Fall 1991

InfoTech Update, Volume 1, Number 1, Fall 1991

American Institute of Certified Public Accountants. Information Technology Division

InfoTech UPDATE

Practical Advice For Implementing Technology

New IT Membership Division Formed

In May 1991, the AICPA Governing Council authorized formation of the AICPA Information Technology Membership Division. Shortly after the division was established, *InfoTech Update* interviewed Michael W. Harnish, CPA, a partner at Crowe, Chizek & Company in Oak Brook, Illinois, and chairman of the Information Technology Executive Committee, which oversees the division. In the following discourse, Chairman Harnish describes the division and its plans for the future.

InfoTech Update: *Why did the Institute decide to form the Information Technology (IT) Membership Division?*

Michael W. Harnish: In 1988, the AICPA commissioned the Strategic Planning Committee to review far-reaching strategies for the Institute in accordance with the goals of the AICPA and its members. In its report of October 1988, the committee identified major goals the AICPA should strive to attain. One of those goals was to develop a major focus regarding the technology needs of members. That was the basis from which the AICPA formed a special committee, the Information Technology or IT Committee, on December 15, 1989. The IT Committee's formal charge was "to study members' technological needs and recommend programs to meet those

needs." We found that the profession needed to improve its IT knowledge. One of our major decisions in order to raise that level was to establish a membership division.

ITU: Do members need to be "high-tech" practitioners to benefit from the IT Division?

MWH: Definitely not. Although the Information Technology Division sounds "high-tech" and "leading edge," we really have geared this division to the everyday member in private industry as well as in public practice—the "non-technocrats." We want a very broad representation of membership in the division. The IT Division is one of the first truly multi-disciplinary divisions within the AICPA. I don't want the words "information technology" to scare people. I want to see the division cut across all of the traditional segments present in

continued on page 2

In This Issue:

3
LAN Disasters And How To Avoid Them

6
Becoming A Leader In Technology

7
Information Security: Responsibilities And Opportunities

9
System Auditability And Control Report

InfoTips

Here are a few simple tips, which can be used right away, to enhance your use of Windows 3.0. They are taken from a presentation made by Marc A. Moskowitz, CPA, at the June 1991 AICPA Microcomputer Conference. He is a member of the Management Advisory Services Department at Morrison & Morrison, Chicago, Illinois.

- **Hardware**
  The most important tip to follow before entering the Windows 3.0 world is to use the correct hardware. Although you can use an 8088 processor, performance will be very slow. A more appropriate setup is a 386SX computer, a 40MB hard drive, 2MB of RAM, a VGA monitor, and a mouse.

continued on page 2

continued from page 1

the AICPA and to benefit all of our members.

As we all know, information is being viewed as an increasingly valuable asset to many businesses. Those who can use and understand technology become not only more experienced, but also more capable of understanding the businesses they serve as employees, auditors, and consultants, and the risks these businesses face. Consequently, even someone without a strong IT background can gain significantly from division membership's offerings and benefits.

ITU: What kinds of things can people who join the IT Division expect to receive?

MWH: We've given that a lot of thought within the Executive Committee. We have developed short-term and long-term deliverables which will be of interest to members. In fact, being a member of the IT Division in itself is almost a deliverable. In the short-term, our Newsletter *InfoTech Update* will provide a practical link between technology and the application of that technology within one's firm or company. We also want to provide technology tools to members—especially productivity-oriented tools. We intend to work with vendors to provide samples or full, working copies of those tools to membership in order to give them real hands-on experience.

ITU: Will you be able to provide other tangible benefits?

MWH: I think one of the largest benefits will be our work with vendors to provide discounts on technology products—equipment and software. This will help offset the capital impact of technology on members' practices or businesses by offering some substantial savings. We are also trying to establish an annual conference in conjunction with the successful AICPA Microcomputer Conference.

ITU: And in the long-term?

MWH: Long-term, we are thinking about the creation of case studies of technology use in business, such as the application of electronic data interchange (EDI) and bar coding. Other long-term benefits will be the development of seminars, CPE courses, and educational guidance. Another long-term goal is coordinating with the AICPA, state societies, and other national and international groups. We've already opened dialogues with similar groups in both Canada and England. Finally, we will also analyze the benefits of offering an accreditation for an information technology specialist.

