Microcomputer Security: Audit Problems and Solutions

Frederick Gallegos and Daniel Basica

The use of micros in business is increasing at an astounding rate as managers, clerks, and office workers enter the information age. Many tasks that were considered too small to automate on the company mainframe are now done with micros. But with computing power at everyone's fingertips, auditors and management must deal with the risks and exposures of micro use.

The security problems involved with micros are many, but management has audit methods and tools available to solve them. The first step is to identify audit problems, after which auditors and management must implement the necessary countermeasures

Audit problems with micros

Micros are vulnerable to risks of three major types:

- Physical security of hardware
- Physical security of data and software
- Data integrity

To establish a secure micro environment, planners must address each of these problem types with the appropriate strategies and equipment.

Physical security of hardware

Although micros pose unique hardware security problems, their solutions are relatively simple, requiring little more than good business sense.

Theft. Micros represent a large investment in small, often portable, packages that are easy to steal. Modular design adds further risks; for example, a half-height disk drive module can be hidden in a briefcase. Many micros have removable circuit cards and memory clips that could disappear just as easily. Employees may steal micro components because they have similar computers at home and want compatible equipment.

With computing power at everyone's fingertips, auditors and management must deal with the risks and exposures of micro use.

A micro used at a single workstation can be secured to the workstation or locked in a cabinet specifically designed to house a micro Also available are rolling, lockable cabinets that allow the unit to be used in different areas Although these measures do not eliminate the possibility of theft, they do reduce risk. A small investment in theft deterrence often provides adequate protection

Damage. Portable micros must be monitored closely because they are most often used away from the office Users of such equipment should be instructed in its proper care Problems can stem from heat, vibration, or shock, heat damage, for example, can occur if a micro is stored in the trunk of a car on a hot day.

Some computers have a routine that must be followed before they can be relocated. This rou-

tine usually involves moving the read/write head on the fixed disk drive to an unused portion of the disk or locking it so that it cannot damage the fixed disk drive or delete data.

Another problem with micros is their vulnerability to fluctuations in line voltage. Power surges can cause equipment failure as well as data loss. This problem can be remedied through the use of a surge protector, which filters the voltage. The micro is plugged into the surge protector, which is then plugged into an AC wall outlet Most of these devices are inexpensive and effective

Eating, drinking, or smoking near a micro can cause damage as well. Food and beverages are obvious hazards, but problems caused by cigarette smoke are not as well known. Diskette drives are especially vulnerable to damage from smoke because the space between the read/write head and the disk surface is much smaller than a smoke particle. A smoke particle lodged between the drive head and the disk could ruin both. Some users who have smoked near computers have never experienced problems, but the fact remains that smoke can be damaging. Eating, drinking, and smoking are prohibited in most mainframe facilities; the same rule should be in effect for micro installations

Physical security of data and software

The physical security of company data and software programs is often overlooked, yet diskettes packed with confidential information could be carried out of the office by an employee without detection. Micros are popular in departments that perform confidential operations, and, in the wrong hands, a confidential diskette could do great damage. Company-designed spreadsheet models are also likely candidates for theft. The risk increases when micros are networked or connected to the company mainframe.

Many firms implement extensive security measures to protect their mainframe computers and data, but relatively few safeguard their micros with similar controls Practices that are widespread in micro use (e.g., disks with no password protection, diskettes left on desktops, diskettes without proper labeling, and applications software stored in unlocked cabinets) would not be tolerated in a mainframe environment.

Micros represent a large expense in small, often portable, packages that are easy to steal.

Some common sense must be applied when micros are used to process critical or confidential data. Diskettes containing such data should be kept in locked drawers or in a safe, depending on the sensitivity of the data. In addition, various types of data security software are available for micros, including password protection, encryption/decryption schemes, and copy protection programs.

Password protection. Data files and programs can be shielded from unauthorized users by password protection software. Software features include password schemes for single-user or multiuser stations, multiple password levels, and audit trails Audit trails record such data as user ID, files used, duration of use, types of transactions performed, and denied accesses. Password protection is not as critical for diskettes because they can be physically secured, but if the system includes a disk, password protection software is highly desirable.

