INDUSTRIAL AND COMMERCIAL

SECURITY

ADJU 276

COMPUTER FACILITY

SECURITY DESIGN

Rexford G. Booth
29 November 1978

A. STATEMENT OF PROBLEM

1. Background:

The Heck Department Stores of Carter City are expanding their operations and have decided to invest in the latest Giant Computer Company equipment including inventory control from point of sale cash registers.

2. Description of Current Facilities:

The building housing the to be replaced computer equipment is on the banks of the Four Mile Trot. This is a low rent area and, although there have been periods of high water, the dam at Deer Croft has always kept things under control.

3. Decisions to be Made:

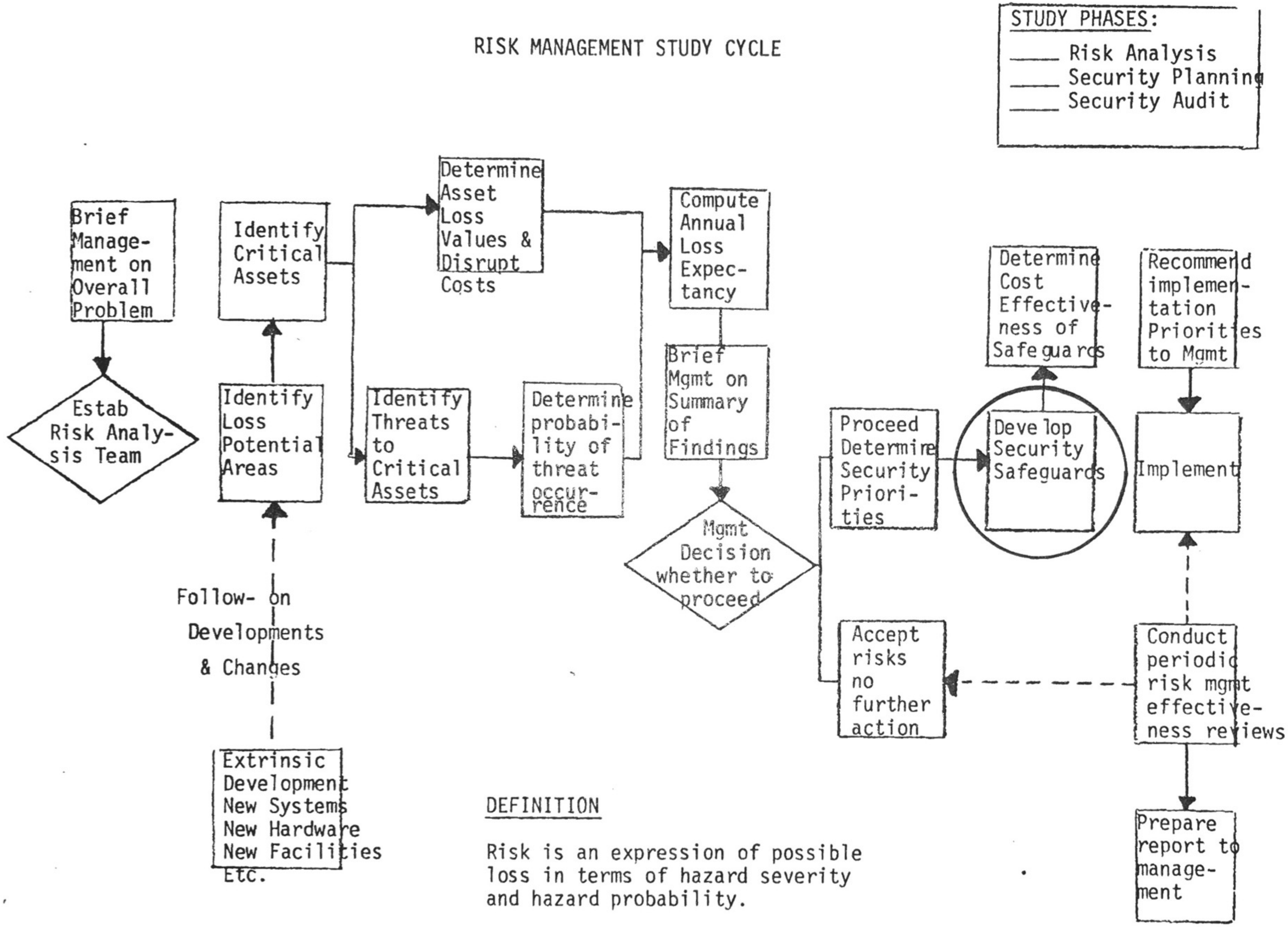
a. Should the new computer equipment be installed in the present building or a new location?

b. What security measures should be implemented?

