Chapter 11

Computer Security

Expensive equipment and sensitive information is usually concentrated in a military computer complex. The importance of the Army computer complex has increased correspondingly with the use of automatic data processing (ADP) in a variety of military activities. Protective security measures should be established for the equipment, information, operational programs maintained in the complex, and for the facility that houses the processing, main storage units, and remote components.

Computer complexes are susceptible to the security hazards discussed in appendixes B and C. Additionally, magnetism poses a possible threat to the computer complex. A magnet, depending upon its size and location, can scramble recorded data. Also, strong radar signals can interfere with the operation of data processing equipment.

An integrated staff effort is recommended for formulating and executing a security program for a military computer complex. The user is responsible for classification of informational elements contained in the input, data base, and output. At the local data processing installation (DPI) level, the systems security officer has staff responsibility for security of the facility in which the machines are located, to include remote terminals. Local military intelligence has staff responsibility for security of the data contained within the machines.

The physical security expertise available in the provost marshal's office should be used to the maximum extent, and should be complemented by the technical knowledge in other staff areas, such as management information systems, communications and electronics, security office (G2/S2), facilities engineer, fire and safety. Computer expertise, not organic to the installation, may also be considered as a source for additional information and advice.

11-1 Physical Protection

Primary considerations should be the building design and the corresponding applicability of protective measures.

a. Building Design. This includes both existing structures and those being planned and under construction. Selection of protective measures may be influenced by the construction materials used to meet building specifications. Existing physical security measures should be reevaluated as part of the planning process for future modification, expansion, or renovation. Considerations in the selection of a location for the computer complex should include whether it will be:

(1) Housed in one or multiple buildings.

(2) Positioned on one or more floors of the buildings.

(3) Other activities located around it.

(4) Exposed to hazards described in appendixes B and C.

> **Note:** Ideally, a DPI should be located in a separate building. This increases the feasibility of applying appropriate physical protection. Alternatively, it should be located on the second floor of a multi-story structure. This reduces unnecessary pedestrian traffic around the DPI and thus reduces the possibility of unauthorized persons gaining access to or observation of DPI operations.

b. Protective Measures. Computer complexes may require differing degrees and types of protection depending on the physical characteristics of each location, surrounding environment, and vulnerability to security hazards (see figure 75).

(1) Physical security measures may include:

(a) Protective barriers consisting of fences, gates, and doors (chapter 5).
(b) Locking systems (chapter 8).
(c) Protective lighting (chapter 6).
(d) Security force personnel (chapter 9). In some cases well trained receptionists can perform the same duties as security personnel during normal working hours.
(e) Personnel movement control (chapter 4).
(f) Intrusion detection systems (chapter 7).

(2) Electric power. Without electrical power a computer complex cannot operate.