Data encryption/decryption. This type of program scrambles data into meaningless characters and symbols. A key must be used to restore encrypted code to a form readable by human beings or by other computer programs. Some packages use a federally approved standard while others use their own methods. Although encryption software prevents data from being read, encrypted data can still be destroyed or copied.

Copy protection. Copy protection programs prevent data files and applications software from being copied. Many different schemes are used, and some are harder to crack than others. Some vendors market packages that reputedly bypass copy protection schemes;

nevertheless, copy protection programs reduce the likelihood that data will be copied. Copy protection software is not appropriate for use on system software, however, because the copy protection feature could interfere with backup procedures.

Many commercially available software programs are protected by some type of copy protection scheme to prevent users from making illegal copies. Purchased software programs for micros are protected by copyright laws, and they include documentation defining the legal uses and backup procedures to be followed. Buyers should read the documentation supplied with the software to determine their legal rights and obligations. In many cases, programs are intended for use on one machine only; purchasers cannot legally make copies and use them on several machines.

Diskettes packed with confidential data could be carried out of the office without detection.

Software development companies have recently filed successful lawsuits against firms that have made multiple copies of programs. In one case, management was unaware that lower-level employees were making copies for themselves. Management must verify that purchased software is used according to the legal documentation provided by the manufacturer.

Local area networks. When micros are connected by means of a local area network (LAN), the security risk increases, and proper data security measures must be taken. At a minimum, password protection and an audit trail are necessary to maintain the privacy of confidential files and records. In addition, the LAN should support concurrent processing and the locking of various levels of files and records.

Micro-mainframe link. Linking a micro to the company mainframe can be both rewarding and devastating. When a terminal is connected to the host, data can be viewed only on the screen, but a micro equipped with the proper software and hardware can tie into the mainframe, find the desired information, and download that data to a diskette or fixed disk. Users can then do whatever they wish with the data after logging off the host. Thus, anyone with access to a properly equipped micro can obtain mainframe data unless extensive security measures are taken.

If a micro is linked to a mainframe, extra security steps should be taken to restrict and control access. A common method of connecting a micro to a mainframe is to use a modem to dial the host. A callback device can be installed on the host that receives the incoming call from the modem, breaks the connection, and then calls the modem back at a predetermined number. Although this prevents outsiders from dialing into the host, the host is still vulnerable to data theft from inside the organization. Another problem can result with a callback device: most of the communications software packages permit preprogrammed dial-up number and password sequences, and if these sequences are not secured properly, anyone using the micro can call up the communications program, which will automatically dial the host and supply the necessary passwords.

The importance of adequate security regarding a micro-mainframe link cannot be overstated. Security controls placed on the mainframe are useless if micro access is not properly regulated.

Data integrity

Assuming that data is physically secure, how can one be sure that it is current, accurate, and complete? A major problem with regulating micros is that in many cases one person is the programmer, systems analyst, and end user. The typical separation of duties in mainframe systems development does not exist in the world of micros. Moreover, many users are not experienced computer operators.

Data compatibility. To provide the most effective control of data with micros, a company should decide on a standard hardware and software configuration. For example, the data produced on the accounting department's Ap-

ple III with a VisiCalc program is not very useful to the IBM Personal Computer running Lotus 1-2-3 in finance. A planning committee should define organizational requirements and then choose the appropriate hardware and software. Neglecting to do so results in repetitive data keyed into each of the incompatible programs.

Data backup. Many micro users realize the importance of data backup only after disaster has struck. Data files should be backed up every time the file is used. It is best to keep at least three "generations" of data—grandparent, parent, and child. In the unlikely event that the parent and child are destroyed, the most recent sets of transactions could be reapplied to the grandparent. Ideally, each generation should be kept in a different location. It is also advisable to retain all transaction documents in case a file must be rebuilt. Each generation should be labeled clearly in order to avoid using obsolete data to process current transactions.

Anyone with access to a properly equipped micro can obtain mainframe data unless extensive security measures are taken.