4. Present Status:

The company officer in charge of computer operations has briefed management on the overall problem and a Risk Analysis Team has been established. The Risk Management Study has proceeded to the circled block on Figure 1. Management made the decision at the end of the Risk Analysis phase of the study that the newer and far more expensive computer equipment should be installed in a new facility, one not prone to damage due to flood and one that would intrinsically provide a higher degree of physical security. The floor plan for the new building, a cinderblock-brick veneer shell, is shown

RISK MANAGEMENT STUDY CYCLE



DEFINITION

Risk is an expression of possible loss in terms of hazard severity and hazard probability.

FIGURE 1

in Figure 2. This paper will deal with the actions required to develop security safeguards for the new facility. The yet to be constructed new building will be located in a newly developed industrial complex located ten miles South of Carter City and 100 yards from the Shirley P Memorial highway. The complex is enclosed by an eight foot high chain link fence except for front and rear entrances on major traffic arteries.

B. PHYSICAL SECURITY SAFEGUARDS

1. Exterior Barriers:

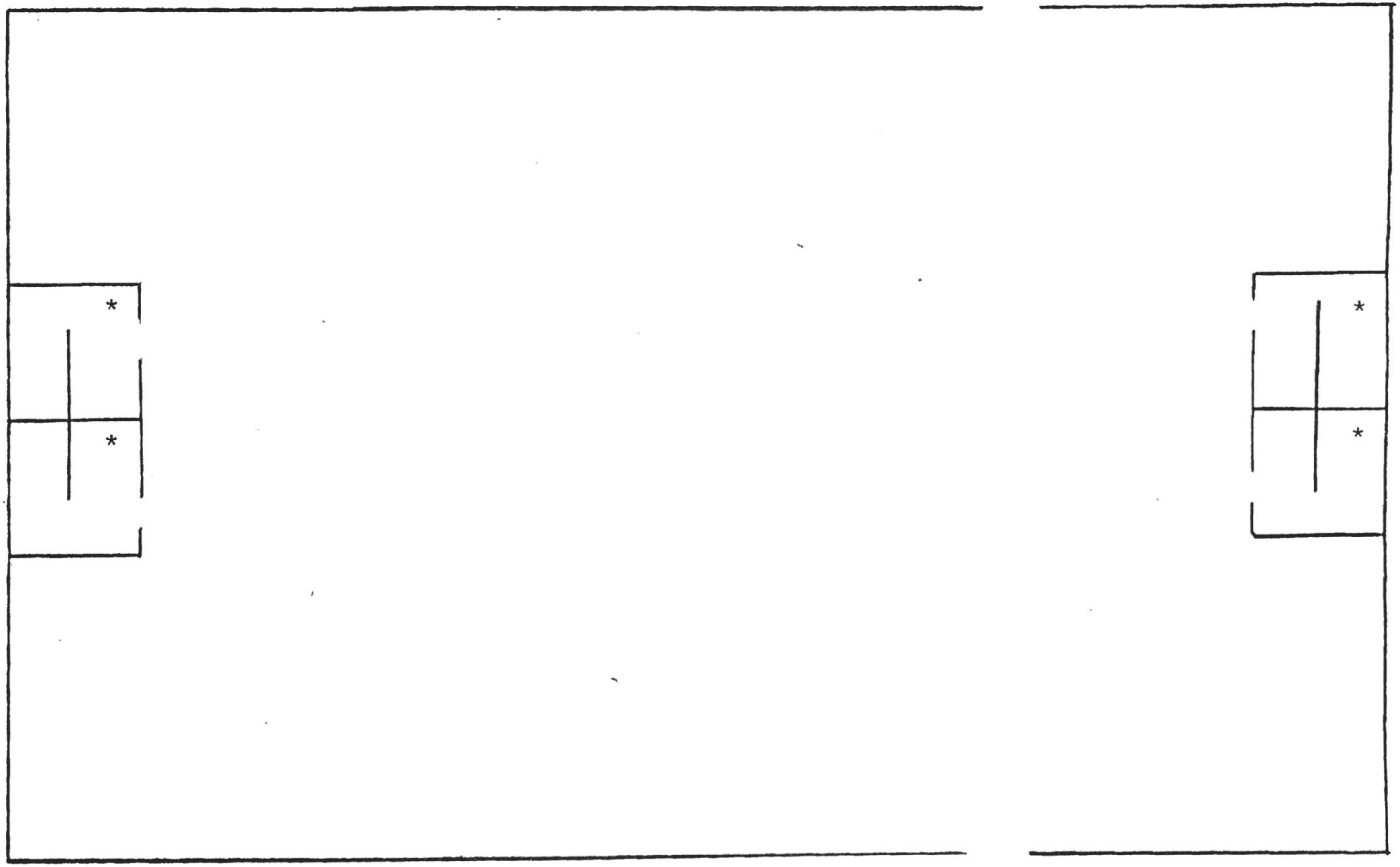
Due to aesthetics, lack of space, and the existance of a fence around the entire complex, additional fencing will not be provided. Lighting will be provided for the exterior of the building, both for security and for personnel safety.

