Computers, security, and the audit function

by NORMAN R. NIELSEN
Stanford Research Institute
Menlo Park, California

INTRODUCTION

As the role of computation spread in the world of commercial data processing and in the world of organizational administration, concern and attention were directed toward such matters as programming techniques, computer capabilities, and computer performance measurement and evaluation. However, because computers became increasingly essential to the conduct of an organization's daily activities, and because these systems frequently controlled vast amounts of organizational resources, the computer became an object of attack. In some cases the organization was the target; the computer was the means to attack it. In other cases personal gain was the goal; the computer was merely the means for misappropriating corporate assets. Parker1 has chronicled more than two hundred cases of computer-related crimes. Therefore, concern has recently been focused on the security of computer installations and the maintenance of computer system integrity. In 1974 both AFIPS2 and the National Bureau of Standards3 have published guidelines for computer security.

The organizational auditor has long been involved in one fashion or another with the auditing of applications processed in whole or in part by computer systems. Until recently, though, his concern has been with the application itself, not with the computer system. Great faith was maintained in the basic integrity of computer systems. Now, however, the growing incidence of computer-related crimes has shattered that faith. The auditor must also concern himself with the basic security of the organization's computer facilities and with the means by which the integrity of the systems is maintained. Thus, the auditor is rapidly being thrust into an area in which he has traditionally had little expertise or responsibility.

COMPUTER SECURITY

The growing role of computing

Computers are becoming an integrated part of the operations of many organizations. Computer systems schedule daily work flows and product assembly sequences in manufacturing. In the transport industry, reservations, traffic movement control, and crew and equipment scheduling are computer-based. Banks are critically dependent upon overnight computer processing, so that they may open their doors the following morning. Governmental organizations rely upon computers for the disbursement of funds and the maintenance of records concerning their constituent citizens.

The computer has thus become a vital cog in most organizations. The period of time during which an organization could continue to exist in the face of the cessation of computer processing will, of course, vary from organization to organization. However, the time periods are all short in relative terms, and these periods are tending to become shorter every year. Thus, security as related to the continued availability of these computer systems to serve their organizations takes on particular importance.

Computer files as assets

Computerized files of data are in many organizations becoming synonymous with the assets recorded in them. Thus, a bank's files of account balances are just as much "cash" as the depositors' actual funds. A few bits changed in a file can yield as much real money as an armed robbery. The same holds true for payment systems associated with accounts payable, payroll, claims, dividends, pensions, and credit account balances in other organizations.

Even computerized files that do not represent cash assets are frequently valuable organizational assets in need of protection. Mailing lists are a classic example of this type of asset and have already been the target of thefts.

Privacy

Privacy is a distinct concept that must not be confused with security. However, the privacy of data cannot be assured on an insecure system. That is, a secure computer

...
system is a necessary, but definitely not a sufficient, condition for maintaining the privacy of personal information stored in computer files.

Today there is a great deal of interest in the privacy of the individual and of data relating to the individual. Bills concerned with privacy have been introduced in both the House and the Senate during the past legislative session, and numerous bills have been introduced in the various state legislatures. Although very little of this legislation has yet become law, it is clear that additional legislation will be forthcoming in this area. While the immediate impact of new laws is likely to focus on privacy considerations per se, there will necessarily be a derivative impact on computer facility security and system integrity requirements.

EXPANDED AUDIT ROLE

The fact that the security of a computer facility can no longer be taken for granted and the integrity of a computer system can no longer be assumed is leading to a much broader role for auditors in an organization's EDP operations. Considered below are six areas where much greater auditor participation is now required.

Physical security

Because of the critical role played by computing in most organizations, the auditor must take steps to verify that appropriate levels of physical security surround the computer facility. Consideration must be given to fire detection and extinguishing equipment, to pumps and alarms, to air conditioning equipment and air intakes, to power cables and communication lines, to window areas and walls, to construction, to activities and hazards in neighboring buildings and adjacent floors, and to cleanliness of operating areas.