New users should be instructed to save their work at frequent intervals as a safeguard against power or equipment failure. The effort required to save a file every 20 to 30 minutes is a small price to pay to avoid the frustration of losing an entire afternoon's work.

Program backup. Purchased software programs should be backed up when they are received. As discussed earlier, these programs supply documentation outlining the buyer's rights and obligations, as well as backup procedures. In many cases the software company will provide a backup copy for a nominal fee; the copy should be stored in a safe place.

User-written programs should be backed up when completed, and a new backup copy should be made when any modifications take place. Any modification to a program must include updating the documentation.

Computer models and user-written programs. End-user programming can lead to data errors that are difficult to detect. For example, a user may design an excellent spreadsheet model, but incomplete testing could result in a program that works only part of the time. Unaware of the problem, everyone concerned would assume that the data from the spreadsheet program was correct. More than one firm has made major decisions based on incorrect micro data.

User-written micro programs must be designed with the same care as those of mainframe systems. Each program must be thoroughly tested before it is used and should be accompanied by complete documentation, including:

- All assumptions of the program
- A program listing
- Sample transactions
- A narrative description

Programs should be audited periodically to verify correctness of data. When a program is modified, it must be retested and the documentation updated.

Many micro programs are written in an interpreted version of BASIC. This can be dangerous because anyone using the program could modify it. It is much safer to use a compiled version of the program and remove the source code from the system. In addition, a compiled program can be executed more quickly than an interpreted one. The benefits derived from a compiler easily outweigh the cost of purchasing one.

Use of current data. All data and program disks must be labeled clearly to avoid using old data or a superseded version of a program. Care must be taken when generations of backups are used so that only the most recent data is used. Old tax tables or outdated inventory pricing can cause costly errors.

Auditing tools. The micro market is growing much faster than audit tools for micros are being developed. Currently, few audit packages are available. Most of the software being written for micros is geared to mass marketing, and audit utilities offer only a small vertical market.

Recently, however, some programs have been written that aid in auditing the formulas in spreadsheet models. Two of these programs are Micro Decision Systems' Docucalc and Consumer Software Inc's Spreadsheet Auditor, written for the Apple and IBM Personal Computer, respectively.

Many micro users realize the importance of data backup only after disaster has struck.

For the most part, auditors must make use of the programming tools that are currently available, including cross-reference, file recovery, disk explorations, sort/merge, file dump, and other utilities. Fourth-generation languages, statistical packages, and report writer programs can also be helpful to auditors. Micro versions of some mainframe programs, such as SPSS, FOCUS, and SPF, are available; auditors familiar with the mainframe versions can use the micro versions with little or no training. Some ambitious EDP auditors have even written their own programs or extension commands to operating systems to fill the void until more software is available.

Conclusion

Ready or not, auditors and managers must provide security measures as micros continue to move into the office. Careful planning and control of micros can lead to increased productivity and better business decisions.

The accompanying box contains a partial listing of software and hardware available for micros. Obviously, this list should not be considered comprehensive because new products are constantly being released.

Frederick Gallegos is manager, Management Science Group, U.S. General Accounting Office, at its Los Angeles regional office. He is also a trustee for the EDP Auditors Foundation for Education and Research. He earned his bachelor's degree in data processing and his master's from California State Polytechnic University, Pomona.

Daniel Basica is a microcomputer support analyst for Denny's Inc, La Mirada CA. He earned his BS in computer information systems, specializing in accounting and auditing, at California State Polytechnic University, Pomona.