ITU: What areas will the IT Division focus on initially?

MWH: We will concentrate on the following areas, not necessarily in this order. First, we want to analyze the impact of IT on data security. Second, we want to analyze the potential impact of technology on the management of a practice and the functions of the members in industry —their personal use of technology as well as its effect on the world around them. Third, we are interested in the impact of technology on the audit and attest functions. Fourth, we will analyze the impact of technology on the consulting functions of many of our members.

ITU: Do you have far-reaching goals for the division to benefit the profession?

MWH: We want to improve the public's perception of the CPA as someone skilled in information technology. This will increase the public's recognition of, and confidence in CPAs as leaders in the application of new technologies to information management and thus help to maintain their traditional role as advisers to business. **IT**

InfoTips *continued from page 1*

- **Do Not Load Mice Drivers**
  If you will be using Windows 3.0 programs only, do not load mice drivers before entering Windows. Windows 3.0 automatically supports most mice for Windows 3.0 applications, and the mice driver is not needed. However, if you plan to use a mouse for non-Windows 3.0 mice-supported applications, you must load the mouse driver prior to entering Windows 3.0.
- **Use Opposite Hand for Mouse**
  If you are right-handed, consider using a left-handed mouse and vice versa. This will allow you to have your natural hand free for the use of the numeric key pad. In addition to swapping hands, the left and right mouse button should be changed via the control panel.
- **Use Correct Netware IPX.COM and NET3.COM or NET4.COM Shell**
  If you are running Windows 3.0 with a Novell file server, use Novell Shell 3.0 revision D. Novell Shells prior to 3.0 are not compatible with Windows 3.0. Novell Shells prior to Revision D have caused problems with Dynamic Memory Pool 1.
- **Use the SYSEDIT Utility**
  SYSEDIT is a command found in the system subdirectory of the Windows directory. When running the command (SYSEDIT.EXE), the four main system configuration files (CONFIG.SYS, AUTOEXEC.BAT, WIN.INI, and SYSTEM.INI) can be edited simultaneously.
- **Be Cautious When Exiting Windows**
  Do not enter keystroke commands until the DOS prompt appears. Windows 3.0 needs time to close down all open files. Entering keystrokes during this process may cause the system to freeze. **IT**

INFOTECH UPDATE, Fall 1991, Volume 1, Number 1. Publication and editorial office: 1211 Avenue of the Americas, New York, N.Y. 10036.

Anthony J. Gambino, CPA
Editor

Richard D. Walker, CPA
Director

LAN Disasters And How To Avoid Them

By Donald Hunt, CPA

The word disaster conjures up thoughts of devastating tornadoes, raging fires or erupting volcanoes. To most of us, a disaster is something that happens to other people, somewhere else.

Although you'll never see coverage of one on the news, a LAN disaster can cause major problems for a business, rendering a network totally or partially inoperable or creating management problems on a massive scale. A crashed server can prevent a company from entering orders for days. An erratic network interface card could scramble a long, but very important, invoicing run. In any form, a LAN disaster spells major problems.

Common LAN disasters can be prevented or remedied more effectively if they are anticipated, and recovery plans are made in advance. The key is planning. Disaster prevention and recovery planning should be an essential part of your business strategy as well as an important aspect of technology planning. Preventing disasters and recovering from unavoidable ones generally do not involve complex, technical issues. If the planning is not done, or not done right, however, this failure can pose a serious risk to an organization's ability to do business. This article will focus on four common types of LAN disasters and give you practical tips on how to avoid or recover from them. Preventing or recovering from LAN disasters is not a technical issue—it's a management responsibility.

Donald Hunt, CPA, is a partner at Anderson, Hunt & Company in Atlanta, Georgia. He is also a member of the Information Technology Executive Committee.

