DIRECTED PATROL

A New Concept For Departmental Operations

Prepared for

University of Louisville

Department of Public Safety

UNIVERSITY OF LOUISVILLE
Department of Public Safety

DIRECTED PATROL

A New Concept For Departmental Operations

Prepared for

University of Louisville
Department of Public Safety

By

Daniel P. Keller
Director of Public Safety

James G. Elder
Crime Prevention Specialist

John W. Nolte
Crime Prevention Specialist

July, 1977

TABLE OF CONTENTS

TABLE OF CONTENTS

Dormitory Security

New Student Orientation

New Faculty and Staff Orientation

Female Safety & Security

Office and Classroom Security

Vending Machine Security

Security Product Library

Architectural & Environmental Security Recommendations

Security Surveys

Displays

Posters

Bi-Monthly Management Report

Crime Prevention Workshop

"Crime Line"

Motor Vehicle Security

Emergency Telephones

Bicycle Security

Alarm Systems - Electronic Monitoring System

Media

Statistical Analysis of Crime

Exterior Campus Lighting

Public Speaking & Contact

TECHNICAL INFORMATION.....

Introduction to Security and Risk Management

Perimeter Entrance Protection

Intrusion Detection Systems

- Introduction and Organization of the System
- Sensors
- Control Function
- Annunciation

Security Lighting

FORWARD

FORWARD

The purpose of this manual is to outline a new approach towards crime control for the University of Louisville Department of Public Safety. Although labeled as "new", this approach is really a combination or consolidation of the disciplines of law enforcement, crime prevention, security and investigation. If the specific strategies and approaches outlined in this manual are adopted and adhered to, the following results should be achieved through the concept of Directed Patrol:

1. A reduction in the number of preventable crimes on campus;

2. An improved relationship and level of communication between the university community and the Department of Public Safety;

3. An increase in the reported crime rate due to improved public confidence of the department;

4. The experiencing of a greater degree of job satisfaction on the part of the officers of the Department of Public Safety;

5. A higher rate of interception of crimes in progress;

6. Higher ratios of recovered stolen property;

7. Increased community support for the department through a better understanding of campus crime problems and,

8. Perhaps most importantly, an increased recognition of the responsibilities of each member of the university community to endeavor to reduce crime hazards.

The Traditional Approaches to Crime Prevention

The Police

According to many writers, "The police justify their existence on the premise that if criminals are detected, arrested, and punished, the crime rate will decrease." The traditional methods employed by the police have been preventive patrol of uniform officers (usually vehicular) and follow-up investigation by plain-clothes investigators. Much doubt, however, has surfaced in recent years concerning the crime prevention effectiveness of uniformed preventive patrol and the crime solving capabilities of specialized investigators.

In spite of various validity problems, the Kansas City Patrol Experiment cast serious doubts upon the effectiveness of preventive patrol. A recent study

conducted by "The President's Commission of Crime for the District of Columbia" found that an individual uniformed police officer in Washington, D.C. can be expected to detect a burglary no more than once every three months and a robbery no more than once every 14 years.

A study conducted by the Rand Corporation for LEAA revealed that in more than half the criminal cases solved, the suspect's identity was known or readily determinable at the time the crime was reported to the police. The study further concluded that serious crimes are seldom solved through leads developed independently by police investigators.

The Courts

It is popular to say these days, but merely simple logic, that effective crime deterrence must be based upon swift and certain punishment. Nothing could be further from the fact, however. Our courts have created an avoidance and escape response system. Plea bargaining, overcrowded and inefficient courts, legal technicalities and Supreme Court decisions all serve to work against the principle of swift and certain punishment.

There has never been a valid study which proved conclusively that criminals as a whole are any less intelligent than the general population. For those individuals of criminal intent or those who have little or nothing to lose from criminal pursuits, our current court system is virtually a blessing. It, combined with the other elements of the criminal justice systems makes a mockery of the saying, "crime doesn't pay." It does.

Corrections

Penal institutions have vacillated between the theories of punishment and rehabilitation for the past two hundred years. The current popular theoretical approach in dealing with convicted offenders is that they should be institutionalized or placed in a community program for treatment. Columbia Socialogist Robert Martinson concludes, however, after studying hundreds of such programs for 20 years, "The prison which makes every effort at rehabilitation succeeds no better than the prison which leaves its inmates to rot." Succeeds, that is, in reducing the huge number of repeat offenders.