Physical Security Devices

Switch Security, Model 144
Protects on/off switch on computer, $39.95
SE-KURE Controls Inc
5685 Lincoln Ave
Chicago IL 60659
(312) 728-2435

CompuCart
Locking cabinet for micro, wheels for portability, $595
Smartware Inc
557 Howard St
San Francisco CA 94105
(415) 974-1500

Computer Security Alarm
Motion detection device sets off alarm if computer is moved, $125
Smartware Inc
557 Howard St
San Francisco CA 94105
(415) 974-1500

PC-LOK
Locks micro cabinet and power switch, no drilling required, $99
Qualtec Data Products Inc
1116 Olive Branch #3
San Jose CA 95120
(408) 973-0456

AC Surge Protector
Filters voltage peaks from AC current, $147
Black Box Catalog
PO Box 12800
Pittsburgh PA 15241
(412) 746-2910

Datashield Power Source, Model 200
Provides 30 minutes of power, $349.95
Jameco Electronics
1355 Shoreway Rd
Belmont CA 94002
(415) 592-8097

Uninterruptible Power Supply, Model 1350
Supplies continuous power in case of power failure, $750
Dymarc Industries Inc
21 Governor's Ct
Baltimore MD 21207
(301) 298-9626
(800) 638-9098
TWX: (710) 234-1990

Surge Suppressor
EMI/RFI filtering, 6 plugs, $29.95
Digatek Corporation
2723 W Butler Dr
Phoenix AZ 85021
(602) 995-8371

Transient Voltage Protector
6 outlets, eliminates voltage spikes, $63
Expotek Inc
2017 Cactus Rd
Phoenix AZ 85022
(602) 528-8960

Data Security—Port Protection Devices

Gateway
1 port, 20 access codes, $395
Adalogic
559 Union Ave
Campbell CA 95008
(408) 377-3050

Dialsafe 3 Plus
3 ports, 65 access codes, optional to 200, $895
Backus Data Systems Inc
1440 Koll Cole #110
San Jose CA 95112
(408) 279-8711

Entercept
1 port, 1 access code shared by all, $595
Integrated Applications Inc
8600 Harvard Ave
Cleveland OH 44105
(216) 341-6700

Multi Sentry
16 ports, expandable to 128, 1,000 access codes, $21,500 ($1,343 per port)
International Mobile Machines Inc
100 N 20th St
Philadelphia PA 19103
(215) 569-1300

Lineguard 3000
3 ports, 100 access codes, $1,120
Western Datacom
5083 Market St
Youngstown OH 44152
(216) 788-6583

Barrier
1 port, 1 access code shared by all, $369
International Anasazi Inc
2914 E Katella Ave
Orange CA 92667
(714) 771-7250

SAM (Secure Access Multiport)
22 ports, expandable to 64,256 access codes, optional to 2,304, $13,750 ($625 per port)
Lee Mah Inc
729 Filbert St
San Francisco CA 94133
(415) 434-3780

Oz Guardian
1 port, 160 access codes, modem included, $750
Tri-Data Inc
505 E Middlefield Rd
Mountain View CA 94039
(415) 969-3700

Data Encryption

DATA-LOK
Protects single files or groups of files, MS-DOS, $69
Qualtec Data Products Inc
1116 Olive Branch #3
San Jose CA 95120
(408) 973-0456

Encrypt-It
Communications package and IBM PC expansion board, can use for electronic mail, $1,160
TLC Inc
Ellis Sarasota Bank Bldg
Sarasota FL 33577
(800) 237-4433
(800) 282-8432

P/C Privacy
Available for IBM PC MS-DOS, CP/M-80, and Apple-DOS 3.3, $140
MCTel
Three Bala Plaza East
Suite 505
Bala Cynwyd PA 19004
(215) 668-0983

Public Key Encryption
Use for disks or data transmission, choose levels of security, $199
Datamorphics Ltd
PO Box 820
Stittsville, Ontario
Canada K0A 3G0
(613) 836-3270

IRE Scrambler
Uses FIPS 46 standard, Model SC-12 to 1,200 bps, $495
Industrial Resource Engineering Inc
PO Box 57
Timonium MD 21093
(301) 561-3155

Watchdog
Menu driven, partioning of data, for IBM PC and PC XT, $295, quantity discounts available
Fischer-Innis Systems Inc
4175 Merchantile Ave
Naples FL 33942
(800) 237-4510
(813) 793-1500

Copy/Password Protection

Bit-Lock Security
Multilayered security, works on IBM PC and PC XT, TRS-80, Apple, and Commodore, price not available
Microcomputer Applications
7805 S Windermere Ccle
Littleton CO 80120
(303) 922-6410