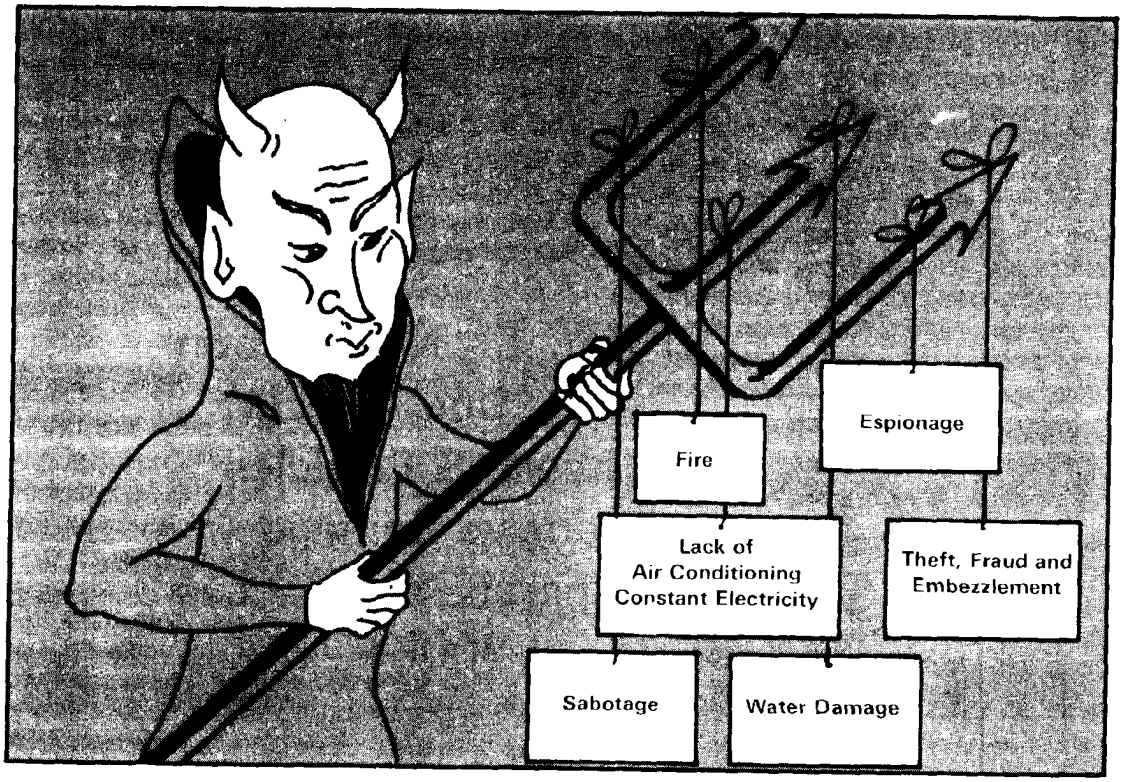

Figure 75—Computer hazards.

All power sources to the computer complex must be continually protected. Three specific problems dealing with electrical power are:

(a) Transients are temporary oscillations that occur in a circuit due to a sudden change in voltage or load. This sudden change can cause errors in passage of data within the computer.

(b) A brownout is a short period of curtailment in electrical power; however, it lasts longer than a transient.

(c) A blackout is the same as a brownout but for an extended period.

(3) Emergency power. This energy source should be available to insure continuous operation of the computer complex. There are at least two types of emergency power available—dual feeds and genera tor.

(a) Certain military installations may maintain their own power source and also use commercial power. Dual feed would incorporate both on post and commercial power sources into the computer complex. There should be emergency cutoff switches for all electrical utilities at every exit from the DPI. Such switches will break every electrical circuit when thrown and will minimize damage from electrical fires.

(b) There are many different generators that can provide an alternate power source to the computer complex. Costs of alternate power sources are high but may be necessary to insure continuous operation of the computer complex.

(c) Loss of power may be caused by natural or manmade reasons. Physical security planning should include measures to prevent or minimize the effects of power losses.

