EXECUTIVE GUIDE TO COMPUTER SECURITY

ACCIDENTAL ☐ ☑ ☐

INTENTIONAL ☑ ☐ ☑

DISCLOSURE

DESTRUCTION

MODIFICATION

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
and
Association for Computing Machinery

FOREWORD

This booklet has been prepared for an audience of executives and managers, other than computer and ADP managers, in organizations using computers to help them understand the necessity for computer security and the problems encountered in providing for it.

There are still many gaps in our knowledge. Much more work needs to be done before an organization will be able to implement security provisions which are specific and justifiable responses to defined threats. There are, however, measures which may be taken and this booklet provides a general discussion of those solutions which are available today.

A question and answer format was selected to organize the material in a manner which might logically represent a general approach to analyzing computer security problems. The material in this booklet was drawn from the report of a workshop of top technical experts in the field of computer security, held in December 1972.

The Institute for Computer Sciences and Technology at the National Bureau of Standards, U.S. Department of Commerce and the Association for Computing Machinery. the nation's largest technical society for computer professionals. have been jointly sponsoring* a series of workshops and action conferences on national issues. These workshops were designed to bring together the best talents in the country in the respective areas to establish a consensus on 1) current state of the art. 2) additional action required, and 3) where the responsibility for such action lies. The workshop on computer security was the first in the series and did, indeed, establish a precedent of satisfying those goals.

BASIC TERMS

Privacy is a concept which applies to an individual. It is the right of an individual to decide what information about himself he wishes to share with others and also what information he is willing to accept from others. The privacy issue has not resulted from the development of computers, but the heightened interest in it can be laid to the capability of computers for storing vast amounts of readily usable data.

Confidentiality is a concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection which will be provided.

Data integrity exists when data does not differ from its source documents and has not been accidentally or maliciously altered, disclosed or destroyed.

Data security is the protection of data against accidental or intentional destruction, disclosure or modification, using both physical security measures and controlled accessibility.

Controlled accessibility is the set of technological measures of hardware and software available in a computer system for the protection of data.

Physical security is protection against physical destruction and theft of assets, including data.

* The National Science Foundation provided financial assistance in planning the series.

WHY SECURITY?

1. WHAT IS COMPUTER SECURITY?

Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs and data to assure that organizational assets and individual privacy are protected.

2. WHY SHOULD I CARE ABOUT COMPUTER SECURITY?

Computer data and programs represent an increasingly important part of the assets of every organization in our economy. Every day both business and government become more dependent on computer systems to carry out normal business operations. There are over 130,000 computers installed in the U.S. today representing a current value of $29.2 billion. There is no way to place a value on the millions of data files and programs used on these machines, or on the value of the services performed by these same machines. Their worth in this sense is clearly inestimable. These assets must be safeguarded.

Consumer and public interest groups as well as individuals are now beginning to demand that their concern for protection of individual privacy be taken into account in the design and operation of modern information systems. The President in his 1974 State of the Union address called for attention to this critical national problem at the highest levels of government. His concerns included modern information systems, data banks, credit records, and electronic snooping as well as ostensibly collecting personal data for one purpose and then using it for another. In fact a number of bills are currently being proposed in the states as well as the Federal legislatures to insure rights of privacy and establish requirements of data protection. Every data processing activity will be impacted by the provisions of the legislation.

Every organization will need to adopt procedures and provide safeguards to protect these valuable assets and meet the requirements of legislation.

3. WHAT MUST I PROTECT THESE ASSETS AND INFORMATION AGAINST?

Threats to computer system security arise from the unpredictability of environmental conditions and people. Data processing facilities and assets must be protected against natural catastrophe and hostile activity so that the impact on the operations of the organization are minimized. These threats include destruction by environmental forces as well as theft or destruction by individuals. Nature only destroys; man both destroys and acquires. Exposure to these threats creates risk for your organization.

4. ARE THE THREATS WHICH CAN BE PERPETRATED BY PEOPLE ON MY COMPUTER SYSTEM REALLY SERIOUS?

Such threats are very *real* and *serious*. Companies have been nearly put out of business by unauthorized manipulation of their data files.