Procedures (and training in the use of those procedures) are just as important as physical facilities. Personnel must know how to respond in an emergency, to protect the safety of employees as well as to protect equipment and data files. Emergency equipment must be tested on a regular basis. Clearly, it is not the auditor's responsibility to develop procedures and to carry out such tests. However, he must determine the adequacy of the equipment and the procedures that have been developed for safeguarding the facility, and he must verify that the procedures are being adhered to properly.

Access control

An organization's computer facility cannot be sealed off from the outside world, for a variety of personnel and materials must regularly move in and out of it. Again, the auditor must be concerned with the adequacy of the procedures for controlling such movements and with the verification that these procedures are being followed faithfully.

The most obvious area of concern is the movement of personnel. This includes not only regular employees, but also maintenance personnel, temporary employees, visitors, deliverymen, and so on. Further, unrestricted movement to all areas within a controlled area is unlikely to be necessary or desirable, requiring the establishment of proper access controls within the basic controlled area.

Controlling the movement of materials in and out of the controlled area may at first glance seem straightforward. However, there are many subtleties. Bombs have been shipped into computer rooms in boxes thought to contain paper for the printers. Waste and spoiled outputs hauled away in the trash have often yielded valuable or sensitive information to scavengers. Tapes or printed reports can easily be concealed in a briefcase or on the person of an individual leaving a facility.

Changes in computing technology in the past few years have added a new dimension to access control. It used to be that data inputs were physically shipped to the computer facility from the user departments or branches. Authenticating the input materials and controlling the distribution of outputs was relatively easily accomplished. Now, however, much of the input and output process is conducted over telecommunication lines. Ensuring the identity of incoming requests is a much more difficult task. This is true even when dedicated rather than dial-up telephone lines are being used. It is not surprising that a variety of research, such as that of Evans, Kantrowitz, and Weiss;* Purdy;* and Friedman and Hoffman' has been conducted in this area.

Operating procedures

A variety of operating procedures have a direct impact on the security and integrity of an organization's computer facility and data files, so the auditor must extend his concern into this area as well.

Separation of duties has long been a key tenet in the manual handling of financial transactions. However, the extension of this concept to cover the automatic handling of transactions within data processing systems has not always been made.

Further, the data processing operation itself requires some additional types of separation that have heretofore been foreign to the auditor. Production run scheduling and control, computer operations, and data library responsibilities must be separated. Even in environments where a single employee is quite capable of performing these duties himself, the combination of responsibilities must be avoided. Many of the cases of computer abuse studied by Parker* resulted from an uncontrolled combination of responsibilities.

The procedures that must be examined by the auditor can become fairly technical in the operations area. For example, the safeguards over the improper or erroneous
Programming

Programming represents the heart of a computer system, and it places two different types of requirements upon the auditor. First, as for the areas mentioned previously, a number of procedures need to be examined with respect to their impact on system security and integrity. These include the development and use of programming standards, the enforcement of documentation standards, the independent testing and examination of new software (systems, applications, modules, or simply patches to existing programs), and the independent operation of that software on the production computer system.

The separation of duties goes beyond the aforementioned split among development, test, and operation. The development of programs is (with today's technology) an inherently "buggy" process. Thus, there needs to be a separation of the production computer system from the development system, of the production files from the test data. Privacy considerations are likely to lead to the aforementioned test group being delegated the responsibility to provide programmers with "sanitized" test data, data that are like "live" data but that do not contain meaningful identification such as actual names or addresses.

The second type of responsibility for the auditor in this area concerns the program design process. Computer programming technology is such that a wide variety of functions can be included in a program at little cost if planned for in the original design. However, it is often prohibitively expensive to include any of the same functions after program development has been undertaken. Thus, it is critical that the auditor play a significant role in the program design process. It is at this point that he must seek to include the proper programmatic control features and to add the necessary audit trails to facilitate his auditing of the system when it becomes operational. The continued integration of functions within the computer system often leads to the loss of customary audit trails, but the technology is such that the auditor cannot afford to wait until he notices that the audit trails have vanished.

Personnel

Many aspects of this area are already familiar to auditors, including employee bonding and employee background investigations. However, surprisingly little is done to make the data processing employee realize that he is in as much a position of trust as is the employee of a bank trust department. A great deal of confidential or sensitive information passes through the computer system, and the employees frequently have access to it. Consideration must also be given to the protection, following an employee's termination of employment, of the program developments and sensitive data previously exposed to him.