2. Doors, Windows, Locks, etc:

As shown in Figures 2 and 3, there is only one entrance and two exits. The entrance door, although aesthetically pleasing, will be a steel door with a recessed mortise lock fitted with a Medico high-security cylinder. The steel exit door will not allow entrance from the outside and will be equipped with alarmed emergency exit hardware on the inside. Since the Heck Company has committed itself to a long term lease, and since the lease was negotiated prior to construction, no windows, sky lights, etc. will be included in the building. Ventilation openings will be kept to a minimum size and will be alarmed.

3. Interior Layout:

The floor plan of the new building will be modified as shown in Figure 3. The computer facility will be included in a separate cube within



* Rest Rooms

FIGURE 2. FLOOR PLAN OF SHELL

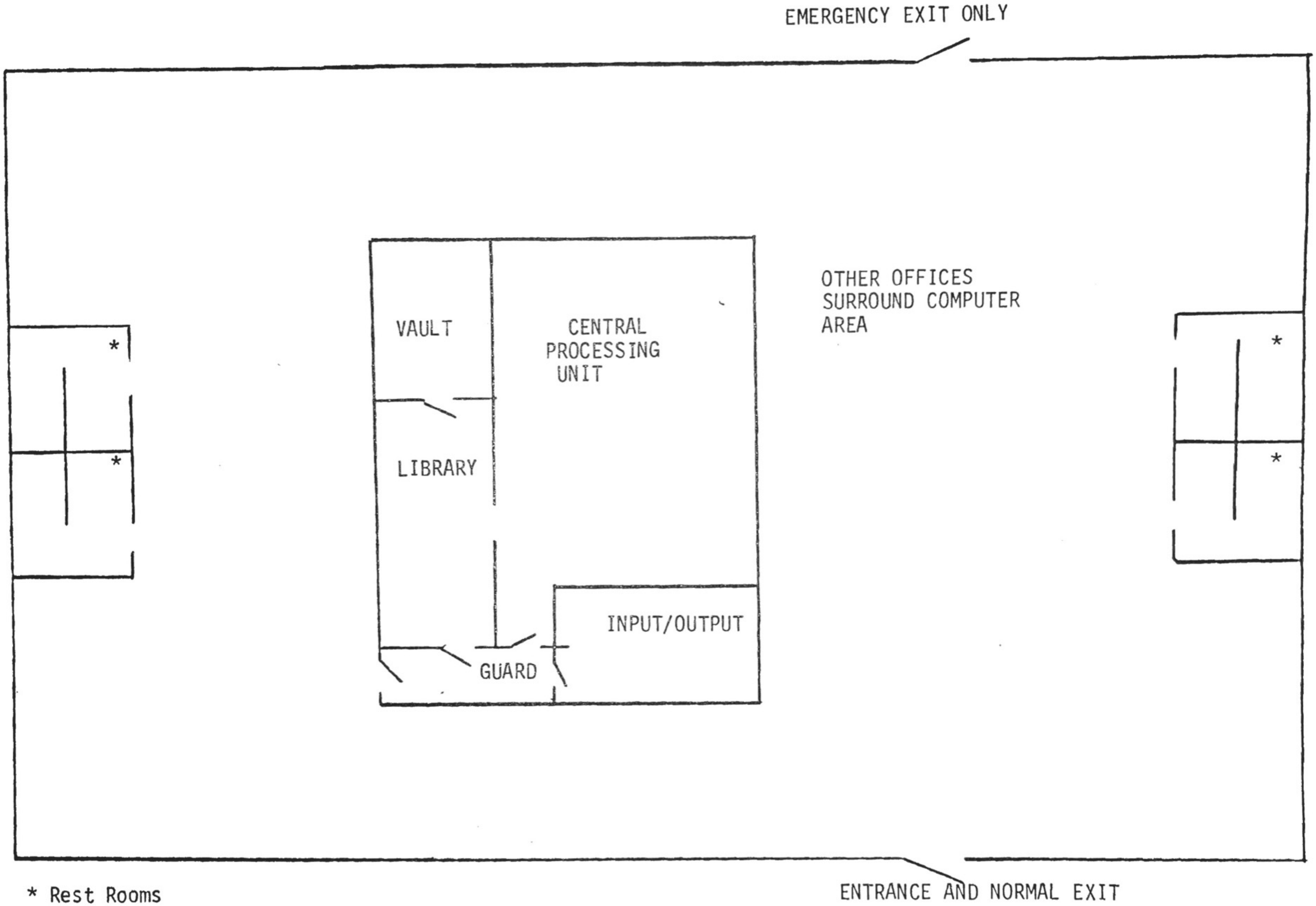


FIGURE 3. PROPOSED FLOOR PLAN

the new building and will include a vault, library, central processing unit (CPU), input/output room, and guard area.

4. Alarm System:

The new computer facility will be operated two shifts per day six days per week. To provide protection during the non-duty hours, a Grade AA Central Station No. 2 Keyed alarm system will be installed. Since the vault will contain computerized data representing: accounts receivable (into the millions of dollars), inventory records, proprietary information on promotions and sales, personnel records, etc, the vault will be protected by a separate Grade AA Central Station Complete alarm system. Latching duress sensors will be provided for the door guard and the librarian.

5. Fire Protection and Alerting:

The CPU room, because of the severe damage that could be caused by water, will be equipped with a Halon type dry fire extinguishing system and the remainder of the building is to be protected by a wet pipe sprinkler system. The fire/smoke detection sensors will report on both the vault and premise alarm systems.

C. PERSONNEL SECURITY

1. Access Control:

During normal operational shifts, one guard will be provided to monitor ingress and egress of operational personnel. Due to the relatively few personnel on each shift, access control will be by area keyed picture badges supplemented by personnel recognization (both by guard and by operational personnel). The guard, from his vantage point, controls ingress to each area; input/output room, library, and CPU room.

2. Employee Supervision:

Every organization with a computer is vulnerable to fraud. The odds are quite high that the perpetrator of this fraud will be one of the employees. The thief in an organization may be anyone. He may not profit from his theft, but he will steal anything. Any item with a physical presence can be stolen, whether it is gold, garbage, or information.