The most common situation is the manipulation of computer system resources for personal gain. Direct physical assaults on computer facilities for purposes of destruction are relatively rare. Nevertheless persons motivated by revenge or antipathy toward modern technology have made direct physical assaults resulting in serious damage.

In a study of computer-related crimes, the significant fact appeared that many people who consider themselves honest citizens who would not steal from other people have no compunction about stealing from a computer because it is a faceless nonentity. The same study revealed that the financial gain from computer crime has little appeal for some people, but they will commit a crime for the thrill of "beating the computer".

In reading the following examples, it will be obvious that the individuals involved were apprehended, but it must be assumed that much computer-related crime is not detected and is, in fact, still going on.

a. Internal threat, job related: Because of his familiarity with a bank's programs and procedures, a teller in a New York bank was able to transfer $1.5 million to his own account without leaving any trace of his activity, completely foiling both automated and manual auditing systems. Authorities became suspicious only when his name was associated with a large betting operation.
b. Internal threat, not job related: An EDP manager and part of his staff used their company computer to "handicap" horse races and pocketed the profits.
c. External threat, computer manipulation: An engineering student discovered a way to gain access to the computerized supply system of a telephone company. He claims to have obtained and sold nearly $1 million in equipment before getting caught.
d. External threat, forms manipulation: A man substituted deposit slips, magnetically coded with his account number, for the blank ones available on a bank's customer counter, causing the computer to place other customers' deposits in his account. He then withdrew the money and disappeared.

SITUATION TODAY (The Real World)

5. ARE THE MAIN PERSONNEL THREATS TO A COMPUTER SYSTEM WITHIN OR OUTSIDE AN ORGANIZATION?

Without question, the "trusted insider" is the greater threat to any computer system. An employee (programmer, janitor, or even manager) with knowledge of the system and its defenses is the most likely to subvert a system. The inept ones are caught immediately; the competent ones may go undetected indefinitely. As organizations place more and more valuable data into large data banks, the potential payoff for an inside job will get bigger and bigger.

6. CAN DATA IN A COMPUTER SYSTEM BE COMPLETELY PROTECTED?

No. For every defense there is an alternative offense, but a level of security can be provided that is commensurate with the risk. The desired protec-

tion level is that which makes the cost of subverting the system greater than the benefit to be gained by its subversion.

7. CAN STORED DATA BE SECURE FROM DESTRUCTION OR COMPROMISE?

Security of stored data depends on the storage media and the threats to which they are vulnerable. There are two types of threats:

—individuals who have physical access to the storage media.

—individuals who have computer access to the storage media.

In the first case, experiments have demonstrated that magnets can destroy data stored on magnetic media, but must be placed in almost direct contact with the medium, e.g. magnetic tape, to cause damage. Physical access to the storage area must therefore be carefully controlled.

In the second case, a user of a computer system can erase data on storage media (either accidentally or maliciously), using the computer. The attack which is most difficult to detect comes from someone who deliberately and surreptitiously modifies stored data for his own benefit.

8. CAN COMMERCIAL COMPUTER SERVICES BE EXPECTED TO PROTECT DATA?

To a limited degree and for a price. Computer services usually operate insofar as possible according to guidelines and instructions provided by their customers; special care such as the use of a dedicated computer may be provided for users if requested and paid for. Eventually, the requirement for computer security may create specialized computer facilities which are certified to be secure for specified purposes.

9. IS A DEDICATED SYSTEM SECURE?

A system dedicated to a specific task is more secure than one in which the tasks are still being developed or are rapidly changing. Reservation systems in which the terminal operation has only limited data entry/retrieval capabilities are difficult to probe.

The security of such systems depends on careful control of the actions the user may perform; however, the integrity of data in these systems still depends on the integrity of the source.

