of accounting and auditing knowledge. Summa, RAW and ANet will be working to build expertise and sources of information in particular areas and sharing this knowledge with the other providers.

ANet mirrors RAW on this server and RAW mirrors ANet on its server. If you are coming to ANet from North America you might prefer to use the RAW server

ANet Services

Here are the various services provided by ANet.

- ANet and the management team

ANet mailing lists include:

ANews-L - News

AAAES-L - American Accounting Association AI/ES Section Newsletter

AAATC-L - American Accounting Association Teaching and Curriculum Section Newsletter

AAcrdn-L - Accounting Program Accreditation

AAccSys-L - Accounting Information Systems

AAudit-L - Auditing

ABooks-L - New Books

AEthics-L - Ethics

AEthnog-L - Accounting Ethnography

AFinAcc-L - Financial Accounting
AGvNFP-L - Governmental and Not-for-Profit Accounting
AIntAcc-L - International Accounting
AIntSys-L - Intelligent and Expert Systems
AJobs-L - Academic Positions
AMgtAcc-L - Management Accounting
AOilAcc-L - Extractive Industries
AProfsn-L - Academic/Profession Interface
ASocial-L - Social Accounting
AStdnt-L - Accounting Student List
ATax-L - Taxation
ATeach-L - Teaching and Learning
ATechno-L - Accounting and Technology
ATwoYear-L - U.S. Two-Year College System

Subscribe through email to Listproc@scu.edu.au with message: SUBSCRIBE listname yourname

Arthur Andersen

This site of the Big Six firm features "A Brief History of Accounting," an animated review of the industry which takes visitors from the first known transaction records in 3600 B.C. to modern times. Visitors must have Netscape *Navigator* and Macromedia *Shockwave,* both of which are available through links at the site.

URL http://www.arthurandersen.com/firmwide/new/

Bisk Publishing Co.

This site provides information about the education resources available for business law, accounting, and tax professionals. The site includes a demo of their CPE program, a catalog, state board of accountancy requirements, and other professional information.

URL http://www.bisk.com

California CPA's Education Foundation

A continuing education service for accountants. Contains information on seminars and CPE events and provides links to the "Electronic Accountant" Newswire service and CPE Exchange articles.

URL http://www.calcpaed.org

CPENet

Nonprofit Internet continuing education service for financial professionals, with course offerings that include Medicare Cost Reimbursement, Risk Assessment, and Audit of Advanced Systems among others.

URL http://uu-gna.mit.edu:8001/~compass/

Cyber-Accountant Forum

A discussion group for accountants who do business on the Web. Topics include career opportunities on the Internet, electronic marketing and consulting, and intranets.

URL http://www.lacher.com/cyber_accountant/

The Electronic Accountant

An e-zine published by Faulkner & Gray, this site is updated three times per day to offer the most recent industry news, features, and reviews of Web sites of interest to accountants. Also provides a list of discussion groups.

URL http://www.electronicaccountant.com

Enterprise 2000 and Network Press home page

A management and network organization serving the accounting profession. Users can order books and reports published by the Network Press, receive a catalog of Enterprise 2000 services, or participate in a discussion forum for CPAs. For information, email network@sam.neosoft.com.

URL http://www.NeoSoft.com/neopolis/e2000/

Financial Economics Network

Internet discussion group where subscribers exchange ideas and information through email on banking, accounting, stocks, bonds, corporate filings, etc.

Subscribe through email to listserv@wsuvm1.csc.wsu.edu with message: subscribe fen yourname

General Accounting Office of Policy's BBS

Provides resources for government auditors and GAO's Policy and Procedures Manual available for download.

Dial 202-512-4286 or access through FedWorld

Gleim Publications

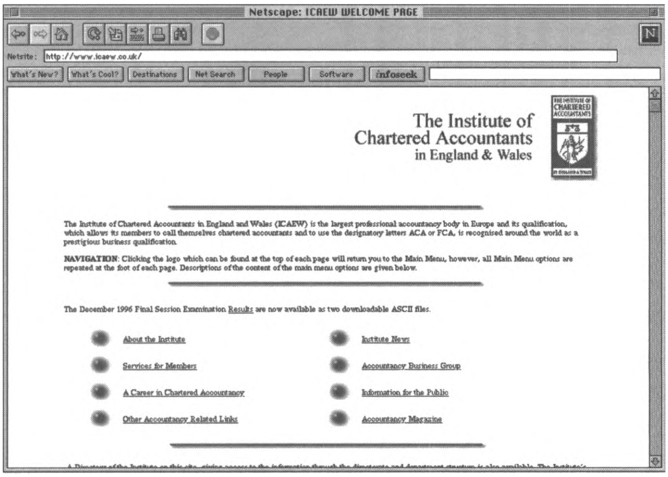
This site provides information about CPA, CIA, and CMA exams, how to pass the exams, and order forms for books and software.

URL http://www.gleim.com

ICAEW

Site maintained by the Institute of Chartered Accountants of England and Wales for its members and the worldwide accounting community. Includes links to many accounting-related sites and is the graphic-intensive counterpart of the Summa Project at the University of Exeter, which is primarily text based.

URL http://www.icaew.co.uk/



The Institute of
Chartered Accountants
in England & Wales

The Institute of Chartered Accountants in England and Wales (ICAEW) is the largest professional accountancy body in Europe and its qualification, which allows its members to call themselves chartered accountants and to use the designatory letters ACA or FCA, is recognised around the world as a prestigious business qualification.

NAVIGATION: Clicking the logo which can be found at the top of each page will return you to the Main Menu, however, all Main Menu options are repeated at the foot of each page. Descriptions of the content of the main menu options are given below.

The December 1996 Final Session Examination Results are now available as two downloadable ASCII files.

- About the Institute
- Services for Members
- A Career in Chartered Accountancy
- Other Accountancy Related Links
- Institute News
- Accountancy Business Group
- Information for the Public
- Accountancy Magazine

Institute of Management Accountants (IMA) Bulletin Board

Lists employment opportunities, new publications bibliographies, catalog of publications, CMA exam information, continuing education information, news, articles, and a research forum.

Dial 1-800-229-1268

K2 Enterprises

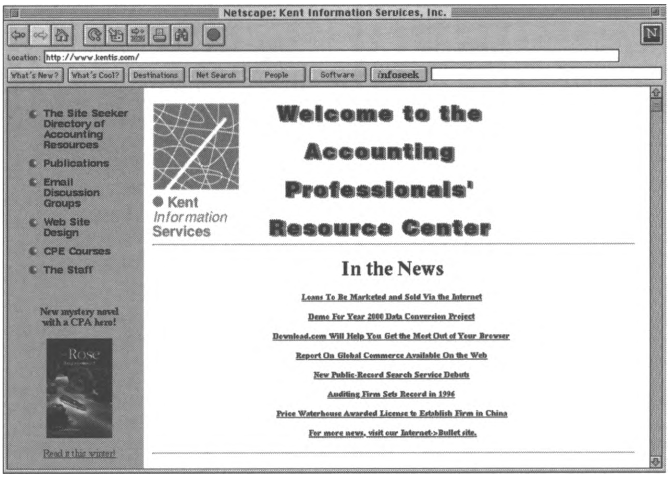
The K2 Enterprises home page is the contact point for information about K2 Enterprises' CPE seminars and conferences. The site also offers a list of Internet sites on accounting and non-accounting topics.

URL http://www.K2E.com

Kent Information Services, Inc.

Provides links to sites of interest to accounting professionals as well as information about the services and products offered by Kent Information Services, Inc., including the CPA's Internet Reference Guide. The site also provides descriptive and ordering information about the CPE courses offered by Kent Information Services, Inc., sample articles from the Internet Bulletin for CPAs, and the Site Seeker area which includes an extensive list of resources for Accounting Professionals.

URL http://www.kentis.com


Netscape: Kent Information Services, Inc.
Location: http://www.kentis.com/
What's New?
What's Cool?
Destinations
Net Search
People
Software
infoseek
The Site Seeker Directory of Accounting Resources
Publications
Email Discussion Groups
Web Site Design
CPE Courses
The Staff
Kent Information Services
Rose

Welcome to the Accounting Professionals' Resource Center

In the News

Loans To Be Marketed and Sold Via the Internet

Demo For Year 2000 Data Conversion Project

Download.com Will Help You Get the Most Out of Your Browser

Report On Global Commerce Available On the Web

New Public-Record Search Service Debuts

Auditing Firm Sets Record in 1996

Price Waterhouse Awarded License to Establish Firm in China

For more news, visit our Internet->Bullet site.

New mystery novel with a CPA hero!

Read it this winter!

McGraw-Hill

The publisher provides information about self-study courses that fulfill CPE credit requirements.