Experts in loss prevention claim that 50% to 75% of all employees are involved in occasional pilferage of items from their employer. About 25% of employees are involved in systematic stealing of items, and about 5% steal in volume. The computer can be used most successfully in these last two areas to assist in thefts. When employees are involved in systematic stealing, they come to expect the extra income and adjust their standard of living accordingly. Thus, once involved in this type of activity, the employee is likely to steal for a long period of time.

Heck Company management will develop plans to be on the lookout for employees who:

a. Consistently borrow money

b. Associate with undesirables

c. Drink excessively

d. Live beyond income

e. Gamble

f. Object to procedural changes

g. Shun vacations

h. Become overly friendly with shippers

3. Privacy Safeguards:

The Heck Company computer records contain personal data on customers and employees. Privacy is defined as:

a. The right of an individual to self determination as to the degree to which the individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations.

b. The right of individuals and organizations to control the collection, storage, and dissemination of their information or information about themselves.

Heck Company will establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience,

or unfairness to any individual on when information is maintained. The following will be considered when establishing these safeguards:

a. The Privacy Act of 1974

b. Freedom of Information Act

c. Fair Credit Reporting Act

E. INFORMATION SECURITY

1. Soft Spots:

To quote from Brant Allen's Embezzler's Guide to the Computer, published in the Harvard Business Review, July-August 1975,"To steal from an organization, it does not really matter what industry you are in or whether you work for a profit-oriented, governmental, or not for profit group. It does help, however, if you are in a position of responsibility and are a "trusted" employee the greater your responsibility, the better. Knowledge of basic accounting, record keeping, and financial statements is also necessary, though the same is not so of the computer. You are in the ideal position of not needing to know a lot about computer technology in order to beat it. The auditors and management must, however, know a great deal in order to catch you at it. The best embezzlement schemes have to be well executed to work, but the ideas are simple."

The following soft spots are discussed in Mr. Allen's guide:

a. Disbursments Fraud: "A voucher is the next best thing to money."

b. Inventory: "It is easier to convert goods to cash."

c. Sales Manipulation: "Shipping documents are vulnerable."

d. Payroll Fraud: "It is easiest in companies with a large, varying work force."

e. Pension Benefits and Annunities: "Keep a deceased pensioner on the file."

f. Accounts Receivable: "The computer can be your scapegoat."

