Security considerations for personal computers

by W. H. Murray

The wide use of personal computers and general access to telecommunications links have intensified the need for computer security. Security practices as discussed in this paper relate to protecting an organization's personal computers as physical property, protecting the organization's data and applications, and protecting the organization itself. These matters are discussed from the point of view of protection from the improper use of personal computers.

Users and managers of personal computers are becoming increasingly aware of the necessity to protect the computers, their applications and data, and the organization from unauthorized or unintended events.[1-6] In this paper we deal with the identification and selection of protective practices. This process begins with the identification of the resources to be protected and the hazards to be avoided. The personal computer is itself valuable and therefore must be protected from damage, destruction, misuse, or conversion. It also contains data that must be protected from modification, destruction, or disclosure, as well as applications that likewise must be protected from tampering or interference. And, of course, the business organization, its other computers and applications and their data, must be protected from failures, errors, or malicious acts related to personal computers on the part of their users.

Protecting the personal computer

Because the personal computer is a valuable piece of office equipment, it should be protected as valuable property. As it is for office equipment, this protection is usually afforded by the normal office environment. Whereas special protection may be required for the data—as later discussed in this paper—it is not normally necessary for the equipment. However, protective shells and cabinets are available and should be used as required.[7,8]

Some people assume that because a personal computer is a "computer" it must be placed in the same kind of protective computer room environment as is normally provided for large-scale computers, including special environmental conditioning, fire suppression, and personnel access controls. Such a level of protection is not usually necessary for personal computers. First, because they are low-power devices, they generate less heat than a light bulb. Second, they are designed for use in a wider range of temperature and humidity than is usually found in an office. Third, personal computers are neither more vulnerable to fire nor more likely to cause a fire than other office equipment. Finally, personal computers are neither more valuable nor more sensitive to interference than other office equipment. Copiers, for example, often cost more than personal computers as well as having some potential for interference and abuse. In comparison with a large computer, large-scale systems incorporate highly privileged override controls. These privileged controls are reserved to management to protect one user from others. On the other hand, personal computers normally have a single user, and all controls are reserved to that user.

As for insurance, the same kind of insurance that covers other office equipment also covers personal computers.[9,10] Many large organizations self-insure their office equipment. Other companies insure under policies with broad coverage that include personal computers along with other office equipment. Although it is good practice to check, only rarely is special coverage necessary. Most homeowners' policies cover personal computers in the home except where they are used for business or are otherwise specifically excluded.

Protecting data

Data must be protected from unauthorized or unintended modification, destruction, or disclosure.[11] The consequences of such tampering with the data are more a matter of the data themselves rather than of where they are stored. The expected rate of problems, however, varies with the nature of the media on which they are stored.

In primary storage. Data in primary storage are invisible except as displayed. These data can be destroyed by a power loss, a power surge, or even a jolt of static electricity. Personal computers may be more vulnerable to static electricity than other terminals or systems. Such losses are usually only annoying, but could be costly if static were to occur several hours into a long job that had no checkpoints. The risk of static electricity can be limited by an appropriate environment. Although backup power is not often used for personal computers, it is available. Power surge protectors are also available and may be used if necessary. The best protection against data destruction is to keep copies.[11] Thus, data in primary storage should be periodically saved on secondary storage.

On diskette. All other things being equal, data are less sensitive to accidental disclosure when stored on diskette than when stored on paper. On the other hand, data stored on diskette may be considerably more vulnerable to accidental erasure than the same data stored on paper.

Data recorded on diskette are usually protected from disclosure by removing the diskette from the computer and storing it in a safe place, as though the data were on paper. Occasionally disks may be used or shared in such a way as to make off-line storage infeasible, in which case the data are protected in a manner similar to that recommended for fixed disks.

Data stored on diskette may be protected from modification and destruction by the preparation of backup copies. Usually, one or two extra copies are all that are required. Since computers are very good at preparing cheap, dense, portable copies, backup copies are not unduly expensive. Thus, the risk of destruction can be made very low by producing many copies and dispersing them widely, but this low risk is achieved through an increased probability of disclosure.