URL http://www.mhcec.com/mkcec/mkcpe.html

Pacioli Center at Loyola College in Maryland

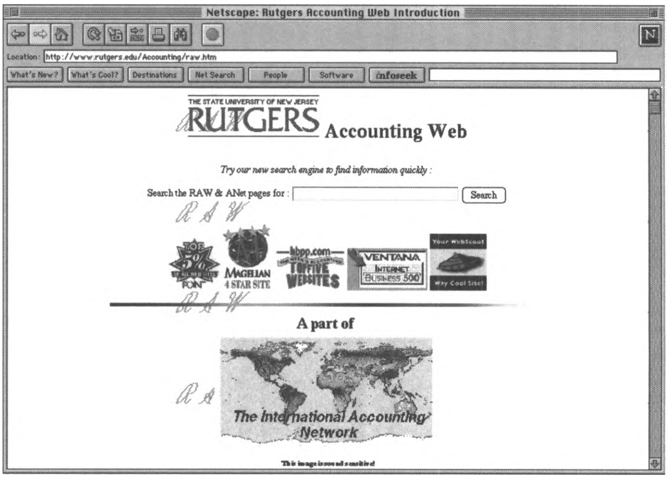
Hosts a mailing list called AECM-L (Accounting Education using Computers and Multimedia) which discusses how hardware and software can be used in accounting education.

Subscribe through email to MAILSERV@LOYOLA.EDU

Rutgers Accounting Web

The accounting department Internet site of Rutgers University provides a list of Internet resources for accountants.

URL http//www.rutgers.edu/Accounting/raw.htm



Netscape: Rutgers Accounting Web Introduction

Location: http://www.rutgers.edu/Accounting/raw.htm

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS Accounting Web

Try our new search engine to find information quickly :

Search the RAW & ANet pages for :

A part of

The International Accounting Network

This image is sound sensitive!

School Business Official's Internet Pathfinder

Includes links to technology information and an Accountants' Resources center. Provided by the Florida Information Resource Network.

URL http://www.firn.edu/~asbo

Software Publishers

A Bit Better Software Publishing

URL http://www.eskimo.com/~realtime/

AccuFile (electronic filing for tax professionals)

URL http://www.vans-inc.com

APPX Software, Inc.

URL http://www.appx.com:80/appxhome.html

Brentmark Software

URL http://www.brentmark.com

Business Logic Corporation

URL http://www.blcorp.com

CoolTax Canadian Tax Software

URL http://www.cooltax.com/

Creative Solutions

URL http://www.cbsolution.com/index.htm

DacEasy, Inc., Small Business Center
URL http://www.daceasy.com
Financial Navigator International
URL http://www.finnav.com:80/
Great Plains Software
URL http://www.gps.com
Grifftax
URL http://www.grifftax.com
Heritage Software (CPELOG)
URL http://www.halcyon.com/cpelog/
Independent Systems and Programming, Inc.
URL http://www.taxsoft.com
Infomast, Inc.
URL http://singapore.com:80/products/infomast/infomast.htm
Intuit, Inc.
URL http://www.intuit.com
Majengo Paperless Audit Software (UK)
URL http://www.majengo.com
Micro Information Products
(non-profit and governmental agencies)
URL http://www.mipinc.com
Monnet Financial Systems
URL http://www.monnet.com/
Navision Software
URL http://www.navision-us.com
Parsons Technology (an Intuit Company)
URL http://www.parsonstech.com
Peachtree Accounting
URL http://www.peachtree.com
Platinum Software
URL http://www.platsoft.com
Plus & Minus Accounting Software
URL http://talyon.com:80/talyon.html

Pro Taxes, Inc. (Canada)
URL http://www.protaxes.com/tmplocx.html
Professional EDI Tax Return Software (Florida)
URL http://member.aol.com/proedi
Red Wing Business Systems
URL http://www.redwingsoftware.com
Rock Creek Technologies
URL http://www.rockcreek.com
Satori Software
URL http://www.satorisw.com/
SBT Accounting Systems, Inc.
URL http://www.sbtcorp.com/
SCS/Compute
URL http://www.scscom.com/
Seagate Software
URL http://www.img.seagatesoftware.com
Solomon Software
URL http://www.solomon.com/
STF Services Corporation
URL http://www.stfservices.com
State of the Art, Inc.
URL http://www.stateoftheart.com/
Tax Resources (specializes in audit defense)
URL http://www.uniqueds.com/taxaudit/
Taxbyte Canadian Software
URL http://www.taxbyte.com
TaxPrep Information Systems
UR L http://www.taxprep.com/
Taxware International
URL http://www.taxware.com/
Timeslips Corporation
URL http://timeslips.com/
CaseWare International
URL http://www.caseware.com:80/

Summa Project at the University of Exeter, Exeter UK

Links to a number of UK and other sites of interest to accountants in public practice, industry, and government, like FINWeb, EDGAR, Security and Exchange Commission's online database, Financial Executive Journal, and Global Network Navigator.

URL http://www.icaew.org.uk/

Tax Accounting and Professional Network (TAPNet)

Bulletin board provides tax and accounting professionals a means to obtain feedback and share information with colleagues on tax accounting issues.

Dial (603)585-9170

University Accounting Departments

Aberdeen University Department of Accountancy
URL http://www.abdn.ac.uk/~acc025
University of Iowa Accounting Department
URL http://www.biz.uiowa.edu/acct/
Pacioli Center at Loyola College, Maryland
URL http://pacioli.loyola.edu/pub
Louisiana State University Accounting Department
URL http://www.lib.lsu.edu/bus/account.html
Oregon State University Accounting Department
URL http://www.bus.orst.edu/cob/acctng/acctng.htm
Rutgers Accounting Web at Rutgers University
URL http://www.rutgers.edu/accounting/raw.htm

Washington Accounting Network (Waccnet)

Maintains listing of accounting information and mailing lists as well as the AuditNet Resource List. Lists are available through anonymous ftp.

For information, email earl@eskimo.org

Auditing

AAudit-L

Subscription discussion group on auditing issues.

Subscribe through email to LISTPROC@scu.edu.au with the message: SUBSCRIBE AAudit-L yourname

ACL mailing list

Moderated discussion forum for issues related to using ACL (Audit Command Language) software. (ACL is a PC-based software program that allows users to read, analyze, and report on data from mainframe, mini, and microcomputers.)

Subscribe through email to listserv@etsuadmn.etsu.edu with message: SUB ACL-L yourname

ACAU-L

Listserve for college and university auditors.

Contact Chuck Jefferis through email at cjefferi@moose.uvm.edu

Association for Computing Machinery

ACM is an organization dedicated to information technology. They have a special interest group for Security, Audit and Control that can be accessed from this site.

URL http://www.acm.org/sigs

Association of College and University Auditors (ACUA)

The ACUA has set up an ACUA Library that contains audit programs, audit reports, questionnaires, guides, program reviews and other resources about audits for institutions of higher education. The file also has a index that lists and describes all the available resources.

URL http://www.acua.org/acua.htm

Association of Healthcare Internal Auditors (AHIA)

The only international organization dedicated to the advancement of the healthcare internal auditing profession.

Email AHIA's Executive Vice President at Charlie Dal@aol.com

Audit-L

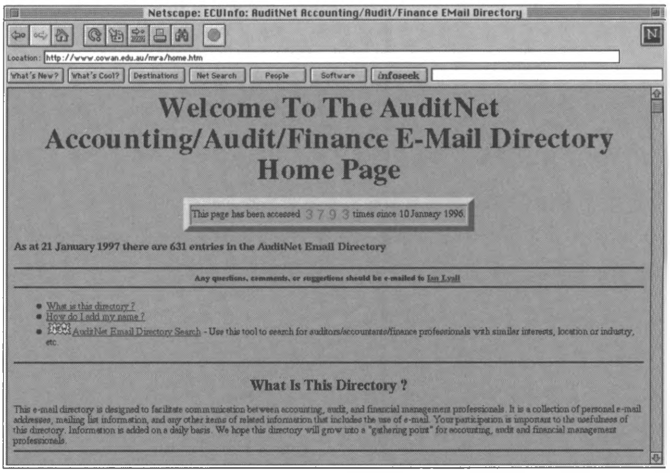
A general audit discussion list open to auditors from all industries and companies with emphasis on auditing issues that cross industry/organizational lines.

Subscribe through email to listserv@etsuadmn.etsu.edu with message: SUB AUDIT-L yourname

AuditNet Accounting, Audit, and Financial Management Email Directory

Lists contact information for accounting, auditing, and financial management professionals as well as related mailing lists.

URL http://www.cowan.edu.au/mra/home.htm


Netscape: ECUInfo: AuditNet Accounting/Audit/Finance EMail Directory
Location: http://www.cowan.edu.au/mra/home.htm
What's New?
What's Cool?
Destinations
Net Search
People
Software
infoseek
N

Welcome To The AuditNet Accounting/Audit/Finance E-Mail Directory Home Page

This page has been accessed 3 7 9 3 times since 10 January 1996.