10. WHY DON'T COMPUTER MANUFACTURERS "BUILD-IN" PROTECTIVE DEVICES AND OFFER TOTAL SECURITY PACKAGES?

Until recently there has not been a general requirement to develop protected computer systems. Hardware and software solutions have not been found for all security problems. However, some protective devices, such as automatic equipment for personal identification, will become available, or perhaps even "standard", just as automatic transmissions did in the auto industry. Toward this end, large groups of users with similar security needs, such as the Federal Government, can lead the way by establishing uniform specifications of security for computer systems.

11. DO SPECIFICATIONS EXIST FOR A SECURE COMPUTER FACILITY?

No specifications exist for a general computer system to achieve a given level of security. Dedicated systems have been implemented to specifications based on restricted security requirements using restrictive solutions. General security solutions may be found for some common problems, but each facility must define its own detailed specifications.

12. ONCE I HAVE DETERMINED REQUIREMENTS FOR MY FACILITY, HOW CAN I ASSURE THAT THEY ARE SATISFIED?

Through compliancy testing. Security features are usually evaluated for completeness, effectiveness, and correctness. Then they are subjected to simulated attempts to breach security. For example, if a security feature of a system is the authentication of remote terminal users through randomly generated passwords which are periodically replaced, then a compliancy test would be a check to see if any of a specified number of randomly generated fake passwords would be accepted. Good design specifications include the range of compliance which will constitute an acceptable test.

13. CAN COMPUTER SECURITY AND THREATS TO THAT SECURITY BE MEASURED?

Computer security can be measured in terms of the probability that a facility's defenses will be breached by specific threats. For example, the operating system of a secure computer must be designed so that the probability of a penetrator obtaining executive control of the computer system—and thus access to all programs and data—is extremely low. No theoretical methods exist for assigning numerical probabilities to such a situation occurring in the various types of computer systems. Only when a large body of statistics has been accumulated for specific threats can honest numbers be assigned as probabilities. Until then measurement of computer security and the threats to it will be based primarily on intuition and limited experience.

VULNERABILITIES

14. WHAT IS THE MOST VULNERABLE POINT IN ANY COMPUTER SYSTEM?

Relatively speaking, remote terminals are the least secure points of computer system. A system is more vulnerable if it may be accessed from remote terminals both because of the possibility of "bugging" and because remote terminals typically have little supervision. A remote terminal provides a convenient spot from which a would-be penerator could launch a software attack. This is an attack on a system in which the penetrator gains entry either by simulating another's identity or by using anomolies of the system to probe the hardware and software defenses in order to access unauthorized data or to obtain control of the executive programs. Such an attempt could be disguised as a parametric study of efficiency or other "system" study involving a wide range of hardware and software. Once he finds the key to executive control, the penetrator can compromise any data he wishes and can also erase evidence of his attack and leave a way open for future access.

15. CAN A SHARED SYSTEM BE SECURE?

Shared systems are currently not secure because of their complexity and lack of cohesive security design. Computers can be shared in several ways with varying degrees of security. In order of increasing risk, some examples of computer system sharing are:

—Batch-processing systems which sequentially process users' programs while sharing the central processor between a single user and the input/output system. A user of this system has little control in obtaining others' data while it is being processed but may obtain it while it is being prepared for processing, either accidentially or intentionally, through his program.

—Multi-programming systems processing several *local* users' programs simultaneously. A user can accidentially access another users' data, but the central processor will not be under his direct control, eliminating most opportunities for deliberate compromise of data.

—Multi-programming systems allowing programs and data to be entered remotely. Such systems are vulnerable to the same threats as a local multi-programming system as well as to threats associated with remote terminals.

—Interactive time-sharing systems processing several users' programs simultaneously. Each user has interactive control over his program and can therefore actively search for other users' data. Some time-sharing systems also allow remote access and consequently are subject to threats through remote terminals.

16. CAN COMMUNICATION LINES BETWEEN COMPUTERS OR BETWEEN COMPUTERS AND PERIPHERAL EQUIPMENT BE BUGGED?

Assuming that "bugging" means the surreptitious attachment of "listening" devices to computer equipment, the answer is, "Yes". The communication lines linking a computer facility with peripheral equipment in other buildings, with remote terminals, and with other computers in a network are highly vulnerable to electronic eavesdropping.