Some protection from erasure can be gained by making a copy of the data on the fixed disk itself.

On fixed disk. Data on a fixed file must be protected from accidental erasure, from failure of the device that would make it unrecoverable, and from disclosure.

Protection from erasure. As with data on diskette, data on a fixed file are protected from erasure by making copies. Some protection from erasure can be gained by making a copy of the data on the fixed disk itself. The usual practice, however, is for the copy to be placed on a diskette.

Protection from device failure. Copies on diskette are also the usual form of protection against the failure of the device itself. This is usually done by storing on a diskette with scheduled frequency those data sets that have been opened for writing since the last scheduled backup. This capability is usually provided by the operating system (including PC-DOS).[12] The frequency of backup is selected so as to balance the time required for the backup against the updates that could be lost. Given the low incidence of failure of such devices, we have found that running the backup program at least once per day or once for each session is reasonable.

Although daily or by-the-session backup is the general method for large, fixed disks, it is limited to use

with large numbers of small data sets. For a small number of large data sets, the amount of data that must be written is usually large compared to the amount of data that has actually changed. Therefore, for such applications, dumping the whole file onto a tape may be the more economical method. The added cost of the tape drive may be justified on the basis of the time savings in writing large files on tape rather than on diskette.

For systems that are connected to other systems, consideration should be given to the use of those other systems for the storage of backup copies of files. This procedure use can vary in sophistication from simply uploading a file to complete applications that provide schedule management and security.

In the worst case, when it is necessary to recover a file, the time to recover is not important in the backup decisions. Recovery is done infrequently, whereas backup is done frequently. When recovery is necessary, the fact that it can be done at all makes the time required seem trivial.

Protection from disclosure. Because fixed files cannot be removed for protective storage, it is often preferable to store confidential data on diskette. However, the greater speed and size of the fixed file may justify the use of other protective measures to protect confidential data.

Safe environment. The simplest way to protect confidential data on a fixed file is to lock the room in which the file is kept. Where it is not possible to limit access to the premises where the file is kept, smaller protective environments may be used. Cabinets for personal computers and the contents of their files are available that offer protection against theft of the device itself as well as the files.[8]

Power locks. Casual browsing in a benign environment, such as a personal office in a secure building, can be prevented by mechanisms that control access to the power to the personal computer. Such devices provide lock-and-key control over the power. They may also be used with complementary devices that sound an alarm if the device is disconnected from its intended power source. In an attended environment, these devices also offer some protection against theft of the device itself.

Access control. Where concern is limited to the data rather than the property, conventional access control mechanisms or encryption may offer the most economical protection.[13–17] Access control may be used where the device and the data are shared by several users. Not only can it exclude unauthorized users, but it can also control sharing among users. Because there is a measurable performance penalty, such access control should be reserved for situations involving the sharing of a personal computer and data.

Access controls for personal computers may resemble those for larger systems, whereby each user receives an identifier and/or a password. However, because all users have the ability to replace the operating system with one of their own choosing, identifier-password mechanisms rely upon encryption of the files for their integrity. A file on a fixed disk is encrypted under a key belonging to the access-control mechanism. This mechanism can deliver the file in the clear text to those specified by management as having legitimate access only. Thus, a user employing his own operating system to bypass the access-control mechanism can access the encrypted file only.

Encryption is also applicable where data on portable media pass beyond the control of the owner.

File-by-file encryption employing private keys managed by the user may have an economic advantage over full access control where only a small percentage of the data is confidential and where only the device is shared but the files are not. This kind of encryption is also applicable where data on portable media, such as diskettes, must pass beyond the control of the owner and his trusted associates and to confidential files passing across communication lines.