As at 21 January 1997 there are 631 entries in the AuditNet Email Directory

Any questions, comments, or suggestions should be e-mailed to Ian Lyall

- What is this directory ?
- How do I add my name ?
- NEW AuditNet Email Directory Search - Use this tool to search for auditors/accountants/finance professionals with similar interests, location or industry, etc.

What Is This Directory ?

This e-mail directory is designed to facilitate communication between accounting, audit, and financial management professionals. It is a collection of personal e-mail addresses, mailing list information, and any other items of related information that includes the use of e-mail. Your participation is important to the usefulness of this directory. Information is added on a daily basis. We hope this directory will grow into a "gathering point" for accounting, audit and financial management professionals.

AuditNet Email Listing

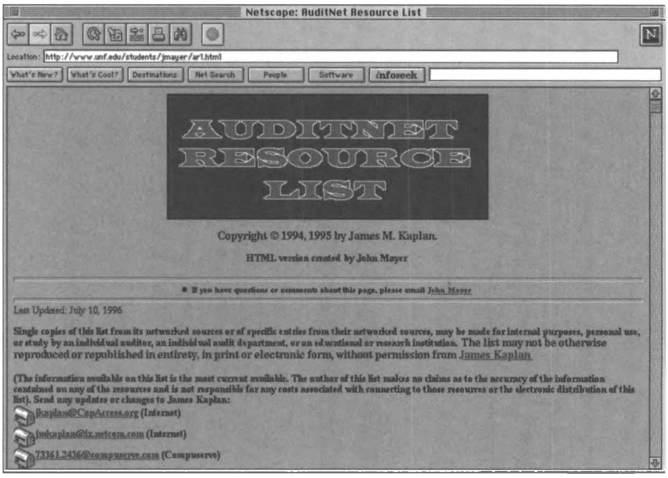
Email address listing for auditors in government, industry, and academic institutions. Listing in AEL is by request.

Email request to Jim Kaplan at jkaplan@capaccess.org

AuditNet Resource List

Listing of Internet resources pertaining to auditing compiled by Jim Kaplan.

URL http://www.unf.edu/students/jmayer/arl.html



Location: http://www.unf.edu/students/jmayer/arl.html

Copyright © 1994, 1995 by James M. Kaplan.

HTML version created by John Mayer

- If you have questions or comments about this page, please email John Mayer

Last Updated: July 10, 1996

Single copies of this list from its networked sources or of specific entries from their networked sources, may be made for internal purposes, personal use, or study by an individual auditor, an individual audit department, or an educational or research institution. The list may not be otherwise reproduced or republished in entirety, in print or electronic form, without permission from James Kaplan

(The information available on this list is the most current available. The author of this list makes no claims as to the accuracy of the information contained on any of the resources and is not responsible for any costs associated with connecting to those resources or the electronic distribution of this list). Send any updates or changes to James Kaplan:

jkaplan@CapAccess.org (Internet)

jmkaplan@ix.netcom.com (Internet)

73361.2436@compuserve.com (Compuserve)

AuditNet Software Sharing

An FTP posting of audit programs shared through listservers.

URL ftp://ftp.unf.edu in directory pub/auditnet/programs

Auditor General of Canada

A report containing more than 1000 pages of information organized by the results of studies and audits completed.

URL gopher://gopher.phoenix.ca:70/11/auditor

Australian Universities Internal Audit mailing list

Available to all Internal Audit staff of Australian Universities (and other interested auditors).

Subscribe through email to INTAUDIT-L-
REQUEST@Levels.UniSA.
Edu.Au with message: Subscribe INAUDIT-L

Columbia University Internal Audit

Section of the Columbia University Web site includes "A Guide to Internal Controls," "Internal Control Issues," and "Auditing at Columbia University: A Service to Management."

URL http://www.columbia.edu/cu/ia/index.html

CPENet (under Accounting subject heading)

CTI-CCC-AUDIT mailing list

Sponsored by the Centre for Accounting, Finance, and Management at the School of Information Systems, University of East Anglia, UK.

Subscribe through email to mailbase@mailbase.ac.uk
with message: Join cti-acc-audit firstname lastname

FinanceNet Financial Audits mailing list.

See FinanceNet mailing lists under Government subject heading.

Fin-audits

FinanceNet mailing list for discussions of auditing topics like relations between CFO and audit communities, agency audit findings, follow-up and validation procedures, and financial audit resources.

Flowcharting BBS

Online bulletin board assistance from Patton & Patton, makers of Flowcharting software.

Dial 408-778-9697

Government Accounting/Auditing Units

Albuquerque, New Mexico, Internal Auditing Department
URL http://www.cabq.gov/aud/home.html
California State Controller's Office
URL http://www.sco.ca.gov/gragraph.htm
Columbia University Internal Audit
URL http://www.columbia.edu/cu/ia
Florida State Comptroller
URL htp://www.dbf.state.fl.us/
Indiana University Internal Audit
URL http://www.indiana.edu/~iuaudit/main.html
Texas Comptroller of Public Accounts
URL http://www.window.texas.gov/comptrol/compinfo.html
University of Florida Office of Inspector General
URL http://nervm.nerdc.ufl.edu/~ufoig
University of Massachusetts Controller
URL http://www.umassp.edu/html/controllers.html
University of Massachusetts Internal Audit
URL http://www.umassp.edu/html/auditors.html

IGNet

Internet-based electronic communications network that collects and exchanges information of interest to the Inspector General community in all levels of government.

URL gopher://www.sbaonline.sba.gov:70/11/ignet

Information Security Discussion List

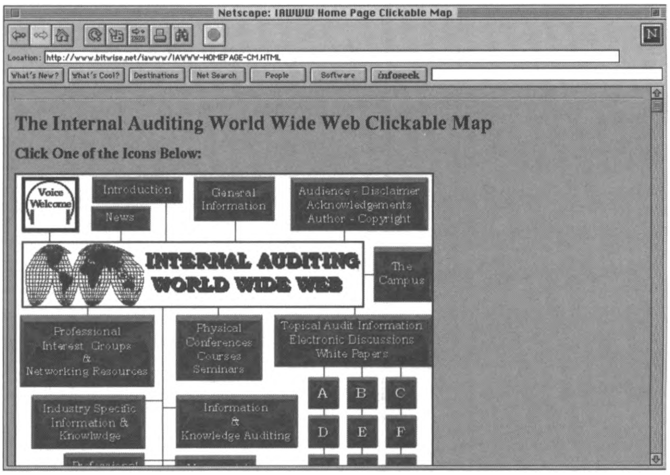
A non-moderated Internet mailing list for information security and auditing professionals in government, industry, and academic institutions.

Subscribe through email to listserv@etsuadmn.etsu.edu
with message: SUB INFSEC-L yourname

Internal Audit World Wide Web (IAWWW)

A production prototype demonstration project for warehousing information related to the internal auditing profession across lines of associations, countries, and industries. Includes sections for electronic discussions, white papers, various auditing specialty disciplines, and industry-specific information.

URL http://www.bitwise.net/iawww/
IAWWW-HOMEPAGE-CM.HTML



Netscape: IAWWW Home Page Clickable Map

Location: http://www.bitwise.net/iawww/IAWWW-HOMEPAGE-CM.HTML

The Internal Auditing World Wide Web Clickable Map

Click One of the Icons Below:

What's New?
What's Cool?
Destinations
Net Search
People
Software
infoseek
N
Voice Welcome
Introduction
News
General Information
Audience - Disclaimer Acknowledgements Author - Copyright
INTERNAL AUDITING WORLD WIDE WEB
The Campus
Professional Interest Groups & Networking Resources
Physical Conferences Courses Seminars
Topical Audit Information Electronic Discussions White Papers
A
B
C
D
E
F
Industry Specific Information & Knowlwdge
Information & Knowledge Auditing

JohnSon's Accounting/Auditing Page

Student page at University of North Florida with links to the Office of Management and Budget, Governmental Accounting and Standards Board, The Yellow Book, and much more.