17. IS BUGGING THE ONLY FORM OF ELECTRONIC EAVESDROPPING?

No. Electromagnetic and acoustic emanations from a computer facility can be detected and interpreted

by a listening post outside but in the vicinity of the computer center. However, detecting these emanations is not "bugging" since a listening device need not be attached to equipment or planted within the computer facility. Communication lines, unshielded electromechanical equipment, and CRT terminals can act as signal sources. All such emanations must be suppressed to achieve a highly secure environment.

18. IT SEEMS THAT AT PRESENT NO COMPUTER SYSTEM IS SECURE. IF THAT IS TRUE, WHAT CAN I DO?

Although a system which has been designed without security as a prime objective cannot be totally secure, much can be done to improve its security. Systems designed for security are under study now. In the interim, the actions available for improving security fall into two main classes: technical and management solutions.

TECHNICAL SOLUTIONS

19. WHAT ARE THE TECHNICAL SOLUTIONS?

They fall into three categories of solutions: computer-based protection techniques, identification techniques, and security audit techniques. All three must be integrated into a secure system according to its security requirements.

20. WHAT ARE COMPUTER-BASED PROTECTION TECHNIQUES?

They are methods based either on hardware or software, but are in either case an integral part of the computer system design, which perform functions such as keeping the data files of different users segregated in a shared system. Some of these techniques are available now such as memory read/write inhibit and segmentation of primary and secondary storage. New programming techniques also permit a compartmentalized approach to data handling.

In systems of the future designed with security as a primary consideration, access to processing resources and data files will be centrally controlled and restricted to a minimum. Design will be based on modular structure in which every module will be like a watertight compartment in a ship; access to one module will not automatically permit access to any others. The barriers between users will be well defined to limit accidental damage and inhibit browsing through another user's files or programs. In addition, technical design criteria for secure systems will include requirements for access controls to be active at all times with no possibility for manual bypassing and for security features to be specified in terms of complete design, correct implementation and proper installation and operation. Data in communication links will be protected, e.g. encrypted.

21. BUT WHAT CAN BE DONE NOW?

In addition to the memory segregation and programming techniques mentioned above, data can be encrypted during both transmission and storage. Encryption, also known as scrambling, is the most inexpensive way of protecting data travelling over long distances from electronic eavesdropping. It is also effective for data in storage or in memory in a shared system. However, it is a method of protection especially subject to internal subversion; its success depends on the security of periodically changed keys. The keys are only as secure as those who have knowledge of them.

22. HOW CAN DATA INTEGRITY BE DETERMINED AND MAINTAINED?

Data integrity may be verified by checking the data or its representation against something known to be accurate. At one extreme, this means checking it word for word against its source. If the source is on tape or in some other machine readable form, the checking can be done by computer, but it is still expensive and time-consuming.

Problems may also be discovered by analyzing systematic errors, trends, and error frequency, but more popular is the use of error-detecting bits, which produce error "flags" when the sums of the data being used do not check with the equivalent sums in the original data. "Bounds controls" are useful because they can sound a warning when data items

are not within certain limits, e.g. an inordinately large check is being issued by a payroll program. Data integrity can also be maintained through redundancy, either by having duplicate copies of the data or by processing the same job on different machines.

23. WHAT ARE THE IDENTIFICATION TECHNIQUES?

Identification is simply the recognition of an individual, a program or a set of data from a name or identification code. Authentication is the verification of identity—a double check, so to speak. Authentication may require that the user supply his unique password or enter his unique key-card. Authentication may even involve physical verification of the claimed identity.