2. Auditability Requirements:

The Heck Company security planning team recognizes the weakness described above and will establish policy and augment methodology to achieve the following:

a. Controls on personnel

b. Controls on sensitive computer programs

c. Controls on new computer programs and program changes

d. Input/output controls

e. Tape and disk library controls

f. Terminal security (software controls)

g. Terminal security (administration controls)

h. Computer logs/systems utilization/versus/time accounting

i. Fire prevention procedures

j. Physical disaster procedures

k. Systems and programming documentation controls

l. Accounting procedures for equipment and supplies

F. SUMMARY

The goal of the Security Planning Phase of the Risk Management Study is to implement the Security Model shown in Figure 4. After implementation of this model, periodic Risk Management Effectiveness Reviews will be conducted to provide the follow-up necessary in proper Risk Management to keep the proper Risk Balance between Loss Cost vs Protection Cost.

SECURITY MODEL

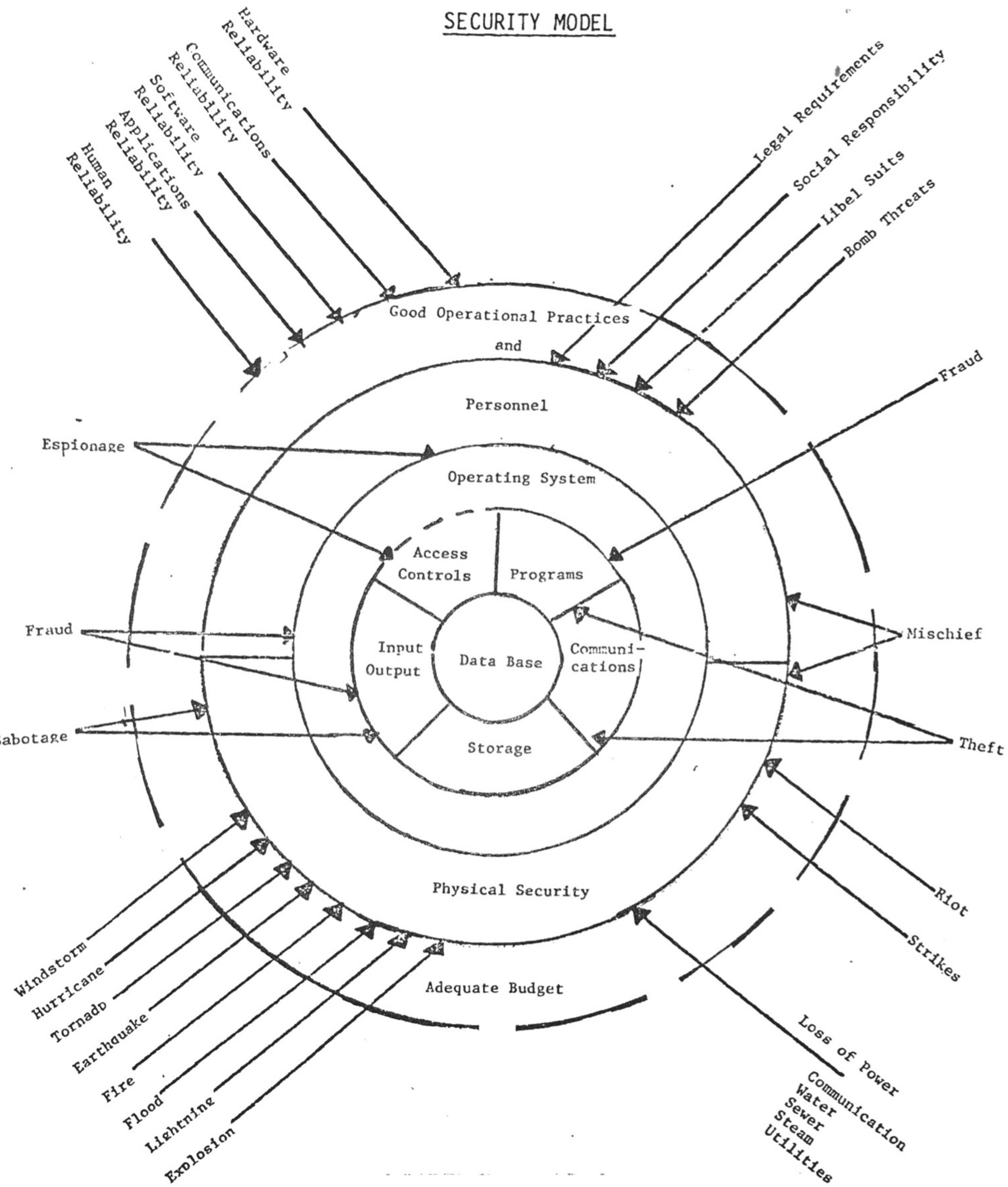


FIGURE 4