URL http://www.unf.edu/students/jmayer/account.html

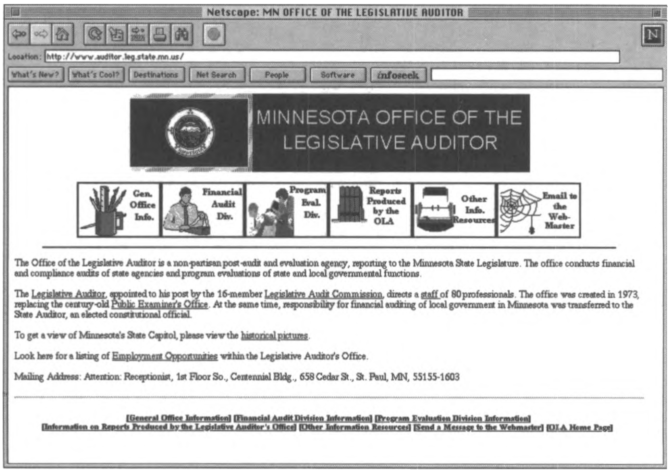
Managerial Auditing (journal)

URL http://www.mcb.co.uk/liblink/maj/jourhome.htm

Minnesota Office of the Legislative Auditor

Provides history of the office, information about the Financial Audit and Program Evaluation Divisions, copies of audit reports including a report on Performance Budgeting, links to the Minnesota legislature Gopher server, and Federal, state, and Internet resources for auditors.

URL http://www.auditor.leg.state.mn.us/



Location: http://www.auditor.leg.state.mn.us/

The Office of the Legislative Auditor is a non-partisan post-audit and evaluation agency, reporting to the Minnesota State Legislature. The office conducts financial and compliance audits of state agencies and program evaluations of state and local governmental functions.

The Legislative Auditor, appointed to his post by the 16-member Legislative Audit Commission, directs a staff of 80 professionals. The office was created in 1973, replacing the century-old Public Examiner's Office. At the same time, responsibility for financial auditing of local government in Minnesota was transferred to the State Auditor, an elected constitutional official.

To get a view of Minnesota's State Capitol, please view the historical pictures.

Look here for a listing of Employment Opportunities within the Legislative Auditor's Office.

Mailing Address: Attention: Receptionist, 1st Floor So., Centennial Bldg., 658 Cedar St., St. Paul, MN, 55155-1603

[General Office Information] [Financial Audit Division Information] [Program Evaluation Division Information]
[Information on Reports Produced by the Legislative Auditor's Office] [Other Information Resources] [Send a Message to the Webmaster] [OLA Home Page]

Multnomah County Auditor's Office Homepage (Oregon)

Includes summaries of recent auditor's reports, an index of past reports, office profile, and an auditor's column.

URL http://www.multnomah.lib.or.us/aud/

National Association of Local Government Auditors (NALGA)

Available through City of Albuquerque, New Mexico, posts excerpts from the LGANewsletter including audit report abstracts. Future postings will include office and committee listings, NALGA mission and objectives, conference and training information. There is also a mailing list for NALGA members and other interested auditors.

Subscribe through email to jkaplan@capaccess.org

National Computer Security Association (NCSA) Forum Auditing Section

Manages a *CompuServe* forum on computer security and ethics with an auditing section that provides auditing professionals with an online real-time international communications forum for discussing auditing and audit-related security issues. Participants share resources, technical knowledge, professional standards, product information, ideas, audit reports, audit programs, training and job opportunities.

Email 75300.2557@compuserve.com

National Intergovernmental Audit Forum Electronic (NIAF) Conference

Provides newsletters, bulletins, files, and message area for government auditors. Access GAO Office of Policy's BBS and join Conference 5.

The New South Wales Audit Office Site

This site provides information about the office, reports and publications.

URL http://www.audit.nsw.gov.au/

Newsgroup

Alt.business.internal-audit

WIU Internal Auditing Home Page

Site at Western Illinois University with information on university auditing procedures and links to other internal auditing sites.

URL http://www.ecnet.users/miaud/wiu/index.htm

Searching

ABC–A Business Compass

This engine provides links to more than 1000 business sites, searchable by subject, industry, or geography.

URL http://www.abcompass.com/

Aliweb

A World Wide Web searching tool that queries the Aliweb database. The database catalogs sites based on descriptions of the services the sites provide.

URL http://web.nexor.co.uk/public/aliweb/search/doc/form.html

All-in-One Search Page

This site is a directory of directories, providing a descriptive listing of Internet search tools.

URL http://www.albany.net/allinone/

Alta Vista

This search engine searches WWW sites and newsgroups by keyword(s).

URL http://www.altavista.digital.com

Archie

Searches titles and keywords of files on all known FTP sites.

Some access sites include:

archie.ac.il
archie.ans.net
archie.au
archie.doc.ic.ac.uk
archie.edvx.uni-linz.ac.at
archie.funet.fi
archie.hana.nm.kr
archie.internic.net
archie.kr
archie.luth.se
archie.ncu.edu.tw
archie.rediris.es
archie.rutgers.edu
archie.sogang.ac.kr
archie.sura.net
archie.switch.ch
archie.th-darmstadt.de
archie.unipi.it
archie.univie.ac.at
archie.unl.edu
archie.uqam.ca
archie.wide.ad.jp

Colorado Alliance of Research Libraries

CARL provides online library catalogs, article indexes, and information databases.

URL telnet://pac.carl.org

Deja News Research Service

This site searches a Usenet news archive.

URL http://www.dejanews.com:80/

Einet Galaxy

An Internet subject index that allows users to browse by subject categories or search World Wide Web, Gopher, and Telnet sites simultaneously using keyword(s).

URL http://www.einet.net/

Harvest Broker

Searches World Wide Web home pages by key words, author, partial text, title, URL and URL references.

URL http://www.town.hall.org:80/Harvest/brokers/
WWW-home-pages/query.html

Information SuperLibrary "Search the Internet" Page

This site lists, describes, and links to a wide variety of Internet search tools.

URL http://www.mcp.com/general/search/srcheng.html

Infoseek

This engine searches WWW sites, Usenet, public databases, and commercial databases. The service charges for usage after the first 100 hits.

URL http://www2.infoseek.com:80/

Library of Congress

Provides an extensive list of Web searching and index resources

URL http://lcweb.loc.gov/global/metaindex.html

Lycos 250

An index of World Wide Web sites, Gopher files, and FTP files that allows users to query by keywords or browse subject categories.

URL http://www.lycos.com

McKinley's Internet Directory

This search engine retrieves lists of sites that are fully described, reviewed, and rated.

URL http://www.mckinley.com:80/

Ohio State University's FAQ index

Allows user to search for lists of frequently asked questions (FAQs) related to keyword subjects.

URL http://www.cis.ohio-state.edu:80/hypertext/faq/usenet/

Open Text

This engine searches Web pages, FTP directories, and Gopher servers by keyword(s).

URL http://www.opentext.com:80

Resources Meta-Index

Bibliography of search tools on the Internet.

URL http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/MetaIndex.html

Ultra Infoseek

Infoseek's updated engine has advanced the size of the database, as well as the way it handles queries. The service features a "virtual real-time index of the Internet" with continuous updates of the database.

URL http://ultra.infoseek.com/

University of Indiana's Mailing List Index

Allows users to find mailing lists related to keyword subjects.

URL http://scwww.ucs.indiana.edu/mlarchive/

Veronica Home Menu

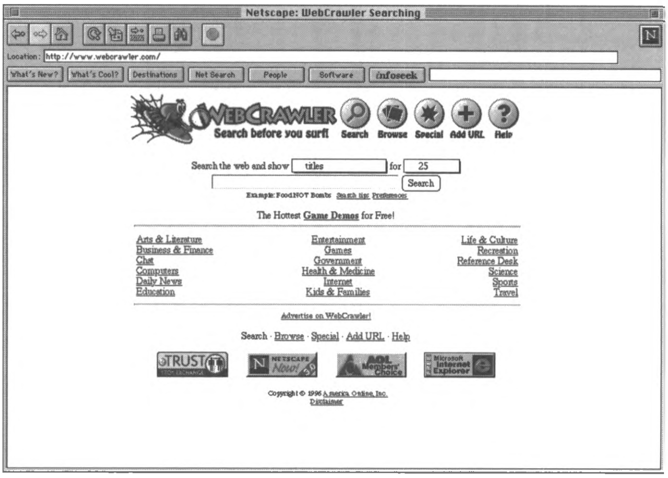
This Gopher menu provides access to Veronica servers, as well as various documents about using Veronica.

URL gopher://veronica.scs.unr.edu:70/11/veronica

WebCrawler

A large index of Internet sites and their contents that users can search by keywords.

URL http://www.webcrawler.com



Location: http://www.webcrawler.com/

Search the web and show titles for 25

Search

Example: Food NOT Bombs Search tips Preferences

The Hottest Game Demos for Free!

Arts & Literature
Business & Finance
Chat
Computers
Daily News
Education

Entertainment
Games
Government
Health & Medicine
Internet
Kids & Families

Life & Culture
Recreation
Reference Desk
Science
Sports
Travel

Advertise on WebCrawler!

Search · Browse · Special · Add URL · Help

Copyright © 1996 America Online, Inc.
Disclaimer

Whole Internet Catalog

A subject guide to the Internet that allows users to search by general or specific subject categories.

URL http://nearnet.gnn.com/wic/

World Wide Web Search Tools

A list of known search engines with general descriptions and links.