24. HOW DOES A COMPUTER SYSTEM AUTOMATICALLY AND RELIABLY VERIFY LEGITIMATE USERS?

A computer system can verify a legitimate user in three ways:

a. From his knowledge of a password, phrase, number, or other privileged information. Passwords are widely used today. They are, however, rather easily obtained by unauthorized persons either from those knowing them or from their notes and printouts, or even directly from the computer memory.

b. From his possession of a unique physical key, such as a card containing unique information. Such physical items, however, are easily lost, stolen, or counterfeited.

c. From automatically measured biometric data, such as hand geometry, fingerprints, voiceprints, etc. These biometric methods promise high reliability and accuracy, but most techniques are still in the research stage.

25. WHAT IS MEANT BY SECURITY "AUDIT"?

Computer system auditing involves an independent and objective analysis of the security of a computer system. A security audit determines the adequacy and effectiveness of system controls vis-a-vis their threats. It includes both scheduled evaluations and after-the-fact investigations of attempted penetrations of the computer system. An automated, real-time audit mechanism can often provide a timely alert of penetration attempts. Whether after-the-fact or real-time, the auditing procedures should provide

sufficient information for damage assessment and for purposes of prosecution.

26. WHAT IS AN "AUDIT TRAIL"?

An audit trail is a record of what processing is being done to specific data and programs in the system and by whom. To be useful this record should be organized (preferably automatically) into reports of the following types:

—Alerts of possible security violations.
—Review of system activity.
—System security status summaries.
—Damage assessment reports.

27. WHO SHOULD DO THE AUDITING?

Both internal and external auditors should be employed. Both should audit some of the same systems so that results can be compared directly. It is important that internal auditors occupy a neutral position as high in management as possible, i.e. they should not have any responsibility for ADP operations.

MANAGEMENT SOLUTIONS

28. WHAT ARE SOME MANAGEMENT SOLUTIONS?

Planning, funding and implementing security solutions are fundamental management actions. In particular, the areas to be considered include physical security planning, personnel selection and education, system selection and procurement of computer system security options, security certification and provisions for computer operations security. Controls used to achieve computer security must be uniformly enforced because of the value of the commodities and assets being protected; this is the reason for total management involvement.

29. WHAT ARE SPECIFIC MANAGEMENT STEPS THAT CAN BE APPLIED TO IMPROVE COMPUTER SECURITY PLANNING?

First, appoint an independent manager of computer system security, i.e. other than the ADP operations managers, with direct authority in security matters. Then organize a computer security program

and conduct a risk analysis. The security program should make provisions for:

—Specifying precisely who can read, use, or modify data. Ensure that technical as well as administrative controls are used to implement these instructions.
—Conducting independent internal and external audits.
—Keeping accurate and up-to-date organization charts, delineations of responsibilities, and work statement.
—Maintaining and promulgating thorough and detailed plans for normal operations, emergency operations, and recovery operations.
—Motivating employees to report insecure practices or suspicious activities, as well as to maintain their own security awareness.

30. WHAT KINDS OF PHYSICAL PROTECTION SHOULD BE CONSIDERED FOR A COMPUTER FACILITY?

The first line of defense consists of good engineering management:

—Locate in areas not exposed to floods, wind, high tides, fire, etc.
—Construct a facility which can be easily guarded.
—Ensure that electromagnetic emanations are minimized.
—Install emergency power sources, water pumps, air-conditioning, etc.
—Provide adequate emergency maintenance facilities.
—Operate the facility to ensure personnel safety.
—Provide backup for data and for data processing.

31. WHAT PERSONNEL SELECTION PROCEDURES ARE NECESSARY BEYOND NORMAL HIRING PRACTICES?

Perhaps none if present practices include a comparison of the candidates' previous salary with his present standard of living and personal wealth (or debts) and careful verification of previous employment records, character references and reasons for leaving.

32. WHAT EDUCATIONAL PROGRAMS ARE NEEDED IN SECURITY?

Security education and training should not be a one-time thing. Refresher courses and periodic security reviews should be required for all personnel. In addition to the basic indoctrination, the following should be considered:

—Handbooks with security rules and penalties for their violation fully and clearly specified.

—Educational and motivational posters.
—Dissemination of some (but obviously not all) of the security measures in force at your facility.
—Publicity for selected cases of computer abuse at other installations when the penalties imposed were severe. Details of perpetration should be omitted, however.