The criminal justice system in our country, as it is today, is premised upon the following sequence of events:

(1) A certain number of crimes will be committed;

(2) These crimes will be reported (not necessarily so);

(3) The police will respond immediately;

(4) Through either initial or follow-up police investigation, the offender will be apprehended;

(5) Any property stolen or damaged will be returned or restitution made;

(6) The offender will be incarcerated;

(7) The offender will be afforded a fair and impartial trial and, if found guilty, will be sentenced to prison;

(8) Once sentenced to prison, the convicted offender will be rehabilitated, often learning a skill or trade;

(9) After paying his or her debt to society, the offender will be released and, due to rehabilitation, will commit no further crimes.

Does it work that way - ask yourself? In a feature article on crime some time ago, Time magazine made an illustrative study of 100 reported felonies. Of these 100 reported felonies, the following happened:

Person Arrested		20
Persons Charged		17
Referred to Juvenile Court	7	
Acquitted	2	
Fined	1	
Found Guilty of Lesser Offense	1	
Placed on Probation	3	
Imprisoned	3	

The Causes of Crime

The causes of crime are numerous and yet quite often very logical and elementary. Among the many identified causes of crime are the following:

1. There are simply more things to steal. Think about it - before we had the CB radio or 8-track car stereo fads, there were far fewer thefts from autos. Before we had IBM selectric typewriters on campus (highly desirable), there were less typewriter thefts. The widespread acquisition of portable stereos, televisions, pocket calculators, office equipment, etc. have led to the current surge in the crime rates because there are simply many more things to steal than there was 25-30 years ago.

2. There have been three major crime waves in the United States in the last century. One occurred in 1875-1880, after the Civil War. Another occurred in 1930-1935, and a third one began roughly in 1963 and continues today. Each one of these major upsurges in crime correspond to a time in our history when the proportion of persons under the age of 24 in our population was at a record high. This same age group is the one responsible for the largest percentage of crimes.

3. An additional factor relating to the major increase in crime in recent years has been the breakdown in influence of social structures and

organizations such as the family, church, schools, neighborhood organizations, etc. The stigma of divorce has virtually vanished in our country which has, in turn, led to a great many more fatherless or motherless children.

4. A relatively new problem that has appeared is the phenomenon of deurbanization. As middle-class and working-class families move out of the central cities (Louisville, for example), the neighborhoods are left in the possession of those who either cannot move or will not move.

5. Drugs, and especially the influx of heroin from Mexico, is a major contributor to the increased crime rate in certain parts of the country.

The Importance of Opportunity Reduction

We can basically view crime as the result of two elements: First the desire (and ability) to commit the crime - for whatever reason - and second, the opportunity to commit the crime. The relationship between these two elements and crime can be reduced to a simple equation:

DESIRE (And Ability) & OPPORTUNITY = CRIME

In order for a crime to take place (generally), it must first exist in the mind of the offender. This criminal state of mind may be the product of any number of a variety of sources, including:

1) Desire for monitary gain

2) Desire for acceptance within a peer group or subculture

3) Desire for revenge

4) Emotional/psychological disorders

The influence of any one of these might satisfy the element of desire. The wide variety and complexity of underlying causes seriously limits the success of efforts to prevent crime by reducing or eliminating desire.

Much like desire, opportunity arises from a variety of sources; however, the sources of opportunity can be specifically identified and proven effective measures can be taken to reduce or eliminate them.

The agency responsible for the protection of the academic institution has a unique opportunity to employ those measures designed to eliminate or reduce criminal opportunities. Most criminal offenses on campus are crimes against property. In addition, due to the nature of the institution, relatively few "professional" criminals choose the campus as a target. Thus, most crimes on campus are crimes of opportunity and can be prevented.

Without minimizing the need for criminal investigation and apprehension, Directed Patrol provides a vehicle by which the greatest amount of crime control resources afforded to the department can be focused upon the goal of crime prevention and opportunity reduction.

DIRECTED PATROL

INTRODUCTION

The University of Louisville Department of Public Safety is responsible for the law enforcement, safety and security of the university community. This responsibility includes the provision of services related to the protection and preservation of life, property, public safety and constitutional guarantees within the parameters of control of the academic institution.

The purpose of this manual is to outline the structure and mechanics of the department's program of Directed Patrol, designed to efficiently and effectively utilize allocated resources to accomplish the above-stated responsibilities.

Statement of Departmental Goals

The following are the goals of the department relating to its crime control responsibilities. The regulation of motor vehicle parking and traffic, an additional responsibility of the Department of Public Safety, is not specifically delineated within the context of this manual.