URL http://web.nexor.co.uk/mak/doc/robots/active.html

World Wide Web Virtual Library

Provides links to Internet collections of resources on various topics.

URL http://www.w3.org:80/hypertext/DataSources/bySubject/Overview.html

World Wide Web Worm

A World Wide Web index that searches by keywords.

URL http://www.cs.colorado.edu/home/mcbryan/wwww.html

Yahoo

An index of World Wide Web sites, Gopher files, FTP files, and some newsgroups with content descriptions. Yahoo can work like a Gopher menu, allowing the user to choose increasingly more specific categories to narrow the search.

URL http://www.yahoo.com

Security

All-Purpose Security Site

Web page with links to PGP and Kerberos software, companies that make digital-money and secure products, CERT's software archives, and security FAQs.

URL http://www.catalog.com/mrm/security.html

Argus Systems Group, Inc.

Security systems for UNIX platforms and Microsoft Windows NT networked environments.

URL http://www.decaf.com/

Arthur Andersen's Computer Risk Management

Consulting services in information systems auditing and risk security.

URL http://www.arthurandersen.com/bus_info/services/crm/index.htm

Atlantic Computing Technology Corporation

This Connecticut-based consulting company specializes in Internet issues, particularly information security and network audits.

URL http://www.atlantic.com

Barracuda Security

A vendor that provides physical security products, such as alarms and indelible-dye cards.

URL http://www.powernet.co.uk/barracuda/

Business Protection Products

The security division of Datamation Systems provides anti-theft devices such as cables and enclosures, security pads, sound alarms, board protection, disk drive locks, and other products to protect physical assets.

URL http://www.pc-security.com/

CCC Online

This site is maintained by the Copyright Clearance Center, a not-for-profit group that helps organizations comply with US copyright law.

URL http://www.copyright.com

Central Command Virus Protection

This provider of anti-virus solutions offers information on products as well as a database of known viruses, links to other software and hardware vendors, and information from research organizations.

URL http://www.command-hq.com/

CERT

Computer Emergency Response Team's server with articles about security concerns, tools, and an archive of alerts about break-in attempts.

URL ftp://cert.sei.cmu.edu/pub

CERT Security Advisories

Indexed list of Computer Emergency Response Team's warnings issued to mailing lists about security-related problems.

WAIS cert-advisories.src

Check Point Software Technologies

Producer of information security solutions, including firewalls.

URL http://www.checkpoint.com/

CMS Technologies

A provider of physical security products.

URL http://www.cmstech.com/

COAST

Based at the Purdue University Department of Computer Sciences, the Computer Operations, Audit, and Security Technology site represents a "multiple project, multiple investigator effort" in information security research. Current and past sponsors of COAST include IBM, Security Dynamics, Hewlett Packard, Sun Microsystems, the Hughes Research Laboratories, the US National Security Agency, and others. This site maintains a valuable index of online resources and puts out an "irregularly-published" electronic newsletter.

URL http://www.cs.purdue.edu/coast/coast.html

Computer Professionals for Social Responsibility

This non-profit group of computer scientists and others focuses on the social impact of computers and technology. The Internet Library site, sponsored by Sunnyside Computing, offers information about the organization, links to other sites, a discussion group on the history of cyberspace, and examination of such issues as privacy rights and technology ethics.

URL http://www.cpsr.org

Computer Security Products, Inc.

This vendor manufactures physical security equipment.

URL http://www.ComputerSecurity.com/

Computer Security Resource Clearinghouse

Maintains security awareness and training information, publications, conferences, software tools, as well as security alerts and prevention measures.

URL ftp://csrc.ncsl.nist.gov
URL gopher://csrc.ncsl.nist.gov
URL http://csrc.ncsl.nist.gov/

Computers and Information Resources (CIRT) Home Page

This site provides links to resources about ethics and security. The site was established by Dr. David Grisham, Security Administrator for the University of New Mexico.

URL http://www.unm.edu:80/~dave/secpage.html
URL ftp://ftp.unm.edu

The Core Rules of Netiquette

This online guide for Internet behavior is maintained by Albion Books.

URL http://www.albion.com/netiquette/corerules.html

Cryptography, PGP, and Your Privacy Web Page

This site provides links and information about computer security, including a series of electronic manuals for managers, such as "Manager's Guide to Email Security."

URL http://www.gocsi.com

Cylink Corporation

Specializes in encryption and network security solutions.

URL http://www.cylink.com/

Data Fellows Virus News Updates

At this site, you can access a database of information about viruses either alphabetically or through a key word search.

URL: http://www.datafellows.fi/news/vir-news/

Disaster Recovery Journal

This journal archives articles and vendor information and provides links to other security-related organizations.

URL http://www.drj.com/

Dr Solomon's Online

An information center for users of Dr Solomon's antivirus software, this site also provides a "Virus Encyclopedia," a tutorial about viruses, virus alerts, and articles on viruses and hoaxes.

URL http://www.sands.com
URL: http://www.drsolomon.com

Dynasoft

This company's products include computer security solutions for client/server environments, including UNIX, and a smartcard-based PC security system.

Firewalls

Subscription mailing list focused on the subject of Firewalls and Internet Security.

Subscribe through email to majordomo@greatcircle.com with this message: subscribe firewalls-digest

FIRST

The Forum of Incident Response and Security Teams is a coalition of more than 30 computer security incident response teams from government, commercial organizations, and academic institutions.

URL http://www.first.org/

GreatCircle Associates

A firm that specializes in training and consulting on Internet security firewall systems.

URL http://www.greatcircle.com/

IBM Anti-Virus Online

This electronic magazine disseminates information about computer viruses through articles, virus and hoax alerts, and technical support from IBM labs.

URL http://www.av.ibm.com/

Information Security

A non-moderated Internet discussion list for information security and auditing professionals in government, industry, and academic institutions.

Subscribe through email to listserv@etsuadmn.etsu.edu with message: SUB INFSEC-L yourname

Information Systems Security Certification Consortium, (ISC)2

A non-profit corporation established in 1989 to develop a certification program for information security specialists.

URL http://www.isc2.org/isc2.htm#isc2

International Association for Cryptologic Research (IACR)

A non-profit scientific organization dedicated to furthering research in cryptology and related fields.

URL http://www.swcp.com/~iac

InterNIC *Site Security Handbook*

Currently under revision, this document is a popular reference guide for Internet Security issues.

URL http://internic.net

Koehn Consulting

This firm specializes in disaster planning recovery.

URL http://www.mailbag.com/users/koehn/drp.html

Livermore Software Laboratories

Hosts a firewall tutorial that discusses potential security threats and gives an overview on firewall technology, products, and implementation.

URL http://www.lsli.com/

McAfee Software

Maker of the anti-virus software, *VirusScan.*

URL http://www.mcafee.com

Memco Software

Provides enterprise security solutions, including UNIX, single-sign-on, and distributed security administration. The site also offers security news, resources, and other information.

URL http://www.memco.com/

National Computer Security Association

An independent organization that acts as a clearinghouse of information on information security issues. The site offers information on cryptography, firewalls, and anti-virus products, and hosts a message board for the discussion of information security topics. The NCSA also certifies security products.

URL http://www.ncsa.com

Netscape Data Security

Netscape devotes a section of its site to discussing Internet security concerns and how its SSL protocol works.

URL http://home.mcom.com/newsref/ref/netscape-security.html

Newsgroups

alt.security
comp.admin.policy
comp.os.ms-windows
comp.security.announce
comp.security.firewalls
comp.security.misc
comp.society.privacy
comp.security.unix
comp.sys.ibm.as400.misc
comp.virus
misc.legal.computing
sci.crypt
talk.politics.crypto

NIST Computer Security Publications

Provides security publications through email.

Email docserver@csrc.ncsl.nist.gov with message: send index.

Subscribe to Computer System Security Laboratory Newsletter by email mailserve@nist.gov with message: subscribe csl-newsletter.

OSHA

The Web site of the US Department of Labor's Occupational Safety and Health Administration contains information on workplace violence concerns, safety, programs, services and safety compliance issues.

URL http://www.osha.gov/

Privacy Rights Clearinghouse

At the site of this non-profit group based in San Diego, you can find papers on personal security and privacy and how technology affects individual rights.

URL http://www.privacyrights.org/

RSA Data Security, Inc.

This vendor of security software and encryption technologies publishes white papers as well as a FAQ on cryptography export laws, which can be downloaded and read in Adobe *Acrobat* PDF format.

URL http://www.rsa.com

Rutgers University Network Services WWW Security

Maintains an index of resources, including current security issues, mailing lists, and a list of documents under discussion by the WTS Working Group.

URL http://www-ns.rutgers.edu/www-security/index.html

Safetynet

Developer of anti-virus, workstation inventory, and other security software.