Normally, considerations of employee relations and unionization are not particularly the province of the auditor. However, the vast concentration of organizational assets in computer systems and the critical role played by computers in the daily affairs of organizations, coupled with increasing attempts at unionization in the data processing field, do have an impact on the assessment of system security, operability, and integrity.

Recovery

Disaster is an unpleasant subject, which is often the reason why human beings do not plan for it. Yet, disasters can and do happen. Thus, the auditor must be concerned with his organization's ability to recover and resume normal operations. The usual considerations include backup power supplies, spare equipment or excess capacity, off-site data storage, and backup computers (on-site, at other locations, or even in other organizations). However, technology is making the assurance of adequate backup in the event of major disaster an increasingly difficult task. The development of large, centralized computer systems, particularly those with extensive telecommunication links, has resulted in systems that are expensive to replicate and in applications that are difficult to move from one site to another because of communications or other special requirements. This frequently results in a disaster plan that is simply a prayer that disaster will never strike.

THE COMPUTER AS AN AUDIT TOOL

The computer is not solely a villain in adding to the problems confronting the auditor; it also brings tools that can aid him in carrying out his responsibilities. Computer power has greatly enhanced the controls that can be employed in application programs, in monitoring system processing, and in controlling and logging facility access. Computer power has also greatly increased the types of tools available in conducting an audit. The following three types are illustrative.

Audit software

In the past several years many software packages have been developed for use in auditing computerized systems. These packages have primarily been intended to permit the auditor to access computer files independently with a minimum of effort, for the purpose of sampling, totaling,
 Dummy branch

The model division or dummy branch is a very powerful tool for the auditor that provides a conceptually different auditing approach. The auditor can introduce test transactions into the system through the dummy branch without having to back them out, without impacting regular company operations, and without introducing the additional control problems associated with audit personnel making direct changes to company records. The dummy branch also provides a mechanism for testing strings of previous transactions for a particular account, salesman, or branch to see whether the previously obtained results are replicated.

Despite the power of the dummy branch as an audit tool, it is not widely used today, largely owing to time and cost considerations. However, the path of technological development of computing may well remove or reduce this limitation (see Audit Implications below).

Contextual audits

Computer processing, coupled with more extensive computer-based data files, is permitting auditors to make contextual audits across time periods and operating division boundaries rather than having to examine a record or transaction in isolation, out of context. Thus, for example, an adjustment made to a payroll record falling within a particular period, out of context. Thus, for example, an adjustment made to a payroll record falling within certain limitations will be accepted as legitimate, since errors are made and do have to be corrected. However, should that adjustment figure be repeated each pay period, there would be cause for further investigation. Similarly, the on-duty time of transportation operating personnel can be correlated with equipment dispatch records and with the independent records of other types of crew members serving on the same equipment. Thus, the auditor can bring to bear tools of much greater power in the conduct of his audit investigations.

AUDIT IMPACTS OF COMPUTING TECHNOLOGY CHANGES

The items discussed in the previous sections reflect developments that affect the work of the auditor today. However, the situation is not static. Computing technology is continuing to change rapidly, and the changes will have an impact on computing styles, which, in turn, will affect security and audit requirements. Therefore, it is important to consider some of the prospective changes and their derivative impacts.

These prospective changes are examined below in four steps. First, the changes in the technology used in various computer system components are examined. Then the impacts of these changes on the use of these components are explored. Next, the collective impacts of these changes on computer system design (hardware, operating systems, and applications software) are treated. Finally, the derivative implications of these system changes on the audit function are discussed.

Prospective technology changes

Recent advances in solid-state circuitry are rapidly being incorporated into currently manufactured computer systems. It is forecast that development trends in large-scale integrated (LSI) circuitry will continue, leading to memory and processor components that are smaller, faster, and cheaper. The use of LSI circuitry will also aid equipment reliability and maintainability. Not only does the use of LSI permit more fault detection and correction hardware to be included in the equipment design, but its packaging and reduced circuit costs permit circuit failures to be isolated and replaced at the chip level rather than at the circuit level. As a result, memory and processing equipment should not only be more powerful and cost effective but also more reliable in operation and more readily repaired when inoperable.