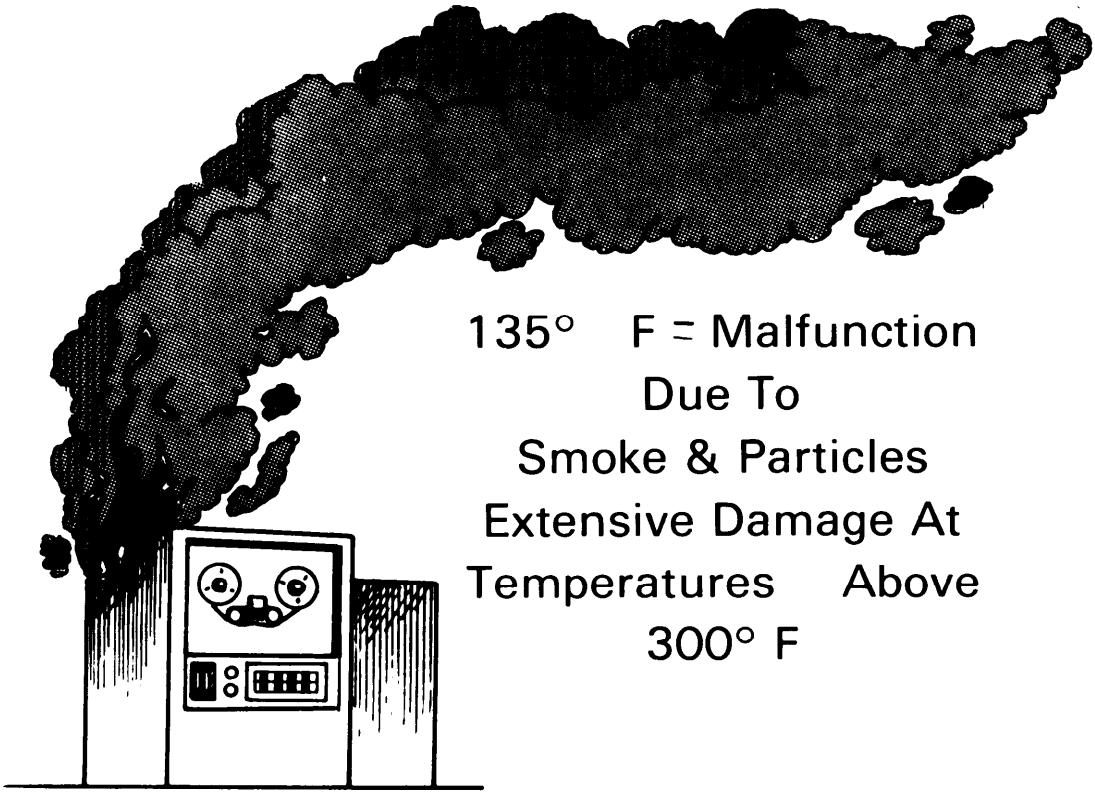

Figure 76—Fire dangers for computer equipment.

(4) Fire prevention. To insure against destruction of the computer complex by fire, comprehensive fire prevention measures should be undertaken (figure 76). Considerations should include the type of construction of the building that houses the computer complex, location and general cleanliness of the area, and the degree of housekeeping within the computer center (ARs 18-1 and 18-2).

(a) Alarms and detectors. The locations, sizes, and functions of alarms and detectors are important in considering fire prevention.

(b) Fire extinguishers. There are a variety of fire extinguishing agents available for use in a computer complex. These extinguishers must be chosen carefully to insure they do the least damage to computers and still extinguish a fire.

(c) Firefighting teams. Any fire control plan must insure that qualified, trained, and efficient personnel can properly use existing fire control devices. They should be-trained to fight a fire in the computer room with minimal damage to computer equipment.

(d) Protective covering. The use of equipment protective coverings can reduce fire and water damage in case of a fire.

(e) Emergency utility procedures. Water and electrical utility cutoff procedures should be specified in case of fire or other disaster.

(5) Air conditioning is required for most computer complexes. A computer complex should have its own air conditioning system. It should not be dependent upon the system that is used for the entire building. The fresh air intakes should be so located as to prevent smoke, dirt, or dust from entering the computer complex. They should contain filters. Periodically the intakes should be inspected to insure

proper operation. Air conditioning systems for a computer complex should have performance monitors. The placement of these monitors is important. Improper placement may cause the system to operate incorrectly. Emergency power sources must also be capable of handling air conditioning systems within the computer room because most computers cannot operate without air conditioning.

(6) Housekeeping. The enforcement of good housekeeping practices increases overall security for computer operations (AR 18-2).

(a) Smoking and eating in the computer room should not be allowed. A cup of coffee accidentally or purposefully spilled on a computer mainframe or tape drive unit could cause extensive damage.

(b) Trash containers within the computer room should be made of fireproof material and have properly fitting lids.

(c) Fire extinguishers should be stored so they are readily available when needed.

(d) Proper disposal of input and output media is important. In the hands of unauthorized persons, this information could be compromised and could lead to breaches of national security.