Padlock
Protects against DOS commands, $99
Padlock II
Diskettes come protected with "fingerprint" and serialization, price not available
Glenco Engineering
3920 Ridge Ave
Arlington IL 60004
(312) 392-2492

Prolok
Uses "fingerprint" method, backups made accompanied by original disk, price not available
Vault Corp
2649 Townsgate Rd
Suite 500
Westlake Village CA 91361
(800) 445-0193
(800) 821-8638

Copy II Plus and Copy II PC
Backup copy protected programs, for Apple II, Plus, IIe, and IBM PC, $39.95
Central Point Software Inc
9700 SW Capital Hwy
Suite 100
Portland OR 97219
(503) 244-5782

Copywrite
Backup copy protected programs, IBM PC or PC XT, Corona, or Columbia, 64K and 1 drive, revised monthly, $50, $12 for updates
Quaid Software Ltd
45 Charles St E, 6th Floor
Toronto, Ontario
Canada M4Y 1S2
(416) 961-8243

Copy Protection
Protects PC and MS-DOS .COM and .EXE files from copy programs such as System Backup, Copy-PC and other programs, requries 64K, $799
Soft Design Co
See dealer for more information

Backup Devices

Sysgen II-6
20MB disk includes tape cartridge backup, other configurations available, prices vary according to options
Sysgen Inc
47853 Warm Springs Blvd
Fremont CA 94539
(415) 490-6770
Telex 4990843

Tallgrass Hardfile
6MB to 70MB with built-in tape system, backs up entire drive or individual files, 35MB and backup, $5,745
Tallgrass Technologies Corp
11100 W 82nd St
Overland Park KS 66214
(913) 492-6002
Telex 215406 TBYT UR

Quentin Q-400, Q-500, Q-700
Up to 20MB fixed disk with streaming tape backup, for IBM, Apple, and Franklin computers, prices vary according to options
Quentin Corp
9207 Eton Ave
Chatsworth CA 91311
(818) 709-6500

Mountain MT-4000-04
35MB fixed disk with backup tape system, backs up 20MB in 6 minutes models from 10MB, $5,595
Mountain Computer Inc
300 El Pueblo Rd
Scotts Valley CA 95066
(800) 458-0300
(800) 821-6066
(408) 438-6650
TWX (910) 598-4504

Ampex PC Megastore
20MB disk with 25MB tape backup; tape is addressable, allowing access to archives, price not available
Ampex Computer Products Div
200 N Nash St MS M-11
El Segundo CA 90215
(800) 421-6863
(213) 640-0150

Vision Series
Disk and tape backup units from 10 to 140MB, 11MB tape backup sells for $1,995
Pacific Datanet Ltd
4701 Patrick Henry Dr, Bldg 9
Santa Clara CA 95054
(408) 980-0693
Telex 759341

Compilers

Microsoft FORTRAN
MS-DOS, based on 1977 standard, supports 8087 coprocessor, $350
Microsoft Corp
10700 Northup Way
Box 97200
Bellevue WA 98009
(800) 426-9400
in WA call (206) 828-8088, ask for operator C6

mbp COBOL
Generates native machine language object code, includes SORT and CHAIN, $750
mbp Software and Systems Technology Inc
7700 Edgewater Dr
Suite 360
Oakland CA 94621
(415) 632-1555

Mark Williams C-Compiler
Supports 8088, 8086, 68000, PDP-11, Z8000, CP/M and PC-DOS, price not available
Mark Williams Co
1430 W Wrightwood Rd
Chicago IL 60614
(312) 472-6659

db COMPILER
Compiles dBASE II programs, no license fees, cross-linkers available, $750
Wordtech Systems
PO Box 1747
Orinda CA 94563
(415) 254-0900

Raging C
For MS-DOS machines, implements most Unix-compatible functions, $500
Microsoft Corp
10700 Northup Way
Box 97200
Bellevue WA 98009
(800) 426-9400
in WA call (206) 828-8088, ask for operator D5