33. WHAT IS SECURITY "CERTIFICATION"?

Certification is a managerial declaration that the security features of a computer system comply with the specifications which, in turn, satisfy the security requirements. The details of technical analysis leading to security certification are not well specified at this time and there is no certifying agency, as such. However, some prerequisite actions necessary to this process are:

—Modeling of the system and the analysis of the model.
—Formalization of the access controls.
—Prediction of system security degradation and its effect.

Certification should take place at discrete points during the design, implementation, and operation of a system, viz.

—To check that the design is complete.
—To confirm that the implementation is correct.
—To determine that the installation meets all design standards and requirements.
—To establish that a system is secure after system modification, failure or penetration (either detected or suspected).

34. WHAT STEPS SHOULD BE TAKEN AFTER A PENETRATION IS DETECTED?

The status of the system's security must be analyzed to determine which portions have been affected and what has been lost. The unaffected portions may then be restarted, but it is crucial not to overlook any program modifications the penetrator may have left behind which permit easy re-entry at a later time. An important factor in computer system recovery is the existence of a reference point. A reference point is a backup set of key programs and data bases—certified to be correct and unmodified—stored at another secure location. With such a reference point and using operations logs and files, the step-by-step recovery and recertification of other programs and data bases can begin. Care should be taken that the access point through which penetration occurred is fully covered in the restored system.

35. WHAT ARE THE COSTS OF PROVIDING COMPUTER SECURITY?

The costs of providing computer security may be broken into three areas: initial cost, operational cost, and overhead cost. The importance of information processing in the business and governmental communities makes the assumption of these costs mandatory at a level commensurate with the risks to the system. At a minimum, this risk is equivalent to the value of the computer equipment.

Initial costs include:

—Physical security equipment controlling personnel access to the ADP facilities.
—Physical security equipment protecting data in storage.
—Additional equipment for identification, data encryption, program isolation, and security auditing.
—Operating system modifications and additional software needed to utilize this equipment.

Operational costs include:

—Salaries of security personnel.
—Maintenance of security equipment.
—Creating and updating user authorization lists, data file descriptions, data encryption keys, and data access records.
—Security training for operations personnel.
—Certifying and auditing system security.

Overhead costs include:

—Impact on computer system efficiency and flexibility.
—Impact on personnel attitudes.

36. WHAT BENEFITS MAY BE DERIVED FROM COMPUTER SECURITY?

The costs incurred in providing computer security must be placed in perspective to the benefits gained by providing it. These benefits include:

—Protection of individual privacy by compliance with security requirements of Federal and state legislation, management policy, and user confidentiality agreements.
—Protection of the physical assets of the computer facility.
—Protection of the financial investment in programs and data.
—Protection of the assets represented by data.
—Better system and data integrity.
—Better reliability and timeliness of data processing.
—Better accounting of data and resource usage.
—Better employee awareness of their importance to the organization.

SUMMARY

37. WHAT PRIORITY SHOULD BE ACCORDED THE VARIOUS MEASURES SUGGESTED FOR IMPROVING COMPUTER SECURITY?

The first step in computer security is simply controlling personnel access to the computer facility. Creating and maintaining a "security environment" will let both employees and outsiders know that safeguards exist.

Next come some administrative measures:

—List hardware and software resources (including data bases) in order of value.
—Perform a risk analysis.
—Formulate the goals of the security program.
—Determine the investment required to counter the estimated threats.
—Create a security organization, assigning it full responsibility for security.
—Plan a security program and implement it.

The order of priority for the next steps depends upon the cost/benefit studies. A common pattern might be:

—Upgrade the initial physical security measures.
—Establish personal identification systems and other controlled-accessibility procedures.
—Control the flow of data throughout the processes of collection, entry, storage, processing and dissemination.
—Make individual users personally accountable for control of, and access to, data.
—Implement software security to the degree indicated by the cost—benefit analysis.
—Shield the facility against electromagnetic leakage.


DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS


acm