Hard Disk Failure on the Server

Sooner or later almost all PC hard disks fail. Head crashes, electronic malfunction, or physical damage can make the programs and data they contain unreadable and, thus, unusable. There is little you can do to prevent electronic malfunction, short of buying quality hard disks, especially for servers. Once a hard drive malfunctions, it is destined for a trip to the factory or the junk heap, and your data is, for all practical purposes, lost. There are usually few options but to replace the hard drive. A situation very similar to an electronic malfunction, in result, at least, is the theft of a server. All of your data are effectively gone. Tips for dealing with the failure of a hard disk come under two categories: prevention and recovery planning.

Prevention

- You can avoid head crashes or other physical damage to your hard disks by taking reasonable precautions: Keep them out of high-traffic areas and in dry, room-temperature conditions. Maintain physical security by keeping servers in a locked room.
- Because electrical problems, from voltage spikes to outages, can have harmful effects on server and network operations, it's worthwhile to invest in a high-quality uninterruptible power supply/power conditioner for your server. Today's models actually connect to the serial port of the server and continually report power conditions to the network, warning the administrator and users of potential problems that may require a shutdown.

Recovery planning

- Know where you can get a replacement hard disk fast. The popularity of hard drive models changes rapidly, and your local dealer may carry only the latest models. Getting an identical replacement delivered to you may take days or weeks—if you can find one. To prevent extended downtime, you may want to invest in a spare hard drive, or get a local service company to keep one in stock. The time to find out that you've got a hard-to-replace model is now.

  If you select a different type of disk to replace your failed one, be sure your replacement model is supported by your network operating system, that you have all the necessary driver files, and that they are the most recent versions.
- Prepare a diskette in advance containing your tape sub-system drivers, restore software, and, in some cases, operating system software, to facilitate getting your applications and data onto the new disk.
- Configure your LAN with multiple servers. This sounds expensive, but the cost may not be prohibitive. The backup server you designate may be a little slower and have less capacity than the primary server, but it can get the key jobs done until a new primary server is up and running. The backup server's hard drive can be preloaded with key user information and permissions; application files can be loaded onto the backup server at the time of the failure. Like all recovery operations, having a valid backup copy of your data is a must.
- A more sophisticated approach is to have servers that are mirrored. Mirrored servers contain identical files and are automatically kept in sync by the network operating system. Normally, only a few keystrokes are all that is required to get your mirror server on-line as the primary server.
- Have a comprehensive file backup plan and follow it religiously. A backup plan should outline who is

continued on page 4

continued from page 3

responsible for backing up files, what files are to be backed up, when they are to be backed up, the backup method, and where the backup media is to be stored and labeled. The plan should be set down in writing and should be tested periodically, a step that is often skipped. The test should consist of restoring all of your backed-up programs and data, and should be carried out on the backup server or on a machine identical to the computer that will be used in case of server or hard disk failure.

The file backup system used for the server and key workstations generally will require specialized hardware and software. Using floppy disks and the DOS backup command is probably not an effective method for a LAN of any size and complexity. Most LANs today are backed up using some form of tape sub-system attached to a server or a network workstation.

PC tape drives are generally one of three types: quarter-inch cartridge (QIC), digital audio tape (DAT), or 8-millimeter cassette (8mm). QIC is often used on smaller LANs, as its upper limit is currently 500MB per cartridge. DAT is a newer technology and can store about 2 gigabytes, or 2 billion bytes. The 8mm drives are also new and promise to store up to 5 gigabytes.

Capacities and speeds are constantly changing. DAT changers soon will offer unattended multiple-cartridge capability. Optical disk sub-systems also are used for LAN backup, but generally are more costly to use than tape because often the optical disks cannot be reused. Magneto-optical (MO) disks are now gaining in popularity, thanks in part to their erasability. These might be an alternative for your backup needs.

Specialized software is available to automate the entire backup and restore process. Look for software that provides for some form of media cataloging, backup scheduling, error detection and correction, local drive backup capability, and easy restore procedures.

- Keep a map of each server's complete directory structure and file list on a floppy disk. This map is easily created using DOS or network operating system commands. Then use the map to verify the completeness of a restored server by printing out the stored map and comparing it to the restored server's directory structure and file contents.
- Keep all original software disks and updates in an organized and safe place. You may choose not to back up and restore applications from the server, but to reload the software from the original manufactured disks. Running around the office trying to locate 20 or 30 different application packages and their updates can slow down the disaster recovery process. Keep an inventory of your application packages and a log of the revisions as they are installed. Try to keep original software diskettes in a single location. Most license agreements allow you to make an archive copy of the software. Keep your archive copies at an off-site location.