URL http://www.safetynet.com/

Security Dynamics

Provides information security hardware and software products. Holds a patent on the SecurID Card, a personal identification token supported by various host, server, and network systems.

URL http://www.securid.com

Security First Technologies

Develops system security for UNIX, networks, and Internet communication authenticity products.

URL http://www.sware.com/

Security Management Online

Online version of the American Society for Industrial Security's monthly magazine. This site contains news and resources, updates on security issues, a discussion forum, and a marketplace of security-related products and services.

URL http://www.securitymanagement.com/home.html

Seven Locks Software

This software company, maker of the *Safe@Home* anti-virus product, provides technical information and white papers on virus identification and prevention.

URL http://www.sevenlocks.com

Snake Oil FAQ

This document by Matt Curtin, chief scientist with Megasoft, Inc., explains how encryption systems work and offers tips on how to choose encryption software.

URL ftp://rtfm.mit.edu/pub/usenet/news.answers/
cryptography-faq/snake-oil

Symantec Antivirus Research Center

Symantec, maker of antivirus software, maintains a research library of recent computer viruses, a virus information database, information about Symantec products, and special coverage of Macintosh viruses.

URL http://www.symantec.com/avcenter.index.html

Technologic

An Atlanta-based corporation that specializes in network security and firewalls.

URL http://www.tlogic.com/

Tecmar Technologies

A producer of tape backup and data storage hardware.

URL http://www.tecmar.com

Telstra Corporation

This Australian company offers a Computer and Network Security Reference Index with links to WWW resources, software vendors and information security consultants, FTP sites, FAQs, and advisory agencies such as CERT and NIST.

URL http://www.telstra.com/au/info/security.html

Trusted Information Systems, Inc.

Provides security analysis and risk assessments, firewalls, mail encryption, and other tools for network and computer systems security.

URL http://www.tis.com

UniTrends Software Corporation

This software company provides specialized backup or utility software for the UNIX platform.

URL http://www.unitrends.com

The World Wide Web Security FAQ

This frequently-browsed FAQ provides an overview of security concerns and potential solutions. Topics include: threats to security, how to run a secure server, how to protect confidential documents, CGI scripts, client-side security, and information on Windows, UNIX, and Macintosh servers.

URL http://www.genome.wi.mit.edu/WWW/faqs/www-security-faq.html

Glossary

A

Access Control List (ACL)

The capability of a router to limit the sorts of packets it accepts by selectively performing duties based on the facts it reads about the packet.

access point

A site vulnerability or potential security problem. An access point is anywhere an unauthorized user may be able to enter a system, such as a keyboard or dial-in line.

Adobe *Acrobat*

A helper application that reads PDF (Portable Document Format) files, files created by converting printer output into compact files, fonts, and page layouts.

Advanced Research Projects Agency (see ARPA)

American Standard Code for Information Interchange (see ASCII)

anonymous FTP

This file transfer procedure was developed to allow users to access files at remote sites by typing "anonymous" when prompted for a user name, and an email address when prompted for a password.

application gateway

An early form of firewall made up of bastion hosts that run special software to act as proxy servers. Also called proxy gateways.

appropriate use

A term used in information security policies that defines what the company allows in the way of employee use of computers, networks, and other hardware or software applications.

ARPA (Advanced Research Projects Agency)

The decentralized computer network of defense agencies and strategic command posts established by the US government in the 1960's to ensure the nuclear defense system would remain functional under a nuclear attack.

ARPANET

The first packet-switching network, developed by ARPA in 1972.

ASCII (American Standard Code for Information Interchange)

A standard numerical code for characters used so that any computer can read text-based files.

authentication

The process of verifying that an encrypted message was (1) sent by the person who signed it and (2) was not altered during transmission. Authentication usually takes the form of a digital signature.

B

backbone

A high-capacity network that links together other networks of lower capacity. A wide area backbone network would typically use digital leased circuits and multiplexers or routers.

back end

The server part of a client/server application, it provides services across the network that have been requested by the client.

back-up server

Software or hardware which copies files so that there are always two current copies of each file. Also known as a shadow server.

bandwidth

The amount of data one can send through any given communications circuit in one second.

bastion-host/dual-homed gateway

A firewall configuration that designates one computer on your private network as the "bastion host." The bastion host is on both the Internet and your network, but it is configured so that no traffic can pass through it directly to any machine on your private network.

binary counting system

The counting system used by computers that has two as the base and uses the digits 0 and 1.

bit

The smallest unit of data in a computer's binary counting system.

boot virus

A virus that infects the boot section or partition tables on a hard disk or floppy disk.

bridge

Device connecting two separate networks to make interconnected LANs look like a single LAN. Bridges can connect networks using dissimilar protocols and do not interpret the data they carry. They control network traffic and security, filtering where necessary.

browser

Software that reads HTML documents and launches the transfer protocols necessary to use the document. Browsers can be either text mode (text only) or graphical user interface (incorporates graphics and mouse interaction).

browser plug-ins

Tools used to change, enhance, or extend the capabilities of a browser. Plug-ins are developed to be used within specific browsers and to interpret particular files or file formats (such as Shockwave, Real Audio, Adobe PDF).

buffer

A software program, storage facility, or hardware device that temporarily stores data to compensate for a difference in transmission speeds or to hold data when there is a difference in timing of events.

bug

An error in a software program that results from a mistake made by the software writers. A bug does not indicate the type of "infection" caused by computer viruses, but is instead an isolated (although potentially annoying) glitch.

bus topology

A network topology in which all network devices are connected to the same cable.

C

cache

To store previously displayed information in the computer memory for quick retrieval. For example, most WWW browsers can cache a number of recently viewed pages so that the user can review them without downloading the pages again.

checksum

A number in a packet that indicates if an electronic message has been corrupted either by an equipment malfunction or by tampering. If an electronic message has been corrupted, the checksum number will be different than the one in the packet header.

checksummer

An anti-virus program that identifies changes in executable files instead of scanning the computer system for a specific virus.

Chief Information Officer

The person in charge of implementing and overseeing the information resources of a company, which normally includes networks, computer systems, and telecommunications.

ciphertext

An encoded, unreadable string of characters. The process of encryption creates a ciphertext out of the original message. See also *plaintext.*

client-server technology

A type of distributed system in which software functions are split between a server computer and a client computer. A client requests information from the server computer, according to a set of protocols, and the server responds to the request.

command.com virus

A virus that changes the operation of the command.com program that controls most PC operations.

command line

The line next to the system prompt where you tell a computer what to do, through written commands. For example, in MS-DOS, the command line is frequently at the c prompt as in c:/>.

commercial online service

A commercial organization that provides proprietary online content along with Internet connections to businesses and home users with PC's and modems (like America Online, Prodigy, and CompuServe).

conferencing

Meetings, either face to face or through telecommunications.

copyright

The legal rights of someone who has created an original text or work. Since March of 1989, when the US adopted the International Berne Convention, the creator holds copyright to an original work as soon as it is fixed in tangible form, whether or not it is published and whether or not a copyright symbol appears on the work.

cracking

Using programming and system skills to gain unauthorized access to systems or information.

cryptanalysis

The process of discovering the secret codes used in encryption. This is often considered "basic training" for aspiring cryptologists.

cryptology

The study of encryption and decryption, or the mathematical systems used to code and decode sensitive information that is sent electronically.

cyberspace

The electronic space through which information flows in computer networks.

D

DARPA (Defense Advanced Research Projects Agency)

Formerly called ARPA, this US government agency funded research and experimentation with the ARPANET and later, the Internet.

data compression

A way of reducing the amount of data to be transmitted by temporarily reducing the number of bits needed to represent the information. When the data is received it is decompressed into its original form.

decrypt

Decoding. Decrypting a message restores it to its original, readable form (called plaintext) from its encoded ciphertext form.

Demilitarized Zone (DMZ)

A network that connects the "trusted" and "untrusted" networks in a firewall. The DMZ is a layer between the networks but is part of neither one.

DES (Data Encryption Standard)

An algorithm designed by the US National Bureau of Standards for the encryption and de-encryption of data using a 64-bit key.

dial-up direct (see SLIP/PPP)

digital signature

A standardized document closing that appears at the bottom of a message or document to authenticate it has been sent legitimately by its stated sender and that the contents remain unaltered during electronic transmission.

disaster recovery plan

A business plan for what to do in case a company or organization's physical location is rendered inaccessible or destroyed by a natural disaster, accident, or terrorism. Disaster recovery plans typically outline how business can be conducted from an off-site location.

discovery virus

A damaging type of computer virus that locates and reports crucial system information, such as the password of the system administrator of a LAN.