(7) Water damage. The following two areas of concern are important in preventing water damage to the computer room:

(a) Natural flooding. Surface water within the computer room is possible if the room is located on the ground floor or basement of an area subject to flooding. Storms may cause damage to the computer room if it is located on the outer wall of a building containing large glass windows.

(b) Manmade fixtures. Plumbing should not be allowed to run over, under, nor alongside the computer room be cause extensive damage could occur if such pipes should burst. Floor drains, sump pumps, and protective equipment coverings may minimize water damage to the computer room.

11-2 System Integrity

a. Hardware is the physical equipment or devices forming a computer and its peripheral equipment.

(1) Alternate data storage refers to equipment/files available as auxiliary or backup to the primary computer system. Alternate storage should not be located in the same computer room with the primary system. Physical security of the alternate should be similar to that of the primary system.

(2) Computer maintenance on hardware is a continuing process. It may involve an unscheduled stoppage or normal preventive maintenance. Knowledge and supervision of maintenance personnel are important. Security requirements differ depending upon whether maintenance is performed by internal or external services. Physical security standards must be strictly enforced during maintenance operations.

(3) Key punch equipment and locations should have physical security equivalent to the material being prepared or punched.

(4) Computer terminals require physical security procedures based on their performance requirements. Location of the system user must always be considered when setting up a system with various station locations. A given user may have full authoritative access to certain information, but certain locations may not have access to that information because of unauthorized persons in the area. Security technical protective measures should be directed toward these areas:

(a) Data controls
(b) Access controls
(c) Password controls.

153-846 0 - 94 - 10

(5) Secure handling of sensitive and classified information should be emphasized to everyone in the computer complex.

b. Software refers to the program and routines used to extend the capabilities of the computer.

(1) Necessary security precautions should be implemented to insure knowledge of who writes the program, where they are written, where they are tested and filed and what is the security classification of the program.

(2) Data file systems contain information that can be processed or produced by the computer. These files must be provided a degree of security commensurate with the importance of the files. A typical data file system allows for the creation of a unique file with the establishment of a password when the file is created. The system must respond to the privacy of the password itself, and must prevent printouts or readouts or system reviews that would reveal the password. In addition to passwords, some files are further protected by a *permissive* system. The names of valid users should be explicitly stated as having certain very specific access to the file, such as *read* or *write.* In this manner a file can be put to its maximum use by allowing differing and restricted use simultaneously to various users at various levels of authority.

(3) Documentation provides the historical reference record of data file systems and programs. The same degree of physical security should apply to documentation as in paragraphs 11-2a(2) and (3).

c. For further guidance in this area, see AR 18-2.

11-3 Procedures and Control

Procedures and controls encompass the entire area of operation concerning the computer complex. The areas of interest are diverse, as the following example shows:

a. Separation of Duties. In most computer complexes, personnel are divided into several functional groupings—programers, operators, librarians, data preparers, and data controllers. These are in addition to internal audit personnel and the security force, which are usually independent of data processing operations. It is not always necessary or possible for these groupings to be separate and distinct; but in a large computer operation they should be so grouped. The **security classification of** these personnel must be **commensurate with the level of classification of the data or program that they are processing or developing.** This factor is highly significant in the staffing and use of personnel.

b. Rotation of duties is sound personnel management and an essential control.

c. Production schedules should contain run authorizations, time estimates, data file and program library release memoranda, data preparation instructions, output routing and input and output checking guides. All production work should be run according to the schedule and all program development should be controlled separately.

11-4 Protection Of Crime Scenes

a. A breach of physical security is, in most instances, a crime; and the scene of the breach must be treated as such. The first principle is to **refrain from disturbing it.**

b. Protection may then be afforded to the scene through the use of other security forces on fixed posts, roving foot patrols, motorized patrols, or by roping or blocking off the area with available materials such as ropes, boxes, or boards (see TC 19-23).

c. Complete protection is essential to **insure that no evidence is moved** until the investigators can record its exact location and condition by the use of notes, sketches, photographs, or other means. Protection also preserves the integrity of the evidence for proper identification and evaluation, and enables investigators to correlate the evidence with the crime and crime scene.