1. Crime Prevention - the anticipation, recognition and appraisal of crime risks and the initiation of some action to remove or reduce them. The anticipated consequences from the effective utilization of resources allocated to the department is the minimizing of crime problems. This goal should be achieved through the employment of proactive measures designed to eliminate or reduce criminal opportunities.

2. The Maintenance of an Academic Environment of Perceived Safety and Security - it is essential for an institution of higher education located in an urban setting to maintain a positive environment of public safety. Student enrollment and attendance is in part directly related to campus safety. What is ultimately important is how safe members of the academic community perceive themselves to be.

3. Criminal Interception - the third departmental goal, in order of priority, is the interception of individuals involved in the commission of criminal acts perpetrated upon the university community. Criminal desire is beyond the ability of the department to address itself to, and all criminal opportunities cannot be completely eliminated in the open environment of an academic

institution. Thus, the department should direct a certain amount of its efforts towards the electronic or physical interception of individuals in the act of committing crimes on campus.

4. Criminal Investigation and Apprehension - it is inevitable that although the previously stated goals are vigorously and innovatively pursued, some crimes will take place on campus. When this occurs, our goal is to actively investigate such offenses, utilizing contemporary criminal investigation procedures to apprehend the offender.

Directed Patrol Objectives

The objectives of the overall program of Directed Patrol are as follows:

1. A total commitment by every officer of the Department of Public Safety to the concept of crime prevention. Each uniformed officer will become a crime prevention "practitioner", complimented and supported by a small number of crime prevention "specialists". Uniformed officers, who inherently have the greatest degree of direct contact with the general public, will be supplied with programs and material designed to enable them to practice innovative crime prevention techniques. The full-time crime prevention "specialists" will work exclusively in the area of crime prevention and will develop the programs and material utilized by the crime prevention "practitioners". They will also assume responsibility for the more technical and detailed crime prevention projects.

2. A second objective of Directed Patrol is that of increased productivity and efficiency from available resources. The program will structure a more efficient utilization of manpower and equipment to achieve the department's stated goals. Random preventive patrol will at least in part be replaced by more positive, directed efforts at crime control. Desired results include a decrease in the crime rate on campus, more positive public contact, crime prevention counseling, crime analysis, concentration on crime, specific and more effective use of motor vehicles and equipment.

3. Improved community relations is an anticipated result of Directed Patrol. Through their crime prevention efforts, uniformed officers will have an opportunity to interact with members of the university community in such a manner as to promote relations with students, faculty and staff. Instead of most interactions being of a negative nature, each officer will have the opportunity to help people protect their persons and property and in turn, to cultivate friends and supporters for the department.

4. A major objective, in regards to the program of Directed Patrol, is that of improved criminal investigation results. Uniformed officers will bear an increased responsibility for initial and follow-up investigation of reported offenses. This reassignment

of primary investigation responsibility should result in improved initial investigations, better report writing and higher clearance rates for reported offenses.

5. Finally, Directed Patrol is intended to provide a greater degree of job enrichment for sworn officers of the Department. This should, in turn, contribute to higher officer morale and professional fulfillment. The program is designed to enable officers to employ a wider variety of skills and discretion in the performance of their assigned responsibilities. The traditionally-specialized law enforcement disciplines of patrol, investigation and crime prevention will be combined within one comprehensive job description.

I. Concept

The principle modification of operations for the Department of Public Safety in regards to the concept of Directed Patrol is the maximum utilization of personnel resources in the employment of more positive, proactive measures directed at eliminating or reducing criminal opportunities at the University of Louisville. No longer will crime prevention be a specialized function practiced only by a few select officers. Instead, every officer (police officer, security officer and Cardinal Patrol) will become thoroughly involved and active in the department's comprehensive crime prevention program. The successful adoption of contemporary crime prevention practices and projects will be the number one priority of the department.

Criminal investigation, as a function of the department, is also modified within the parameters of Directed Patrol. Uniformed police officers will have a wider responsibility for follow-up and scientific investigation. They will no longer serve merely as report-takers and initial, on-the-scene investigators. They will, instead, be held more accountable for follow-up investigation and contact for the Incident Reports they initiate.

This redirection of operational emphasis by Directed Patrol does not preempt nor diminish the need for traditional preventive patrol techniques. Instead, the concept of Directed Patrol consists of a marriage of accepted preventive patrol techniques and contemporary crime prevention measures. Directed Patrol also integrates the principles of preventive patrol and modern crime prevention measures with a broader investigative responsibility for the sworn uniformed officer.