DNS (Domain Name System)

The computer system that translates text domain names into IP (numerical) addresses and maintains routing information for Internet transmissions.

domain

A computer site on the Internet that roughly corresponds to city and street name in addresses on letters sent through the US mail.

download

To copy a file, program, or other electronic material from some outside source to your computer.

downward capability

A feature of Internet software that allows it to work with less advanced software that is also running on the Internet.

dual-homed gateway (see bastion)

E

EDI (Electronic Data Interchange)

A way for computers to exchange information electronically using a shared, standard format.

email (also spelled e-mail)

A fast, inexpensive, communication method that sends electronic mail messages through a computer network.

emoticons

Symbols used to represent emotion and tone in electronic messages sent by email or through Usenet.

encrypt

A process that converts plaintext into ciphertext and prevents any but the intended recipient from reading the message.

F

fair use

A group of circumstances under which one can technically violate copyright without being legally liable. Although there are no hard and fast rules to determine fair use, it is usually applied when reproduction of the work 1) does not harm its commercial value, and 2) indicates no potential for commercial gain on the part of the user.

FAQ (Frequently Asked Questions)

Lists of questions asked frequently by newsgroup or Web site newcomers, and their answers.

file compression utility

Programs such as ***WinZip*** or ***Stuffit*** that compress and decompress data to make files more compact for storage.

File Transfer Protocol (see FTP)

fingerprint

Stored programs against which current programs can be compared to verify their integrity and protect against viruses.

firewall

A combination of hardware and software used to isolate a computer or network and protect it from security risk.

flaming

The practice of being unnecessarily belligerent, rude, denigrating, or hostile in Internet communications.

Frequently Asked Questions (see FAQ)

front end

The client part of a client/server application that requests services across a network from a server, or back end. It typically provides an interactive interface to the user.

FTP (File Transfer Protocol)

1) A client/server program that transfers files between local and remote computers across the Internet using the File Transfer Protocol. 2) A protocol method that defines how to transfer files, such as software programs, graphics, or text files, from one place to another.

G

gateway

A computer system that reformats data so that the data can transfer between networks that are usually incompatible.

group

In the context of network security, a group is a set of users who share common permissions for one or more resources.

groupware

Software tools and technology to support groups of people working together on a project, often at different sites.

H

hardware

The actual machines, such as computers, monitors, modems, and printers, used to run computer programs and complete other tasks.

hashing (also called key initialization)

The process an encryption system uses to convert a passphrase into a key. Systems that skip this phase and use a passphrase as a key are not as secure as ones that employ the hashing feature.

header

The part of the electronic message that identifies information about the packet including content type, source, destination, function, and expected life span.

hoax

A non-existent computer virus. Hoaxes are designed to scare computer owners, fool the media, or earn publicity, as in the case of the IRINA virus.

host computer

The computer that serves as an information resource on the Internet or a central processing unit for a number of computers, by receiving information from and sending data to terminals connected through telecommunications lines.

HTML (hypertext mark-up language)

Language used to format text, incorporate graphics and sound, and imbed links to other documents at other sites on the World Wide Web. The resulting document is called hypertext.

HTTP (hypertext transport protocol)

Protocol that specifies the syntax of World Wide Web pages that allow for links and also defines the specifications for page addresses (URLs).

hybrid system

A type of firewall that combines application gateway and packet filtering features.

hypertext

Data that provides nonsequential links (hyperlinks) between World Wide Web resources.

I

IETF (Internet Engineering Task Force)

The open, international community of designers, operators, vendors, and researchers who coordinate the planning and operating of the Internet.

information content

Informative documents or items provided in electronic form through Internet sites.

information distribution channel

The route through which information is dispersed.

Information Security Policy

A set of guidelines used by businesses or organizations to identify potential security risks and offer ways to protect against such risks.

Information Security Team

The group that creates an organization's information security policy. This may include company officers, technology specialists or consultants, financial professionals, network administrators, and employee representatives.

information superhighway

A term coined by Al Gore for the up-and-coming high-speed global communications networks that can carry voice, data, video, and other services around the world.

integrated services digital network (ISDN)

Low-cost, high-speed, digital communication lines that provide dial-in Internet users with faster access to World Wide Web graphics and high-speed data transfer capabilities.

interface

The boundary across which two systems communicate.

Internet

The world-wide network of networks that allows file transfers, remote login, electronic mail, news, and other services.

Internet Explorer

A Web browser created by Microsoft.

Internet server

An Internet host site that offers a service to other computer users, such as mail, file transfer, news, etc.

Internet Society

A membership organization that fosters the evolution of the Internet through its standards setting process, its publications, and conferences. Standards are set by technical committees (experts from both the public and private sectors) who establish procedures and rules that guide Internet operations.

InterNIC (Internet Network Information Center)

The organization responsible for assigning domain names for Internet addresses and directory services.

interval iteration scheme

A method of backing up data that rotates media on which information is stored to ensure that (1) more than one copy of the data exists, and (2) at least one copy is stored off-site.

intranet

An internal TCP/IP network that provides services similar to those found on the Internet, but which is not necessarily connected to the Internet.

intranet server

An intranet host site where the intranet files are stored and organized and from which the files are distributed to other computer users.

IP (Internet Protocol)

The language or set of protocols that addresses data and delivers it to the correct location.

IP session hijacking

A type of network security attack in which a user's session falls under the control of a cracker.

IP spoofing

A type of network security attack in which one host claims to have the IP address of another, thereby gaining access to systems that define which packets may and may not pass based on the sender's IP address.

ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model defines seven layers of communication types and the interfaces among them. The seven layers are: Physical, Data Link, Network, Transport, Session, Presentation and Applications.

ISPs (Internet Service Providers)

Commercial firms that provide individual Internet accounts to businesses and home users.

ITAR (International Traffic in Arms Regulations)

US government policy that controls the export of arms and technologies such as encryption that are considered potentially dangerous in times of war.

J

"Joes"

Account passwords that are variations on the name of the account's owner, thus easily crackable by someone trying to gain unauthorized access to the computer system.

K

Kerberos

Developed by the Massachusetts Institute of Technology, *Kerberos* is a private key encryption system that uses an Internet site (called the *Kerberos* server) to generate keys whenever a group of users wishes to send messages.

key escrow

A system proposed by the Clinton Administration that would grant governmental approval for the export of strong encryption systems if the encryption keys were held "in escrow," either by a trusted third party or one or two governmental agencies. An example is the Clipper Chip.

keys

Alphanumeric strings that enable an encryption program to encrypt or decrypt messages.

L

LAN (local area network)

A network that connects multiple computers across a small area to a server for the purpose of sharing resources, usually in a business office.

layer

Description of divisions in specifications such as the OSI communications protocol. Functions are grouped together to form steps in the hierarchy necessary for successful data communications.

listserv

A mailing list management program that automatically sends new messages to list subscribers and responds to email requests.

M

macro virus

A virus that is contained within automated step sequences (or macros) in a data file.

mailing list (subscription mailing list)

An online discussion group to which you subscribe to receive messages directly through your email address.

mainframe

A computer designed for batch rather than interactive use.

MBPS (Mega Bits Per Second)

A transfer rate for units of information.

middleware

Software that runs between a client and a server to make communication possible.

military grade

A claim made by some encryption software vendors, the term "military grade" is meaningless because there is no military standard for encryption systems.

modem (modulator-demodulator)

A piece of hardware that connects computers and allows them to communicate with one another by modulating digital data (generated by the source computer) into analog signals that travel through the phone lines to a remote modem. The remote modem then demodulates those analog signals back into digital data that the remote computer can understand.

modules

Smaller parts of large software programs.

multipartite virus

A virus that is capable of infecting both executable files (like a program virus) and the boot section or partition tables on a hard disk or floppy disk (like a boot virus).

N

Navigator

A World Wide Web client by Netscape that facilitates electronic commerce by encrypting information (such as credit card data) sent to secure Netscape NetSite servers.

netiquette

The rules for appropriate behavior that guide Internet interactions.

network

A system of computers connected by telephone wires or other means that allow hardware and software to exchange data.

network administrator

The person responsible for the control of a computer network. Also called a systems administrator.

network computing

A term analogous to client/server computing.

newbies

Inexperienced Internet users.

Newsgroup

A discussion group on a limited topic that shares information through Usenet.

newsreader

A software program that provides access to Usenet.

node

A terminal in a computer network.

NOS (Network Operating System)

An operating system that includes all the software needed to communicate with other computers over a network.

O

One-Time Pad

A feature of some encryption systems that works by having a "pad" of random bits in the possession of both sender and recipient but no one else. The output of an OTP system is equally likely to decrypt to any same-size plaintext without the presence of the correct bits. Once the bits are used from the pad, they are destroyed and never used again.

operating system

A type of software that manages the work done on a computer. The operating system is responsible for scheduling tasks, allotting storage space, and directing interfaces among computers and the various hardware with which they interact.