Your LAN Comes Down With a Virus

Computer viruses on a single PC are a problem. Viruses on a LAN are a catastrophe. Viruses have destroyed entire servers, created intermittent processing errors that ruined the integrity of accounting systems, and even caused hardware devices to self-destruct. They can be disastrous to a business. Here are four key steps you can follow to protect your LAN from the threat of a deadly or at least debilitating virus:

- Learn the basics about viruses and keep up-to-date on the known viruses and their characteristics. Many articles about viruses have appeared in professional journals, including the May 1991 issue of the *Journal of Accountancy*. Some virus protection software vendors provide hotlines and bulletin board services for their users. A small investment in time will pay big dividends in keeping your LAN virus-free.
- Have a written company "safe computing" policy limiting the installation of public domain software or the downloading of bulletin board files. Generally speaking, these should be prohibited or limited to non-network computers. If you choose to allow these files on network workstations, then virus detection procedures should be more sophisticated. The policy should also prohibit the routine booting of hard disk PCs with a floppy disk.
- Use a software product that can detect any existing viruses on your LAN, eliminate them, and protect against new viruses. There are several products on the market which can scan for viruses on network drives and can be loaded as a memory-resident utility for on-line virus detection.
- Follow your file backup plan so that if a virus attacks, you have what you need to reload your server. Because you don't know whether your backups contain the same virus, initiate an anti-virus program immediately upon restoring your network, to prevent a reoccurrence.

Your LAN Administrator Leaves the Company

This is the "Bill or Mary doesn't work here anymore" disaster, and may be the most common cause of LAN calamities. Companies have had major problems keeping LANs running smoothly when a LAN administrator leaves. This is even true when the LAN administrator leaves in good standing and with proper notice. Yet this disaster is easily preventable. The following tips focus on the concepts of shared responsibility, cross-training,

Twelve Tough Questions To Ask Your LAN Administrator

1. Do you have a comprehensive backup/restore plan in writing?
2. Have you tested your backup plan by actually restoring all data and applications to a backup server?
3. Do you create regular directory maps of the server?
4. Do you have a hardware/wiring diagram of our network, and an inventory of all equipment and accessories?
5. What provisions have you made for replacing the hard disk(s) on our server quickly?
6. Who is responsible for overseeing daily or regular backups?
7. Are our backup methods state-of-the-art and complete?
8. What provisions have you made for safeguarding backup media?
9. Who is the assistant LAN administrator and do you regularly confer with him or her on procedures?
10. How often do you require network users to change their passwords?
11. Have you installed a virus-detection application on the network?
12. Do you have a policy against installing public domain software or applications of questionable origin?

and documentation of the LAN setup and procedures.

- Document in writing the entire organization of the server(s)—the trustee rights, user information, and the naming conventions used for servers, volumes, and directories. Much of this documentation can be created by the network operating system. For example, Novell NetWare will let you print out user information from the SYSCON menu and print out the server organization using the MAP command-line utility. IBM LAN Server lets you print out the Domain Control Database, which contains server and user information.
- Maintain a complete and current wiring diagram for your LAN cabling and the physical devices in your LAN. This should include a complete descriptive inventory of all LAN workstations, including information about the workstation hardware, any other devices installed, the version of DOS and ROM BIOS in use, the NIC (network interface card) and its interrupt settings, and the workstation address. Information on how each workstation is configured for the LAN should also be documented. For example, in a NetWare LAN you would want to record the NetWare shell versions of IPX and NETx and save the contents of the SHELL.CFG file.
- Appoint an assistant LAN administrator. This will generally be a part-time job and for a small LAN will only take a few hours per week. The assistant LAN administrator should be familiar with the organization of the LAN and its overall operation. He or she should participate in the testing of the file backup and restore procedures and be familiar with the written LAN documentation.
- Identify a local support company that could provide on-site technical assistance in the event of a problem. The support company could provide you with a temporary LAN administrator, if needed.