We are, by this approach, attempting to marshall the skills and talents of every officer in the department toward the objective of eliminating or reducing criminal opportunities. By virtue of our proprietary relationship with the institution, we have a unique opportunity to affect a comprehensive crime prevention program for the University. To do so, however, will require the combined, coordinated efforts of every member of our department.

II. Organization

The Functional Organizational Diagram of the Department of Public Safety can be found at the end of this section. It

should be noted that a specialized Crime Prevention Section and a specialized Investigation Section do exist, each reporting concurrently to the Director and Assistant Director. The Crime Prevention Section will initially consist of two sworn officers, who will be referred to as Crime Prevention "specialists." The Investigation Section will initially consist of one sworn investigator.

III. Position Roles In Directed Patrol

The following is a description of the particular roles of sworn police officers, security officers and Cardinal Patrol officers within the program of Directed Patrol. These are not comprehensive job descriptions but are instead, a delineation of the respective roles of each position in Directed Patrol.

Sworn Police Officers

1. Uniformed Officers - Crime Prevention "Practitioners"

Each uniformed officer will become a knowledgeable crime prevention "practitioner". Through training and education, sworn officers will be exposed to the most contemporary crime prevention concepts. After the necessary support materials are provided, they will, in turn, be expected to agressively employ these concepts and techniques to reduce criminal opportunities on campus. Since uniformed officers naturally have the greatest degree of public contact, they have the best opportunity to interface their crime prevention skills with the needs of the university community.

The following are some of the areas of responsibility for uniformed police officers within the concept of Directed Patrol:

a. Criminal Incidents - in addition to taking and recording the necessary information and the coordination of appropriate investigative techniques, uniformed officers will have additional crime prevention responsibilities at the scene of a reported criminal incident:

(1) Determine why, from a crime prevention standpoint, the criminal incident took place. Indicate same either on the original Incident Report or, if not appropriate, on follow-up report.

(2) Advise victim of possible crime prevention measures or precautions to be taken.

(3) In some cases, make recommendations to the department concerning crime prevention measures or projects to eliminate or reduce the probability of other such incidents in the future.

b. Public Speaking - sworn officers will be requested to give crime prevention presentations to various campus groups or organizations throughout the university. These presentations may be either general or specific in nature, i.e., female personal protection, dormitory residents, senior citizens - retired faculty, etc. Uniformed officers will also be used to man crime prevention displays and booths set up from time to time in various parts of the university.

c. Operation Identification - the principle responsibility for the carrying out of Operation Identification will be with uniformed police officers. They will specifically be involved in the promotion of Operation Identification in university dormitories and apartment buildings.

d. Security Surveys - uniformed officers will conduct initial security surveys for university facilities. They will use the format to be provided as a supplement to this manual. Formal detailed security surveys will be conducted by the crime prevention "specialists", where warranted.

e. "Crime Specific" - in a program entitled "crime specific", uniformed officers will be provided with an analysis by the Crime Prevention Section of discernible crime trends on campus. The officers will, in turn, take measures to alert members of the university community in the areas where trends are noted and seek active cooperation and assistance to remedy the problem. Such measures may include the distribution and posting of flyers, meetings with staff employees, plain-clothes patrol, etc.

f. Crime Prevention Reporting - uniformed officers will be vitally instrumental in the reporting of crime prevention problems and hazards. They will report inoperative exterior security lighting, file Security Advisory Reports indicating physical

security deficiencies, and leave "Rip Off" cards in buildings, offices or vehicles found unsecured. It will be an important aspect of their role as crime prevention "practitioners" to be alert for criminal opportunities that can be corrected or neutralized.

2. Crime Prevention "Specialists"

As previously stated, the Department will have two (2) sworn officers working exclusively as crime prevention "specialists." These officers will have various crime prevention responsibilities, among them are the following:

a. Crime Analysis - the analysis of crime reports to determine crime trends and patterns. This responsibility includes the recommending of programs or projects to counteract crime problems.

b. The conducting of formal detailed security surveys for university buildings and facilities. The need for such security surveys can be generated through crime analysis, a request by university administrators, or upon recommendation by uniformed officers. Such detailed surveys may also be as follow-ups to those preliminary or initial security surveys conducted by uniformed patrol officers.

c. The design and supervision of installation of alarms, CCTV, access control systems and other related electronic security monitoring equipment.

d. The development of architectural and environmental security recommendations for new or renovated university facilities.

e. The development of university-wide crime prevention programs, to include the design of publications, displays, posters, etc.

f. Liaison with product manufacturers, the State Office of Crime Prevention, the National Crime Prevention Institute and municipal and campus law enforcement agencies involved in crime prevention.

g. Maintenance of a crime prevention library to include product information files and reference data concerning physical security.

h. Coordination with the Training Section for continued

crime prevention training within the Department.

i. The preparation of a bi-monthly crime prevention management report for the Director. This report will include a summary of those significant crime prevention activities involving the Department during the bi-monthly time period.