P

packet

The basic grouping of Internet data. Any message sent through the Internet is made up of packets that carry necessary information, such as the address. The packets are reconstructed when they reach their destination by TCP/IP protocols.

packet filtering

A type of firewall that uses access control lists to restrict what kinds of information a network router will pass on, thereby limiting outside access to an internal network.

packet switching

A communications method by which individual packets are routed between hosts through the most expedient route at that particular time.

password

The oldest line of computer defense, a password is a word, phrase, or string of symbols entered into the keyboard by an individual user in order to gain access to a computer system.

payload

The part of a computer virus program, executed by the trigger, that affects the computer system. A payload may be a relatively harmless error message, or something more damaging, such as the deletion of files or the altering of data.

PGP (Pretty Good Privacy)

A public key security system that uses a formula to create a key from two prime numbers. The key is used by the PGP program to encode messages that cannot be decoded unless you know the two original prime numbers used to create the key.

plaintext

The original message which is encoded into ciphertext, in the case of encryption, or decoded from a ciphertext in the case of decryption. See also *ciphertext.*

platform

The computer operating system and also the standard that governs it.

port

A channel in a communications system that is assigned to each application program.

pristine backup

A backup file made when all executable files and directories are known to be secure.

private key system

An encryption system that requires both the sender and recipient of the data to have the same key. Also called symmetric system.

program virus

A computer virus that infects executable files (such as *.exe* files).

protection instructions

The parts of a computer virus program that protects the virus from being detected. Protection instructions can take the form of encrypted data or a "stealth" technique that interferes with anti-virus software.

protocols

A set of rues that determine how computers will communicate. Protocols allow computers from different manufacturers and running different software to (1) agree on what data means and how to use it, (2) share computing applications, and (3) communicate back and forth.

proxy

The process or having one host act on behalf of another, as in the case of a proxy server which retrieves data from the Internet and returns it to a client computer.

public key system

An encryption system that assigns one pair of keys each to the sender and the recipient, designed so that users would not need to access other sites to generate keys, and so that keys could be distributed through unsecured channels. PGP is an example of a public key system. Also called asymmetric system.

R

remote

Computer (or other hardware) at an outside site with which a local computer is communicating.

replication instructions

The parts of a computer virus that allow the virus to copy itself.

RFC (Request For Comment)

Document series begun in 1969 describing the Internet suite of protocols and related guidelines.

risk analysis

An analysis of a computer system that will determine what assets an organization needs to protect, how they can be protected, and the severity of each risk. Balancing protection cost versus degree of loss is an important part of the analysis.

router

An internetworking device that analyzes network traffic and determines the best route for information (network packets) to travel.

routing

The process of examining the headers on files and moving them to the next site through the most expedient path to the destination.

RSA

RSA Data Security, now owned by Security Dynamics, Inc., developed an important asymmetric algorithm encryption system.

S

S-MIME

A protocol based on the RSA encryption system that transparently encrypts and decrypts email messages sent via such programs as *Eudora Pro* and *Netscape Mail.*

scanner

An anti-virus program that screens a computer system for viruses and alerts the user if a virus is found.

screened host gateway

A firewall configuration that includes both a screening router and a bastion host. The router makes the bastion host the only machine from your network available from the Internet.

screened subnet

A firewall that consists of a small, isolated subnet created between a private network and the Internet. Hosts on the Internet can access hosts on the subnet, as can hosts from your private network, but no traffic can cross the subnet.

screening router

A firewall method that consists of a piece of hardware programmed to allow only certain traffic to pass from one side to the other.

secure hypertext transport protocol (see SHTTP)

Secure Sockets Layer (see SSL)

server

Internet host site that offers a service to other computer users, such as mail, file transfer, news, etc.

server certificate

World Wide Web security strategy that protects clients from inauthentic servers through a one-time challenge-response exchange. Only servers with the correct server certificate and corresponding private key for the challenge issued by the client are judged to be valid.

server software

Software that allows your computer to offer services to other computers.

SHTTP (secure hypertext transport protocol)

A security protocol that encrypts traffic on World Wide Web connections.

SLIP/PPP (Serial Line Internet Protocol/Point to Point Protocol)

Two protocols that treat a computer like it has a complete and continuous connection to the Internet, instead of just being connected with a modem and telephone line on an intermittent basis. (Also called dedicated port, dial-up direct, or dedicated dial-up line service.)

software

Stored instructions (programs) that translate the information you send to your computer into language the computer can understand.

spamming

Inappropriate Internet marketing that consists of arbitrarily posting a message about expertise, contact information, and fees to many newsgroups.

SSI (server-side include)

A command that directs the server to run a program, such as the inclusion of the current date on a Web page.

SSL (Secure Sockets Layer)

A security protocol that creates channel security in which an encryption key is created during an initial message exchange. Because this protocol functions independently of other protocol operations, it can be used with HTTP, FTP, or Telnet exchanges.

stack (also called suite)

A group of protocols that includes a cluster of related protocols.

System Administrator
(also called sysadmin or network administrator)

The systems expert in charge of a computer or network.

T

tape drives

Hardware devices, either internal (requiring a card slot) or external (using a serial or parallel port), that provide convenient storage of large amounts of data on specially-formatted high-volume tapes.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The shared language or set of protocols that defines how computers on the Internet exchange information. IP addresses data and assures it arrives at the correct location. TCP breaks up data files into packets when sent and reassembles the packets in the correct order at the recipient site.

telecommuting

Working at home and communicating with your fellow workers through the phone lines, typically with computer, modem, and fax.

Telnet

A terminal emulation protocol that allows you to log in to other computer systems and function like a terminal on the Internet.

terminal

Part of your hardware, a terminal is an electronic device used to enter and receive data in a computer system.

terminal emulation software

Software that allows your computer to communicate with a remote computer as if your computer were actually a terminal connected with that computer.

Transmission Control Protocol (see TCP/IP)

tools

Programs used to create, manipulate, modify, or analyze other programs, such as a compiler or an editor.

topology

The shape of the network cabling system.

trigger

The part of a computer virus program that controls when the virus is triggered into activity.

U

UDP (User Datagram Protocol)

A simple, transport-layer protocol.

Unix

A popular operating system used by most Internet servers. *Windows NT, Windows,* and *Macintosh* operating systems can also be used on servers.

URL (Uniform Resource Locator)

Information used by the World Wide Web browser to determine where an Internet site is and how to connect to it.

Usenet newsgroups

A collection of thousands of subject-specific bulletin-board type discussion groups on the Internet.

UUCP (UNIX -to-UNIX CoPy)

A type of network that offers limited features, such as file sharing and email. Originally developed to connect UNIX hosts, a UUCP is usually built using dial-up connections. Not an interactive network.

V

Virtual Private Network (VPN)

The process of connecting a main office and a satellite office through the Internet by using encrypted data to protect internal resources.

virus

A program that can "infect" and damage files and programs on your computer. Viruses are designed to reproduce and spread within a computer system or network without revealing their presence.

W

WAN (Wide Area Network)

A network usually constructed with serial lines, extending over distances greater than one kilometer.

***Windows for Workgroups* (WFWG)**

A Microsoft operating system that allows between two and 20 users to share information such as files and email.

***Windows NT* (New Technology)**

Microsoft's scalable 32-bit version of *Windows* aimed at high-end workstation "power" users. It is a standalone operating system that is also a "network ready" system capable of being a small application server for a workgroup of *Windows*-based PCs.

Z

zip disk

High-volume, removable disk that works with a zip drive and can be used for effective backup storage or to handle very large files.

From personal security to organizational policies, ***The CPA's Guide to Information Security***, published by **Kent Information Services, Inc.**, will prepare you to meet the challenges of information security.

Learn to recognize primary information security threats, risks, and tools for protecting information assets.

Understand encryption and how to select reliable encryption software.

Prepare to establish an information security team and select important team members.

Master the process of identifying risks and developing and implementing an information security plan that emphasizes the role and responsibilities of the CPA.

Chapter Sampler

- Physical Security–identifies common risks and how to plan for a secure office setting.
- Viruses–describes viruses, how they work, and how to protect information assets from virus damage.
- Network Security–overviews network security issues and strategies for protecting network assets.
- Organizational Security Issues–identifies the components of an information security policy and strategies for risk assessment.

Authors

John Graves, CPA, is editor of the ***Internet Bulletin for CPAs***, and author of continuing professional education courses on the Internet use for the American Institute of CPAs, Intuit, the Institute of Management Accountants, and other professional associations. Graves was named **1996 Trailblazer in Technology** by ***Accounting Today***. He is an original co-author of the AICPA's first software products, Audit Program Generator (APG) and Accountant's Trial Balance (ATB).

Kim Hill Torrence is co-author of the ***CPA's Internet Reference Guide*** and editor of the ***Internet->Bullet***, a weekly email news service for accounting and financial professionals. She is the former Communications Manager for Ziff-Davis Predicasts where she authored training materials for conducting online research.

● Kent
Information
Services

093003