11-5 Personnel at the Scene

a. Persons at or near the crime scene must be considered as part of the scene and must be identified. Where appropriate, and where jurisdiction of place and persons is clear, they should be detained at the scene and released to investigators.

b. Any questioning of such personnel must meet the requirements for warning of rights under the Manual for Courts Martial, and the Fifth Amendment to the Constitution must be strictly observed, since they may later be considered as suspects, and any improper questioning could prejudice any disciplinary or legal action against them. Careful and complete notes should be made of any spontaneous or voluntary information they offer, or any remarks they make.

11-6 Assistance To Investigators

Security force personnel can assist investigators in numerous ways, both at the scene and during later phases of the investigation. Protection and control of the scene is, of course, the first consideration. Nothing should be disturbed or removed until it is released by the investigators.

a. All information obtained should be turned over to investigators immediately upon their arrival.

b. Provide investigators with any information they request relative to the installation, scene of the breach of security, activities and personnel pertinent to the situation. Such information may include observations as to vulnerability of the area, which permitted the breach of security to occur reports of previous incidents of the same or similar type, when and where they occurred, and their effect on routine operations of the installation; and information concerning the security classification of the area, if any, and the pass or badge system or other personnel circulation control measures (chapter 4).

c. Security force personnel can also provide facilities for the questioning of persons; can insure that personnel are available for questioning; and if apprehension is necessary, provide information as to where the subject can be located and what assistance can be rendered by the command to facilitate apprehension.

d. The security force may also assist investigators, at their request and under their direction, in searching for, locating, and preserving any physical evidence pertaining to the breach of security. In such activities, caution must be exercised to avoid any action that would contaminate or impair the integrit y of the evidence. Evidence must be handled—if at all—strictly in accordance with the directions of investigators, who are ultimately responsible for it.

e. Security force personnel should be familiar with the provisions of FMs 19-10 and 19-20 with respect to handling and preservation of evidence, and adhere strictly to those provisions.

f. Run Control Log. This log should contain detailed records of all runs, errors, interruptions, and restarts. For sensitive operations, a console printer, recording all of the operations listed above, may be located remotely or in a secured part of the computer complex.

g. Operations Review. Sound management of a computer complex requires that actual performance be compared to scheduled

performance and any variations be noted, investigated, and explained. Production schedules and run control logs are essential inputs to this process.

h. Input and Output Control. Quality control and checks of all input and output should be maintained by a separate data control group. Special efforts should be made to insure that data accepted by data control is not altered prior to processing. This is required not just for control, but is essential for detecting and correcting errors.

i. Program Change Control. Changes to production programs should occur only upon authorization. Verification of any change should be made by the internal audit group prior to replacing the audit copy in the library.

j. Master File Control. Master file changes should also be made only by authorization, and should be subject to an internal system of checks and balances.

k. Rigid Control of Passwords. In a teleprocessing environment, passwords should not be assignable from the console, nor transmitted to users by telephone. Wherever possible, terminal identification and password match should be required.

l. Auditing Support. Skilled and experienced audit personnel on the installation may increase computer security by participating in the development and maintenance of standards and procedures for systems design, programing, and operations.

m. File Protection Devices. Maximum use of file protection devices and techniques will assist in preventing accidental or willful destruction of data files.

n. Manual Operations. Systems design should include provisions for short-term manual operation whenever possible in the event normal operations are disrupted.

o. Hardware Monitoring Prevention. An independent survey by technically qualified persons should be conducted at all computer facilities to determine external hardware emissions and methods available to reduce or eliminate emissions capable of being recorded by undesirable sources.