3. Investigator

The Department will utilize one sworn officer as a full-time investigator. In addition to serving as a crime prevention "practitioner", this officer will be responsible for the following areas relating to criminal investigation:

a. Follow-up investigation of criminal incidents requiring immediate attention.

b. Coordination of initial and/or follow-up investigation of major and/or sensitive criminal incidents.

c. To provide assistance and counsel to uniformed officers in reference to their follow-up investigation of criminal incident reports.

d. Liaison with the various elements of the local criminal justice system - courts, prosecutors, police agencies, etc.

e. Maintenance of court and prosecution records.

f. Maintenance of the Department evidence and property files.

g. Coordination with the Training Section for criminal investigation training within the Department.

Security Officers

The Department's eight (8) security officers are primarily concerned with the locking and security of physical facilities. In this role, they are 100% dedicated to the concept of crime prevention. These security officers will be further integrated into the Department's comprehensive crime prevention program through training and instruction. In addition to the locking and unlocking of physical facilities, security officers will:

1. Report inoperative external lighting.

2. Report any inoperative locks, doors, panic bars or other security hardware.

3. Report any suspicious activity observed during their normal tour of duty.

4. Participate in the "Rip Off Card" program.

5. Report open or unlocked windows and doors via the Security Advisory Report.

6. Be alert for and report to the Crime Prevention Section any other security deficiencies they observe.

7. Be knowledgeable about the various crime prevention projects and programs of the Department.

Cardinal Patrol

The Cardinal Patrol (student workers) is responsible for parking regulation and limited security on the four campuses of the university. Through training and instruction, members of the Cardinal Patrol will also be integrated into the Department's comprehensive crime prevention program. In addition to the above responsibilities, Cardinal Patrol officers will:

1. Assist the Crime Prevention Section in the maintenance of crime prevention displays, posters and brochures.

2. Be especially knowledgeable about Department programs to combat theft of and from motor vehicles.

3. Be knowledgeable about other crime prevention projects and programs of the Department.

4. Report any suspicious activity observed during their normal tour of duty.

5. Be alert for and report to the Crime Prevention Section any security deficiencies they observe.

IV. The Role of Supervisors

Supervisors will play a pivotal role in the success of Directed Patrol. Without their support and backing, the degree of success of the program will be minimal. The Shift Commanders and the HSC Post Commander will bear increased

responsibilities to insure that crime prevention activities are being carried out by uniformed officers under their supervision.

Management By Objectives

Each reporting year (fiscal year) a number of clearly-defined crime control objectives will be established for the Department. These strategic objectives will be designed to compliment the Department's long-range goals and the Department's comprehensive crime prevention program. Officers of the Department will be actively involved in the development of these objectives.

The role of Directed Patrol is to serve as a vehicle or means of accomplishing the strategic crime control objectives of the Department. Rather than merely reacting to incidents of crime, we will, through Directed Patrol, take the initiative by establishing strategic crime control objectives and then carrying them out to a successful end. Examples of such objectives may be as follows:

1. To reduce thefts from dormitories by 20%.

2. To have 80% of the dormitory residents participating in Operation Identification.

3. To give crime prevention talks before all new employees and 50% of the new students at the university.

4. To reduce theft from motor vehicles by 10%.

5. To reduce theft from offices by 30%.

6. To improve the reporting of exterior lighting deficiencies or malfunctions on campus.

7. To reduce vending machine break-ins and thefts by 40%.

8. To have 90% of the bicycles on campus registered.

Supervisors & Management by Objectives

1. Establishing Objectives

The four Shift Commander-Sergeants currently rotate every 28 days while the Post Commander-Sergeant responsible for the Health Sciences Center Campus works the day shift and does not rotate. As previously stated, these uniformed supervisors will play a vital role in

the success of Directed Patrol. Prior to their rotation at the end of each month, Shift Commanders will confer with the Director and develop Directed Patrol objectives for the following month. These objectives will subsequently serve as a guide for the Shift Commanders and their officers. These personnel will then be evaluated, both objectively and subjectively, on the accomplishment of the objectives. Since he does not change shifts, the Post Commander-Sergeant will confer with the Director and establish objectives on a three month basis.