Protecting applications

All applications must be protected from interference or contamination from outside themselves. Most such interference is unintentional rather than mali-

cious, and annoying rather than damaging. Nonetheless, the potential exists for one application to so interfere with another as to invalidate the results, make them unusable, or even dupe or mislead the user.

Applications on a personal computer must be protected from other applications running in the same system or in communicating systems. Whenever two applications share storage, it is at least conceivable that an action of one will damage data belonging to the other.[18-20] Computers that are intended for concurrent use by two or more users often implement isolation schemes to prevent this interference. Most systems that are intended for use by a single person at a time do not provide such process-to-process isolation.

To control a communication, one must control the procedures being executed.

Allocation of resources to processes, programs, or tasks. Therefore, the user is responsible for protecting himself from himself by allocating his resources so as to maintain the required isolation among programs. For example, a user can place programs and data for different applications on separate diskettes. On a larger scale, one can allocate the whole machine to an untested program of which the results are unpredictable. The user may test together programs intended to run together, so as to be confident that they do indeed run properly together. After taking these precautions, if one program should interfere with another, the consequences are limited to the user himself, who is best able to correct the situation.

When a program has been written by a person other than the user, the user must protect himself against the behavior of that program. He can protect data from inadvertent modification by removal from the system, and he can protect against disclosure of the data by limiting access to the system to himself. He can protect himself from being duped by verifying the results.

Most of these precautions continue to hold true even when the personal computer is connected to a communications link. The user continues to be in control; all program actions are visible to him and require his cooperation. Nonetheless, the user can protect himself as he does when speaking on the telephone. He talks only to whom he intends; he gives only the data he intends; and he strives to protect himself from being deceived.

Control communications. A user should know with whom he is speaking, and he should originate calls or receive expected calls only. Most systems that a user calls expect data identifying him and authenticating his identity, and the systems respond with confirming data. For example, if a user dials a number and receives the expected data tone, he has probably reached the intended system. If, however, he does not receive the expected prompt, he may wish to hang up and try again. In response to the expected prompt the user must enter his identifier and password. In return, the system transmits such authenticating data as the time and date of the user's last use of the system. If the time and date received are not those that are expected, the user breaks the connection and reports his password compromised. For systems that do not offer such authenticating data, the user may compensate by looking for data that he placed in the system (preferably in the previous session) or by inquiring for data that only he and the legitimate system are likely to know.

At all times, the user retains control of the data transmitted and, in turn, transmits only intended data. In order to control a communication, one must control the procedures being executed. Therefore, users should not execute data received during a communication with a second party. Only exceptional compensating controls or a high level of trust justify deviation from this rule.

Protecting applications from the personal computer

Likewise applications running in a communicating system must be protected from applications running in a personal computer attached to the system. In general, all the controls necessary in any on-line system are also necessary when talking to a personal computer. However, a personal computer can emu-

late the behavior of a terminal and that of its user, and it can be programmed to mount an exhaustive attack, such as by finding an expected answer by exhausting the set of unexpected answers. Therefore, on-line system controls must be rigorously applied. For example, in a system connecting with dumb terminals only and in which passwords are changed frequently, it may be reasonable to be tolerant of user errors when signing on. However, a system connecting to personal computers or to dial-up lines to which they may be connected must be intolerant of such errors. Otherwise the system may be vulnerable.

Two persons should not share the same identifier, even where they share the same privileges and data.

To date, much of the software that enables a personal computer to emulate a terminal requires that the personal computer be dedicated to that emulation. That is, the software permits the personal computer to function as a terminal or as a computer, but not as both at the same time. Thus such software does not support an exhaustive attack. Inasmuch as software to permit the personal computer to function as both a terminal and a computer at the same time is both desirable and feasible, it is wishful to expect this either-or situation to persist for very long.

The controls required to protect all on-line systems operating in environments assumed to be hostile are well documented.[21-29] Those controls are sparsely and inconsistently applied in most systems. On the other hand, the environment is becoming increasingly open, and, with an exploding population of personal computers that environment is potentially more hostile. Therefore, some special cautions are in order.