11-7 Evacuation And Contingency Planning

a. Evacuation planning should be initiated to insure that immediate and effective action is taken in case of required evacuation of the computer complex due to fire, flood, bomb threat or enemy action. These plans should include:

(1) Procedures for securing and priority evacuation of certain data files.

(2) Criteria for destruction of hardware, software, and data files prior to evacuation.

b. Contingency or emergency planning is important in case the everyday operation of the computer complex is disrupted or completely destroyed. Contingency planning should afford the ability to continue operations using auxiliary power sources and alternate equipment.

c. Further guidance in this area is found in AR 18-2.

11-8 Computer Security Program

Computer security is the sum of man y parts. A total security program should include a blend of procedural safeguards, an interface of physical protection, personnel selection, and audit controls. There should be an integration of all interdependent features.

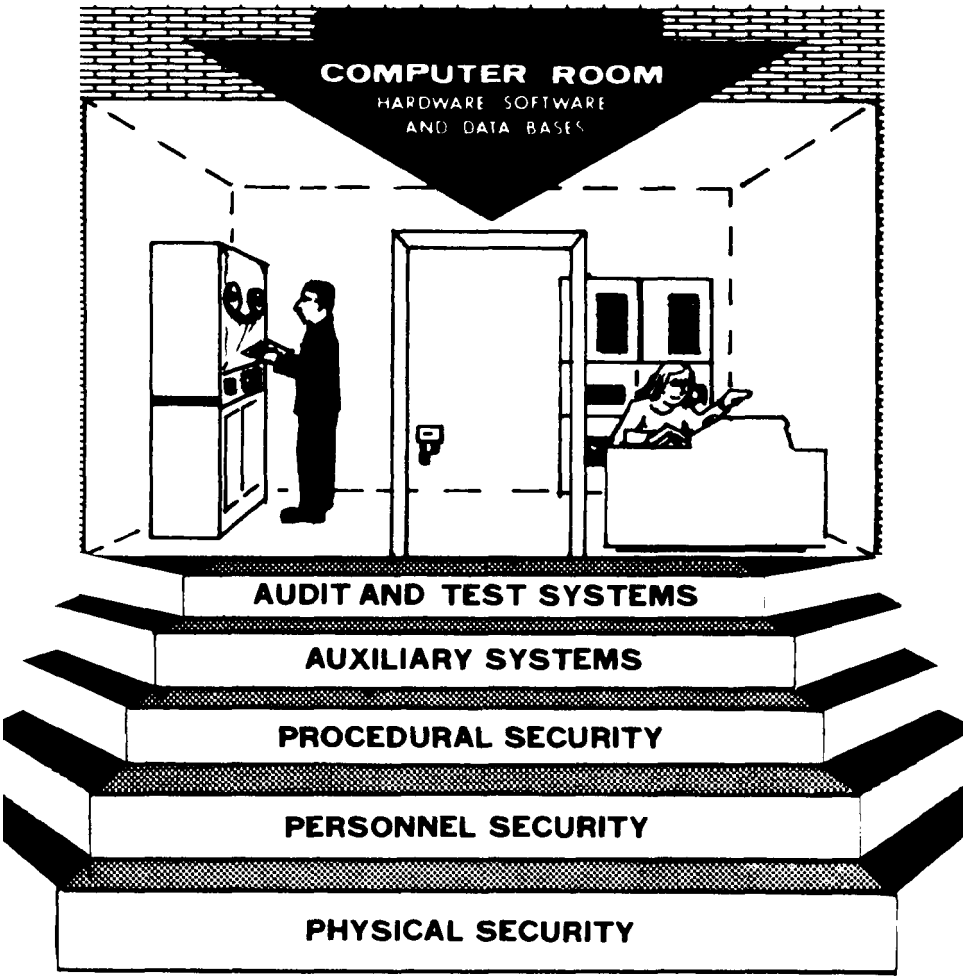

Figure 77—Five steps to computer security.

Where possible, each of these individual controls should be built into the computer system at the start. An effective program is a continuing one.