A variety of trends are forecast in the area of I/O and data transmission equipment. Magnetic storage media will probably retain their dominant role. However, storage density should continue to increase, and storage cost should drop. Access times and transfer rates should continue to improve. Printer technology is likely to advance significantly in the nonimpact area, providing much faster output rates, as well as graphic and image reproduction capability. The development and use of programmable front-end communication processors is expected to continue, so communication processors may soon become an integral part of most standard systems. Digital communication circuits will become much more common, permitting not only reduced costs but also faster, more reliable communications.

Relative progress in the software area is not expected by many to be nearly as striking as that in the hardware area. Operating systems on medium- and large-scale computers are expected to grow larger and more complex as they are called on to provide additional services. In addition, more design emphasis will be placed on system integrity and security considerations. Thus, the processing power required to support the operating system should continue to increase. Program development will continue to constitute a large part of the total cost of computing. Although there are a number of changes on the horizon that should improve programmer effectiveness, these developments are not likely to have as significant an effect upon cost as hardware developments. Hence, programming should be
come relatively more expensive. The use of microprogramming capabilities for support purposes is expected to spread, permitting more effective use to be made of hardware for particular applications, as well as facilitating certain types of program development.

Impact on usage

The increased speed and reduced cost of circuitry should support the trend toward faster and more powerful processors within the main product lines of computer manufacturers. More applications should thus become feasible, either through reduced cost or through reduced processing time. This should assist the spread of on-line processing systems in many commercial areas.

However, these developments in circuit technology will also benefit minicomputer systems. More capable minicomputers will be able to perform many of the functions now thought to require a larger, general purpose computer. Capability coupled with the low cost of such minicomputers should facilitate the distribution of computing functions within an organization (see Impact on System Design below) and should permit greater specialization or dedication of equipment to particular applications.

The miniaturization of circuitry, in combination with low component costs, will probably lead to the incorporation of greater logical capabilities within equipment. This will apply not only to I/O devices and equipment control units but to terminals and user interface equipment as well. Thus, much more editing, formatting, and error correction could be handled at the terminal rather than at the computer. Microprocessors should continue to proliferate as a tool in support of additional equipment capabilities.

Technological developments should also result in faster memories to operate with the faster processors. In addition, forecast cost reductions will permit much larger standard memory sizes. Although larger memories will facilitate program development and will permit more efficient program execution, they will also support a continued need for complex multiprogrammed operating systems, with all the overhead and protective mechanisms associated with serving multiple users “simultaneously.”

The availability of larger volumes of on-line random access storage at lower cost will probably facilitate greater use of on-line systems, as well as greater integration of an organization’s files. Continued system integration implies a further loss of traditional audit trails, unless specific steps are taken to design audit trails and controls into individual applications.

Advances in I/O equipment should enhance many applications. More input should be possible via mechanical scanning without reliance on human keystroking. Image input as well as output should become possible, permitting, for example, an image of the pay-to-the-order-of line from a check to be input and subsequently printed on a customer statement. With the incorporation of increased logic in terminal devices, more input errors should be caught and corrected at the time of input, eliminating more costly error detection and correction in downstream processing.

Networking should be facilitated by the availability of digital communication links, as well as by the greater use of front-end processors. This should enable more accurate communication as well as more appropriate “human interfaces” to be developed for systems. Front-end processors will also facilitate the shifting of loads to other processors (e.g., in the event of equipment failure), permitting more reliable service to be offered with a greater service availability.

Operating systems are expected to offer additional services to programmers and users. This should help to reduce the growing cost of program development, but it is likely to do so at the cost of larger operating systems and increased use of processor cycles. However, the additional functions performed for the user are likely to be considered worth the cost, particularly in view of the expected decrease in computing costs.