Unauthorized Disclosure Of Confidential Information

This LAN disaster can range in its consequences from internal furor over salaries to a major competitive or public relations nightmare if sensitive company information is accessed by an outside party. Passwords and data encryption are two solutions that are easy and inexpensive to implement, but frequently are not used, or are not used effectively.

- Passwords should protect access to the LAN and trustee rights defined for those users who have permission to access confidential information. The network operating system generally has facilities that allow you to perform these functions. Additional password protection often is contained in individual application software products or may be added by network menu programs like Sabre Menu from Sabre Software Corporation.
- Require that passwords be changed by your users on a regular basis. Monthly password changes are not too onerous. If this is not done, passwords quickly become common knowledge in all but the smallest offices. Programs like Novell NetWare and IBM LAN Server enable you to specify the frequency with which users have to change their passwords and enforce the policy automatically.
- If dial-in access is provided to your LAN, special controls should be set up. Dial-in access offers tremendous opportunities to enhance the value of the LAN to outside or travelling employees, but it also offers the greatest risk of unauthorized access to your LAN resources. Your remote access software should have call-back capability, automatic disconnect after a certain number of unsuccessful log-on attempts, and a monitoring report of access violations.
- Highly sensitive information stored on LAN servers should be encrypted. Quality data-encryption software is inexpensive and easy to use. Be sure the encryption software you get meets federal government encryption standards.

Planning for a LAN disaster may not prevent one from happening, but it will make recovering from one much smoother, with less disruption to your business. Lack of planning can compound your problems, multiplying their severity. With networks, failing to plan is planning to fail. IT

Becoming A Leader In Technology

By L. Gary Boomer, CPA

Growth in technology is expected to continue, and successful firms today must address that growth. As illustrated by the following box, firms are already making significant investments in technology. These statistics were compiled from a recent survey of over 30 firms. The firms were located throughout the country and ranged in size from 10 to 300 employees.

Peer Firm Technology Investments

4–5% of gross revenues
$2,500 per employee per year
$2.25 per chargeable hour

Several shared characteristics exist among firms profitably implementing technology. Those characteristics are:

- Strong technology leadership at the partner level
- A written three-year technology plan
- In-house technology expertise
- Use of an outside facilitator
- Planned employee training
- A cost-recovery system.

During the 70s and 80s, firms typically invested in a computer system every 7 to 10 years. Most of the systems were batch-processing, multi-user systems in a separate "computer department" environment. In contrast, enterprise computing (involving everyone in the firm) and a three-year reinvestment time frame are appropriate in today's work environment.

L. Gary Boomer, CPA, is a vice-president of Varney and Associates, a certified public accounting firm located in Manhattan, Kansas. He is also a member of the Information Technology Executive Committee.

The personal computer and local area networks (LANs) give firms increased data processing capabilities. We are in a "distributive processing" environment in which most jobs are processed on the desktop (personal) computer. All employees in the firm are involved. The capabilities of the hardware and software along with firm requirements are changing the way firms do business. Some of the most significant benefits of new technology include:

- Daily time sheet and interactive billing capabilities
- Interactive tax return preparation
- Interactive financial reporting
- Employee access to information
- Electronic mail and phone messaging.

New technology is introduced daily; therefore, firms must have the proper infrastructure in place in order to profitably apply it. Firms must view this undertaking as an ongoing commitment rather than as a one-time investment. Consequently, annual planning is a must. Engaging a qualified "outside" facilitator significantly reduces the amount of time involved in planning. In addition, LANs, other kinds of networks, application software, and employee training are all important issues that must be addressed.

A cost-recovery system, coupled with a planned rate of return on the investment, is also very important. Some firms have implemented an hourly "technology surcharge." The surcharge is calculated much the same way the "markup" on direct labor is computed. Assuming an average annual technology cost of $2.25 per hour, the surcharge would be calculated as follows:

Cost of technology per chargeable hour	$ 2.25
Multiplier	3.5
Technology surcharge	$ 7.88

It should be noted that $2.25 per chargeable hour is an average over a three-year period. The survey shows a range of $2.00 to $5.00 the first year, depending on the following factors:

- Prior years' investments
- How aggressive the firm's plan is with regard to purchasing a computer for everyone and providing the initial training.