User identification. To protect the organization, personal accountability is becoming increasingly important in protecting applications in an environment that includes personal computers. Therefore, each individual who uses these applications must have a *personal identifier.* Personal identifiers, together with node names if used, are like addresses that persons use when writing letters to one another. In a computer, the implicit assumption is that each addressee has been previously authenticated. Under no circumstances should two persons share the same identifier, even where they share the same privileges and data.

End user authentication. For me to use the system, I must first satisfy the system that I am who I say I am. To do this I must have my own secret *password.* My password is not my address. It authenticates me to the system, and it is known by me and the system only. Passwords should be randomly chosen, frequently changed, and long enough to resist a personal-computer-assisted exhaustive trial-and-error attack lasting the entire life of the password. Passwords of three or four characters are not likely to be able to meet this test unless chosen from a large character set or changed frequently.

Access control. Again, because of the potential for exhaustive attacks, authorization to resources should be by means of a list or algorithm that associates the resources with the user name or identifier. This procedure should be used rather than relying upon passwords or lockwords assigned to the particular resources—data sets, files, commands, transactions, or privileges. Because of the potential for high-speed browsing, access rules should have safe defaults. An access default which has been found useful is that access should be implicitly restricted except as explicitly granted, rather than implicitly granted except as explicitly denied.

Administration. Because control is likely to be widely dispersed both organizationally and geographically, administrative procedures for adding and deleting users and granting and revoking authority must be both timely and consistent.[30-32] Special consideration should be given to the procedures for revoking identities and authorities for terminated users or for accounts believed to be compromised. Management must be able to recognize attacks in progress and take prompt, effective, and efficient corrective action. This may involve the most difficult set of choices that management must make. The system itself can aid management by incorporating only those procedures that do not "cry wolf." Too many false alarms condition management to believe that most alarms are false. Therefore, alarm thresholds for denied accesses must be set low enough to permit timely

intervention, yet not so low as to generate too many false alarms. Maintaining management alertness is difficult, but it is not impossible. Alertness requires constant attention to detail and adjustment of the system.

Protecting the organization

In addition to protecting the personal computer, data, and applications, the organization itself must be protected from the potential negative consequences of careless, fraudulent, hostile, unlawful, or unethical uses of the personal computer. These are acts that, although authorized in the sense that all the controls previously discussed are being applied, may still be unintended and damaging to the organization. For example, if the vendor of a licensed software item finds a pattern of copying of that software in violation of an agreement with the organization, he might have cause for action to recover lost revenue. From the point of view of the organization, copying may be permissible or even desirable under the controls discussed. Therefore, additional controls may be required to protect the property rights of vendors and to protect management from charges of disregarding those rights.

Simultaneous connection to two or more systems requires the approval of the managers of those systems.

Policy. Most employees want to do what management intends, and, if a sufficient number do act honorably, the organization will be safe from hazards. When employees fail to do what is expected, it is often because of a failure of management to communicate the expectation properly rather than through a failure of motive or intent. Where a failure of intent is involved, it is often associated with unnecessary temptation.

Therefore, it is wise for an organization to have a clear policy about the use employees are to make of organizational resources and the behavior expected of employees. Such a policy should be so designed and implemented that it holds the employees clearly accountable for their actions. Most organizations already have such policies in place, but the application of personal computers may so change the way people work as to obscure the intended application of those policies. Again, to use the example of a vendor's property rights, an organization may have a policy that their employees will abide by the terms of all contracts and agreements entered into by the organization with its vendors. That this policy applies to personal computer programs may not even be noticed by most employees. Therefore, management may wish to communicate explicitly that employees are not to copy programs in violation of license agreements.