Programming costs are expected to remain relatively high, even though many attempts will be made to reduce them. In addition to new operating system support features, further specialized software systems are likely to be developed to facilitate development and production usage in particular application areas. Use of data base management software should become more widespread, aiding organizations in dealing with increasing volumes of readily accessible files. Greater use of structured programming, chief programmer teams, and similar approaches is anticipated and should improve programming quality and cost effectiveness.

An interesting expected trend is the increasing use of hardware to aid software systems. Thus, specialized microprograms or “firmware” should be increasingly used to adapt computation to support certain types of processing. These tools should facilitate regular program development as well as program execution.

Impact on system design

The changes and developments discussed in the previous two sections are likely to support two opposing trends in the overall architecture or structure of computer systems: a trend toward central systems and an opposing trend toward distributed systems. Short of some unexpected developments, it is anticipated that both types of systems will proliferate, the choice depending on the particular circumstances confronting an organization.

Central systems

Economies of scale for both capital equipment and operational support, more powerful systems, and more capable software should facilitate the development of what might be termed central computer systems. Such systems are characterized by an aggregation of one or more large-scale processors or multiprocessors that are linked together at a single location. Most computing takes place
at this central site, and most files are stored there, accessible to all the computers. Users throughout the organization can input data and receive outputs via terminals attached to a telecommunication network. The key distinction between this form of system organization and the distributed form (see below) is that processing capability and data files are stored at a single location in a star network rather than being distributed geographically and hierarchically throughout the network. It is interesting to note, however, that telecommunications can play a major role in either form of network.

The central type of system organization will favor an integrated file system. Given the cost and performance data mentioned above, the availability of all files to all the processors in one location should push an organization toward broader and more integrated file usage. In a similar manner, application processing steps should show increasing integration, making for more effective processing.

Centralized processing can have an advantage over distributed computing in that there need be no coordination of processing between hierarchical levels, no transfer of files between locations, and so forth. The central system is also better able to play a load-leveling role, since more averaging can take place on a large system than on a number of smaller systems. On the other hand, a central system of equivalent capacity is likely to run more heavily loaded, since a greater portion of its power must be used in support of the operating system.

Other impacts include the greater variety and sophistication of services that can be made available to users of such a system and the ability of a facility to attract more capable staff members. Currently, large powerful computer systems are viewed by computing professionals as being the more attractive systems on which to work. Historically, more new developments and more exciting activities have been associated with these systems. To the extent that this continues, the use of such "advanced" computing systems should be a positive factor in recruitment.

Distributed systems

The decreasing cost of hardware, coupled with enhanced capability, should facilitate the development of what might be termed distributed computer systems. Such systems are characterized by a distribution of computational capability, both geographically and hierarchically. That is, certain types of processing may be done on small local computers, while other types of processing (or portions of processing steps) may be forwarded to more capable processing equipment at a higher level.

Distributed systems can follow a variety of patterns. Hierarchies may be defined by the relative computational power at each level or by the files or file contents available at each level. Individual processors may handle a variety of jobs or be dedicated to particular applications.

An additional impetus toward distributed computing may come from privacy and security considerations. Present-day operating systems are notoriously vulnerable to penetration. This poses a particular problem in connection with the central systems, for "all" users and "all" files are on the same system, with only the operating system preventing unauthorized access to files. The distributed design has the advantage of a simpler (and potentially more secure) operating system and of some physical barriers to file access. This may prove to be a powerful selling point in a world that is becoming more and more concerned about computer security and data file privacy.

A distributed system can have several impacts. The greater specialization of the use of each computer can reduce the complexity required in the operating system. Thus, less memory and storage space need be devoted to the operating system; fewer computer cycles will be needed to run it; less effort will be needed to develop it; and more security "holes" can be avoided.

The greater modularity that can be built into a distributed system can permit greater system flexibility. Growth can be accommodated by adding processors or by replacing processors incrementally. Failures have less of an impact on total performance, since a larger fraction of the total system remains operable. When many smaller processors are employed, it may be economically possible to switch in a replacement or standby processor to take over the function of the disabled one.

Distribution may or may not entail greater use of communication equipment, depending on the application. Processing performed locally reduces the need for communication to a central system. However, the passing of information and file data between hierarchical levels can entail greater communication requirements for certain designs.