Most firms are using a $5.00 to $8.00 per hour technology surcharge. Your time and billing package should calcu-

Automating A Tax Practice

To provide guidance to tax practitioners who wish to explore how specific computer systems can serve current and future tax environments, the Tax Division of the AICPA recently published *Automation of the Tax Practice of the '90s*. This report is organized to be applicable to first-time, as well as experienced users. Checklists are included to assist the practitioner in selecting tax planning and tax preparation software, as well as electronic tax research products.

The report is available from the AICPA Order Department (1-800-248-0445 in New York and 1-800-334-6961 outside New York). Its product number is 061050 and cost is $5.00 ($4.00 to AICPA members). IT

late the charge automatically. It is recommended that a special line item appear in work in process as a "technology surcharge" rather than simply adding it to each employee's rate. This serves as a reminder of the firm's investment in technology. Many firms have established a "no write-off" policy on the technology surcharge.

The questionnaire above will assist your firm in ascertaining its current level of technology sophistication.

If you can answer affirmatively to all of the above questions, your firm is definitely a leader in technology. However, if you respond negatively to many of the questions, and you wish to be a leader, you should place technology planning on the agenda at your next partners' meeting. IT

Assessing Your Technology Sophistication

1. Does your firm have a written three-year technology plan?
2. Does your firm budget annually for hardware, software, and training?
3. Does your firm use an outside facilitator for technology planning?
4. Has your firm set priorities and defined phases of implementation?
5. Does your firm have a personal computer/terminal for every person?
6. Has your firm implemented a LAN, and do you have an adequately trained network supervisor?
7. Has your firm developed a methodology for billing technology costs?
8. If so, does everyone understand and adhere to these policies?
9. Are your partners and staff technology literate?
10. Do you have a partner providing technology leadership?

Information Security: Responsibilities And Opportunities

By Albert H. Decker

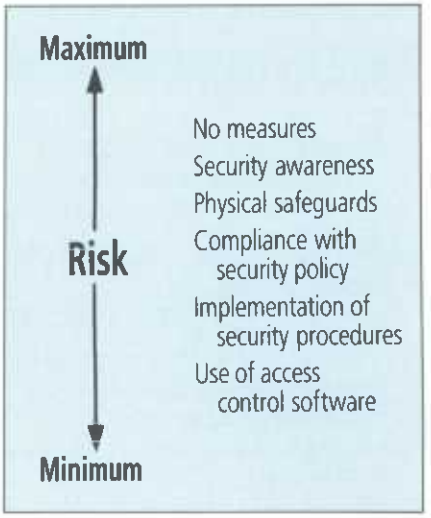
Computer technology continues to take on increasing importance since a vast majority of information is processed by and stored in computers. In today's environment, technology has become more reliable, and the risk of *inadvertent* loss, distortion, or corruption of data is relatively small. Threats to the integrity and existence of data from theft, accidental loss, employee sabotage, or corruption by viruses, however, create a new level of responsibility for management. It is incumbent upon management to assess those risks and to consider what policies, procedures, and controls need to be implemented to mitigate them.

From the organization's perspective, these risks present a "business risk" that should be addressed by management. In addition, for the auditor there may be another dimension: Professional standards such as SAS no. 55 require the auditor to assess broadly the client's control environment. One element of assessing that control environment is to consider information security issues.

Risk Assessment

Because of the growing importance of information security to most businesses currently using technology, each organization needs to make a detailed risk assessment and a plan to address the risks identified by this process. Of course, cost/benefit considerations are integrated into the assessment and planning process. The elements of a detailed risk assessment may seem complex when performing this task for the first time. However, there are many commonsense steps that follow from a risk assessment process that may be quite familiar.

The diagram below shows a basic principle of risk assessment and response: There are a variety of security measures (from simply a security awareness to the use of control software) that can be used to reduce risk. Some of these measures are relatively easy to implement. A significant reduction in risk can be accomplished in many businesses without the use of extraordinary physical controls or sophisticated software simply by increasing user awareness and implementing basic good business practices.