Compiler/C86
Basic compiler for CP/M, MP/M, PC DOS, MS-DOS, need 2 drives and 96K, output relocatable, 8088/8086 object code, $395
Computer Innovations Inc
See dealer for more information

Programming Utilities

SYMD Symbolic Debugger
Identifies programming errors, profiling, for PC DOS or MS-DOS, 1.1 or 2.0, requires 192K and 80-column display, $125
D+V Systems
400 Amherst St
Nashua NH 03063
(603) 811-7140

Cross Reference
Use on ASCII or binary files, produces alphabetic of variables and line numbers, indicates arrays, requires IBM PC, 64K and 1 drive, $24 95
Ensign Software
2312 N Cole Rd
Suite E
Boise ID 83704
(208) 378-8068

Code Smith-86 1.8
Symbolic debugger, pass points and execution path counters, dump to disk, requires MS-DOS and 160K, $145
Visual Age
642 N Larchmont Blvd
Los Angeles CA 90004
(213) 439-2414

Disk Mechanic
Backup, compares and copies zero sectors, repairs damaged disks, alters "hidden" status, recovers "erased" files, requires IBM PC or COMPAQ with 192K, DOS 1 1 and 2 drives, $70
MLI Microsystems
PO Box 825
Framingham MA 01701
(617) 926-2055

PC Versions of Mainframe Software

SPSS/PC
Features and language compatible with mainframe SPSS, transfers files between Lotus 1-2-3, dBASE II, and SAS; complete report writer, price not available
SPSS Inc
444 N Michigan Ave
Chicago IL 60611
(312) 329-2400

PC/FOCUS
Compatible with mainframe FOCUS, can download or upload data and programs, report writer, statistical analysis, relational data base, $1,595
Information Builders Inc
1250 Broadway
New York NY 10001
(212) 736-4433

SPF/PC
Works like TSO/SPF editor on IBM mainframe, 4-way scrolling, split screen, 240-character records, block commands, DOS utilities, upload and download, $149.95
Command Technology Corp
1900 Mountain Blvd
Oakland CA 94611
(415) 339-3530

FSE/PC
Full-screen editor combines features of FSE, SPF, ICCF, and CMS, maximum file size 32,767 records, full set of block commands, $125
Data Processing Development Corp
909 N Mayfair Rd
Milwaukee WI 53226
(414) 778-1175

Statistical Software

StatPAC
Modeled after SPSS for use on micros, up to 5,000 cases and 255 variables on IBM PCs, price not available
Walonick Associates
5624 Girard Ave S
Minneapolis MN 55419
(612) 866-9022
(800) 328-4907

ELF—The Statistical Package
Reads and writes VisiCalc, SuperCalc, Multiplan, dBASE II, and others, performs regression, correlation, factor analysis, probabilities, and more, price not available
The Winchendon Group Inc
PO Box 10339 #200
Alexandria VA 22310
(703) 960-2587

Micro Audit Tools

dFLOW
For dBASE II and dBASE III programs, locates coding errors, logic mismatches, $50
Wallsoft Associates Inc
233 Broadway
Suite 869
New York NY 10279
(212) 406-7026

DocuCalc
For Apple computers, displays formulas for easy verification, price not available
Contact dealer for more information

Spreadsheet Auditor
For the IBM PC and PC XT, works with VisiCalc 3 and others, produces matrix of formulas, $99
Consumer Software Inc
8315 Monterey
Gilroy CA
(408) 848-3384

Compare Master
For IBM PC BASIC programs, displays differences between two files in report, $34 95
N.F Systems Ltd
PO Box 76363
Atlanta GA 30358
(404) 252-3302

The Profiler
Allows performance tuning of programs, can select most used modules for auditing, requires IBM PC, 64K and 1 drive, $175
DWB Associates
PO Box 5777
Beaverton OR 97006
(503) 629-9645

Bruiser and Blister
Bruiser removes REM statements from BASIC programs, Blister provides documentation from source listing, $25 both or $15 each
Diversified Data System Inc
5227 Buchanan Rd
Delray Beach FL 33445
(305) 498-2772