Although moving data around a distributed network requires more emphasis on network security and control, such a network can lead to enhanced security. Efficient message switching and data flow requirements lead to greater standardization of requests, controls, and procedures for within-system communication. This structure, coupled with simpler system logic, can provide a positive increment to system security.

Audit implications

The prospect of the above developments has a number of implications for the auditor. These implications are discussed in three areas: those that relate to all systems, those that relate to central systems, and those that relate to distributed systems.

General

The continued decrease in the cost of computing should be beneficial to the auditor. Running tests or programs...
should become cheaper; running times should be reduced by the greater power of computing equipment. Larger samples should be possible without impacting ongoing operations more severely. Further, it may become possible to use tools never used previously in an organization because of their cost. The use of a dummy branch is a case in point.

The expected loss of audit trails will require greater involvement by auditors in the program development process. Without audit intervention, audit trails are likely to continue to be absorbed into more integrated processing steps, leaving fewer intermediate outputs. Further, with the probable continued high cost of software development and modification, it is imperative that appropriate audit trails be built into new software at the design stage rather than having to be retrofitted after development.

It is likely that many more security features, as well as monitoring tools and facilities, will be contained in computer operating systems. These have great potential for the auditor, but it will be necessary for him to learn how to use these facilities effectively and to incorporate their use into own auditing procedures.

Central system

The integration of data files should lead to greater use of data base management and report generation systems. Although these should ease data base access problems, their use will make more files readily accessible by more individuals. Use of these systems will also permit data from several files to be combined with much less effort, an action that could lead to more serious invasions of privacy.

The complex operating systems of large central systems will probably continue to have security weaknesses that can be exploited by possible penetrators. Thus, it will be more difficult for auditors to ensure the integrity of computer systems. Further, the greater number of programs and files on such a system should make the facility a more inviting target.

The proliferation of terminals at scattered locations, each having direct access to a system with so much information available, poses another problem. Greater attention will have to be paid to the physical access control for these terminals, as well as to the logical control over what can be accomplished by them.

Backing-up such a central system can pose problems because of the telecommunication interfaces at a single site and the large size of a "unit" of computing. Thus, the availability of a computer at another location will not suffice for backup purposes without a great deal of advance planning and (probable) contingency hardware expense.

Although processing capabilities and peripheral equipment capabilities are likely to reduce the audit trails available as a processing byproduct, the effect will be somewhat more pronounced in the central system. With less coordination between levels or nodes, there will be less need and opportunity for intermediate logs to be created.

Distributed systems

The frequently simpler logic of the distributed systems should make audits easier and provide greater assurance that processing is proper and that file integrity is being maintained. The organization of a distributed system provides both greater opportunity for audit monitoring and additional audit tools. In particular, the expected reduced cost of minicomputers, in conjunction with enhanced capabilities, should bring the development of an audit computer into the realm of feasibility. Such a computer could be integrated with the distributed system; yet it could enhance the desired isolation of audit programs and functions.

The possibility of more file movement and system-initiated transfers of programs and data within a distributed system should increase the importance of network design and management. Network protection will become more critical. Although all programming might be handled centrally and distributed to remote processors, a single individual with physical access to a processor at a remote location could load substitute programs and do considerable damage to the network.

Control can be a problem in distributed systems, since remote locations cannot always be staffed and operated at the same level or to the same standard as a central facility, owing to the smaller scale of the operation. Thus, more care may have to be exercised in this area, and increased audit attention may be required.

SUMMARY

The growing role of computing in many organizations, the evolution of computer files into significant assets, and the derivative impact of privacy considerations are leading to a much greater concern for computer security and computer system integrity assurance. These developments are impacting the auditor, adding to his computing-related responsibilities in the areas of physical security, access control, operating procedures, programming, personnel, and recovery. However, computer techniques have also provided additional control and audit tools to assist the auditor.

Computing technology is not static, and future changes in computing technology will affect the manner of computer use and hence the computer security facilities and requirements of the future. These changes will, in turn, impact the auditor, placing new demands (as well as providing new opportunities) for him to ensure the security and integrity of his organization's computing systems, data, and operations.

REFERENCES