The risk assessment process is carried out from the perspective of the business entity. If an organization is making this assessment itself, it should also consider the interaction

continued on page 8

Albert H. Decker is a partner and director of National Information Technology Audit and Security Services at Coopers & Lybrand, New York, New York.

continued from page 7

of its business systems with the business systems of others, including any electronic links or shared data files between the organization and its suppliers or vendors. From the practitioner's perspective, the evaluation should take into account

1) how the CPA brings together and uses information, and
2) how the CPA interacts with the client.

For example, to what extent are client microcomputers or other computing facilities used by the auditor? Are data files shared by the client and the auditor? The first time the CPA reviews a client's security assessment, it may be important to have a technical security resource available to help ensure that the client's assessment is complete and accurate.

The fundamental approach to assessing information security risk is similar to the kinds of approaches to risk assessments CPAs make every day on a wide variety of business and audit issues. While the examples and descriptions that follow relate to the microcomputer environment, there are similar issues for mini and mainframe environments.

1) What am I protecting?

Identify the hardware, proprietary software, and information to be protected against loss or unauthorized access. Prioritize the criticality and sensitivity of the data. Not all data maintained by computer systems or transmitted electronically have crucial value. For example, in a service-oriented business, customer lists, including past patterns of purchases, might be a vital asset which the company wishes to protect against loss or piracy. In other situations, there may be a limited need to store electronic data *after* a hard copy report is printed. Different security responses may be needed when data are maintained electronically for an extended period.

2) Where is it?

Having identified the critical data, software, and hardware exposed to loss, identify where those assets are physically located. In the case of data, identify users and locations in the overall system from which the data can be accessed. For example, data may reside in stand-alone microcomputers, as part of a LAN, in a mainframe, or as part of a database supporting a network—all of which may affect risk.

3) What could go wrong?

Here's the fun part. Everyone is familiar with the kinds of things that can go wrong. For example, laptop microcomputers can easily "walk away," while mainframes do not have this risk. Computers are also subject to the failure of critical components which may affect the integrity of data files. Viruses are more likely to be introduced when programs and data are shared

MICROCOMPUTER SECURITY SOFTWARE MATRIX

FEATURES	ENVIRONMENT			
	Stand-alone Professional/ Administrative	Shared Administrative PCs	Shared Field PCs	Other
Single password or multiple user IDs/passwords				
Boot protection				
Screen locking				
Directory locking				
Program authentication (file integrity checking)				
DOS control				
Restrict copying of .EXE and .COM files				
File encryption				
Audit tracking				

among computers. Microwave data interception is becoming an increasing risk. Assess what could go wrong for each significant item identified in step 1 above.

4) What procedures/controls are in place?

Having identified the risks and issues to be addressed, analyze the existing policies, procedures, and controls that are functioning to lower the security risks. In many established mainframe EDP environments, there will be sufficient measures in place to ensure that the data in those systems are properly protected, provided the policies are followed and the control software is used properly. With microcomputers, a greater vulnerability may exist because of the tendency to rely on the user to address information security issues. In such environments, the quality of protection may vary significantly from user to user.

5) What are the remaining exposures?

Based on the risk assessment (steps 1–3) and the mitigating controls (step 4), identify the remaining exposures to security risk.

6) How should the exposures be addressed?

At this stage, match the remaining exposures with possible solutions. If, for example, a potential exposure to viruses is indicated, the solution may be to develop a policy in which good practices, such as limiting the installation of public domain software, are encouraged, monitored, and enforced. In addition, software packages may help the users of shared files (among microcomputers or different entities) to detect viruses on an infected disk. To protect against microcomputer theft, physical controls such as using door locks and equipment that secures microcomputers to desk units are potential solutions. To control access to the use of proprietary software and files, add or enhance password protection for computer systems. While influencing all steps of this process, cost/benefit considerations will be brought clearly into the picture at this stage. In many cases, adherence to good business practices significantly lowers existing security risks, even before more costly hardware and software solutions are considered.