Guidelines. Hypothetical or suggested guidelines for employee behavior and responsibility with regard to personal computers are presented as follows:

- Employee obligation to adhere to the spirit as well as the letter of all applicable laws, regulations, contracts, licenses, policies, standards, guidelines, business controls, security rules, and other expectations.
- Restricted use of hardware, for example, to business use only.
- Rules concerning connection to other systems. For example, a connection rule might be that personal computers are to be connected only to systems specifically authorized by the appropriate management. Simultaneous connection to two or more systems would require the knowledge and approval of the managers of those systems. Simultaneous connection to a computer of this organization and a foreign system (including user-owned personal computers) would require the approval of the director of information systems.
- Responsibility for the security of hardware, software, data, and other resources.
- Responsibility for data integrity to include correctness of computer results and updating of remote data bases via authorized software and procedures only.
- Identification of the source of data. Preparers of reports must label them properly according to their source (i.e., the identification of the preparer, the systems used, and the data used) and according to the persons who authorized the reports and who are prepared to vouch for their integrity (i.e., manager, business function, or official). Users of data are responsible for proper identification and authorization of the source of the data.

- Ownership of work products. The institution is the owner of all data used or created.
- Management responsibility for controls, supervision, and corrective action. A manager's responsibility to preserve, conserve, and control resources may include personal computers. Managers may be held responsible for authorizing the purchase and use of personal computers.[33] They may also be held responsible for the appropriateness of use and the correctness of the results produced. They are responsible for effective controls, adequate audit trail, timely detection of variances, and necessary corrective action.
- Employee responsibility to report to responsible management all variances from the expected behavior, use, or content of the system.

Of course most of these things have always been implicitly expected and in a legal and ethical sense need not be restated. Nevertheless, it may be useful or even necessary to restate them in the context of the personal computer. When batch applications were the norm, and when all computer-generated output was derived from centralized, well-controlled machines, and when all reports prepared by individuals were handwritten or typed, there was little chance that a user of data would mistake a printout for a prepared report. Labeling and checking were less necessary then than now, when it is possible to go from a mental concept to four-color slides in minutes.

Concluding remarks

Most of the uses and effects of the personal computer are expected to be benign. If this were not so, its use would be so limited as to constitute no problem. Nonetheless, users and managers must be sensitive to the potential hazards and do what a prudent individual would do in the face of those hazards. A safe environment and insurance reduce the risk to the property. A safe environment, protective storage, access control, and encryption limit the risk of loss of confidentiality. Proper copying protects against erasure or destruction. Accountability, checking, and prompt corrective action help to ensure integrity. Finally, a clear communication of policy and intent provide good protection against misuse.

Cited references

1. L. I. Krauss and A. MacGahan, *Computer Fraud and Countermeasures*, Prentice-Hall, Inc., Englewood Cliffs, NJ (1979).
2. D. Neibaur, "Micro installation requires careful planning," *Computerworld* **17,** No. 13, 41–42 (March 1983).
3. M. Zientara, "DP managers encouraging personal computing," *Computerworld* **17,** No. 13, 1, 14 (March 1983).
4. D. R. Brodwin, "On personal computing," *Office Administration and Automation* **44,** No. 8, 92–93 (August 1983).
5. A. Goldberg, "Building micro nets—the clustered approach," *Computerworld* **17,** No. 41A, 39–48 (December 1983).
6. A. Emmett, "Thwarting the data thief," *Personal Computing* **8,** No. 1, 98–105, 204–205 (January 1984).
7. "Computer security: what can be done," *Business Week* (*Industrial Edition*), 126–130 (September 26, 1983).
8. B. Gilbert, "Buying computer furniture that really fits," *Personal Computing* **7,** No. 9, 54–63, 194–195 (September 1983).
9. T. E. Bell, "Your insurance can ruin you," *Personal Computing* **7,** No. 8, 115–119 (August 1983).
10. G. Rifkin, "Protecting your data," *Computerworld* **17,** No. 32A, 59–64 (August 1983).
11. "Configure your business to protect information assets," *Personal Computing* **7,** No. 7, 133–134, 136 (July 1983).
12. H. J. Hinkin, "Microcomputer and mainframe ally to bring offices new power," *Electronics* **56,** No. 16, 105–107 (August 1983).
13. B. W. Lampson, "Protection," *Proceedings of the 5th Annual Princeton Conference on Information Sciences and Systems,* pp. 437–443. Reprinted in *ACM Operating Systems Review* **8,** No. 1, 18–24 (January 1974).
14. *Data Encryption Standard,* National Bureau of Standards, FIPS Publication 46 (January 1977).
15. S. M. Matyas, "Digital signatures—an overview," *Computer Networks* **3,** No. 2, 87–94 (April 1979).
16. A. S. Tanenbaum, *Computer Networks,* Prentice-Hall, Inc., Englewood Cliffs, NJ (1981).
17. P. J. Denning, "A scientist's view of government control over scientific publication," *Communications of the ACM* **25,** No. 2, 95–97 (February 1982).
18. D. E. Denning and P. J. Denning, "Data security," *Computer Survey* **11,** No. 3, 227–249 (September 1979).
19. D. W. Davies, *The Security of Data in Networks,* IEEE Computer Society, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08859 (1980).
20. "Integrated information systems: the microcomputer explosion," *Forbes* **129,** No. 9, 73–94 (April 1982).
21. D. E. Bell and L. J. La Padula, "Secure computer system: unified exposition and multics interpretation," Report ESD-TR, 75–306, Mitre Corporation, Bedford, MA (March 1976).
22. D. E. Denning, "A lattice model of secure information flow," *Communications of the ACM* **19,** No. 5, 236–242 (May 1976).
23. J. K. Millen, "Security kernel validation in practice," *Communications of the ACM* **19,** No. 5, 243–250 (May 1976).
24. H. R. Rahden, "Computer security auditing," *WESCON 1979 Conference Record* **14,** No. 3 (1979).
25. R. P. Cambell and G. A. Sands, "A modular approach to computer security risk management," *AFIPS Conference Proceedings* **48**, 293–303 (1979).
26. R. E. Johnston, "Security software packages—a question and answer comparison of the 'big 3,'" *Computer Security Journal* **1,** No. 1, 15–38 (Spring 1981).
27. C. E. Landwehr, "Formal models for computer security," *Computer Survey* **13,** No. 3, 247–278 (September 1981).
28. S. Fordyce, "Computer security: a current assessment," *Computers and Security* **1,** No. 1, 9–16 (January 1982).
29. *Data Security Controls and Procedures*, G320–5649, IBM Corporation; available through IBM branch offices.
30. K. S. Shankar, "The total computer security problem: an overview," *Computer* **10,** No. 6, 50–73 (June 1977).

31. *SQL/Data System: Planning and Administration,* SH24-5014, IBM Corporation; available through IBM branch offices.
32. B. Feezor, "Links made data available," *Computing Canada* **9,** No. 22, Personal Software Report 4 (October 1983).
33. F. X. Dzubeck, "Telecommunications," *Office Administration and Automation* **44,** No. 10, 105 (October 1983).

Reprint Order No. G321-5226.

William H. Murray *IBM Information Systems and Communications Group, 44 South Broadway, White Plains, New York 10601.* Mr. Murray is Program Manager, Data Security for the Information Systems and Communications Group, where he is responsible for advising group management on the security properties of their products. In a previous assignment, Mr. Murray managed the development of the security subsystem for the IBM Advanced Administrative System. After fifteen years, this system is continuing to operate successfully and is considered to be a model of the state of the art. Mr. Murray is the author of Reference 29 in this issue. Other articles of his have appeared in *Asset Protection, EDP Audit Control and Security, IEEE Spectrum, Computers and Security,* and *The Computer Security Journal.* He has spoken on security to SEAS and the Diebold Research Program in Europe and to the Australia–New Zealand Association for the Advancement of Science. Mr. Murray received a B.A. degree in business administration from Louisiana State University, Baton Rouge; he joined IBM in 1956.