After policies and procedures are developed and implemented, access control software may reduce risks further. One technique to assist in the evaluation of microcomputer security software is to create a matrix like the one shown on page 8.

While a number of access control software products are available, their features must be matched to the risks identified from the risk assessment. How microcomputers are used in the organization (e.g., as stand-alones, or shared) will influence the selection of a package. Features available on various security software products are listed on the left side of the matrix, and the different environments in which microcomputers are used in the organization are included along the top. Completing the matrix with "critical," "desirable," or "unnecessary" ratings helps to focus on security needs more carefully before selection of a security software package.

A Balanced Approach

Because of the impact of technology on business today, information security is vital. Actions to guard against security risk include simple awareness, physical safeguards, developing extensive programs of policies and procedures, and using control software. To be most cost-effective, the first steps taken should always be those that are quickest to implement and that provide the largest risk-reduction return for the expenditure.

There is one final concern. While security is important, there is a need to ensure that the solutions chosen to address the risks do not make the technology so difficult or cumbersome to employ that users are discouraged from taking advantage of what it has to offer. The approach toward information security needs to be balanced.

Balancing user needs and working practices with risk reduction can have a significant effect on a business' operations. The CPA approaching this subject with an informed perspective will better serve the organization. IT

System Auditability And Control Report

In 1977, the Institute of Internal Auditors (IIA) released a major research study to provide guidance to auditors who were learning how to deal with computer technology and its audit, security, and control issues. This first *Systems Auditability and Control* (SAC) report provided a detailed look at controls and auditing techniques, while defining the methods available at the time to look at computerized systems. It concluded that: Internal control responsibility rests with management; inadequate attention had been given to internal controls in automated environments; and new approaches, tools, and techniques are needed by auditors to evaluate and verify controls in data processing systems.

Today, general or information technology controls over EDP have evolved and are generally much improved. However, computer technology changes so fast that new and improved information is needed to help

continued on back page

continued from page 9

auditors address today's issues of control, security, and audit. In the context of this dynamic environment, the IIA decided that it was time to update the SAC report. In 1989, it engaged Price Waterhouse to perform this work. The completely revised and updated report clearly recognizes that the internal audit responsibility regarding information technology has expanded from 1970s-style back-office data processing operations control concerns to the situation at present, where computer technology is an issue at the highest levels of any organization.

The newly updated and revised SAC report includes the following modules:

1 *Executive Summary.* Management concerns and control points from each of the other modules, survey results, and management insights into current and future control issues.

2 *Audit and Control Environment.* A primer describing principles of auditing with emphasis on information systems auditing, control issues, auditing techniques, and major changes since the original SAC.

3 *Using Information Technology in Auditing.* Using the computer to audit and to support other audit efforts and activities. It also covers specific techniques, electronic workpapers, and audit support packages.

4 *Managing Computer Resources.* Managing and controlling physical computer assets and system software. Includes operations, data center management, computer types, and processing issues.

5 *Managing Information and Developing Systems.* Creation and maintenance of business data systems, strategic systems, data architectures, system engineering, and auditor roles in system development.

6 *Business Systems.* Application systems and their use, management, control, and audit. Includes guidelines for implementing and auditing software controls, with practical examples across industries.

7 *End-user/Departmental Systems.* Applications, hardware types, information centers, data center interface, personal computing, the role of intelligent workstations.

8 *Telecommunications.* Voice, data, and image transmission, as well as access to systems and data. Emphasis on networks, links, and emerging issues such as electronic data interchange and voice mail.

9 *Security.* Access controls, role of the security officer, legal issues, the Computer Security Act, and examples of risks such as fraud and abuse, viruses, and more.

10 *Contingency Planning.* Preparedness to recover from any and all disruptions of systems and communications services.

11 *Emerging Technologies.* Artificial intelligence/expert systems, voice recognition/response, image/pattern recognition, and emerging technologies in auditing.

The complete SAC report was issued by the IIA in May 1991. The list price for the entire report is $295. Individual modules are $45 each. The report is available for purchase from IIA, 249 Maitland Avenue, Altamonte Springs, FL 32701 (407) 830-7600. IT

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS
1211 Avenue of the Americas
New York, N.Y. 10036-8775