Examples of possible Directed Patrol monthly objectives (or tri-monthly for the HSC) are as follows:

- First Shift - To provide officers as speakers for new student orientation.

- First Shift - To discuss positive crime prevention measures with the secretaries and other office staff in Davidson and Strickler Halls.

- First Shift - To set up a "rooftop patrol" overlooking the parking lots on the north end of the Belknap Campus.

- First Shift - To man the large crime prevention display in the University Center Building for three days.

- Second Shift - To hold floor meetings with the residents of Unitas Hall and have as many as possible participate in Operation Identification.

- Second Shift - To give four Female Safety and Security presentations with night students of the University College.

- Second Shift - To meet with each of the Security Officers and reinforce crime prevention measures and projects with them.

- Second Shift - To concentrate vehicular patrol in parking lots used by night students.

- Third Shift - To have an officer walk through each dormitory at least once each night.

- Third Shift - To concentrate on the patrolling of vending machine areas.

- Third Shift - To increase the emphasis on the writing of Security Advisory Reports.

- Third Shift - To conduct an exterior lighting survey of the Shelby Campus.

- HSC - To speak before new staff orientation each month.

- HSC - To give a crime prevention presentation to each department in the Dental School.

- HSC - To set up a new crime prevention display in the Medical School Library.

- HSC - To write a proposal requesting improved exterior lighting on Madison Street.

2. Performance Plan

After monthly objectives have been established by the Shift Commanders, they will meet with the patrolmen assigned to their shift and, working together, establish a performance or action plan for the accomplishment of their objectives. This performance plan will serve as a strategy or "game plan" for the meeting of their Directed Patrol objectives. This performance plan may entail special assignments, speaking engagements, modification of schedules, etc. The important consideration is that the Shift Commander (or Post Commander) work together with his Patrolmen to design a plan of action to accomplish their Directed Patrol objectives.

3. Performance Appraisal

Shift Commanders and the Post Commander will be held accountable for the successful accomplishment of their Directed Patrol objectives. They will each be expected to submit a monthly report to the Director of the Directed Patrol activities of the previous month.

V. Evaluation and Feedback

The success of Directed Patrol will, to a large degree, be dependent upon evaluation and feedback. It is anticipated that not every crime prevention project we develop will prove to be either beneficial or cost effective. Of those projects to be outlined in this manual, some will be continued, some will be modified and some may be discontinued altogether. New projects will be added. To achieve maximum utility from departmental resources, however, it is essential that evaluation and feedback be designed into the overall crime prevention program. Methodology for the generation of such

information is as follows:

1. Incident Reports - As was previously explained, officers will be required to include additional crime prevention information on original Incident Reports.

2. Statistical Analysis - Using Uniform Crime Reports, the "Crime Line", and crime statistics generated for internal use, statistical analysis of crime trends or rates will serve to indicate the success of Directed Patrol.

3. Supervisor's Activity Reports - Shift Commanders will include crime prevention activities in their daily Supervisor's Activity Reports.

4. Public Service Questionnaire - Public Service Questionnaires (see end of this section) will be sent to the victims of criminal incidents. Included as a part of this questionnaire is a section requesting the victim to assess the reporting officer's crime prevention efforts.

5. Supervisor's Monthly Reports - Shift Commanders and the Post Commander will file a monthly report citing progress in the meeting of their established objectives. Since some of these objectives may be difficult to evaluate empirically ("to concentrate on the patroling of vending machines", for example), this report will serve as an important evaluation and feedback medium.

VI. Training and Materials

Each sworn officer (22) will receive a minimum of 40 hours of formal crime prevention training. This training will be provided by either the Kentucky Bureau of Training or the National Crime Prevention Institute. In addition, each officer will receive numerous hours of in-service training directed toward the Department's comprehensive crime prevention program.

The audio-visual, multi-media training program will be directed toward crime prevention topics and programs. Departmental training bulletins, also covering crime prevention subjects, will be issued on a periodic basis. Security officers and members of the Cardinal Patrol will receive in-service training correspondent to their level of participation in the Department's overall crime prevention efforts.

Briefcases will be issued to each sworn member of the Department. Contained in these briefcases will be crime prevention

brochures, pamphlets, decals, engravers for Operation Identification, posters, etc. Uniformed officers will be required to have their briefcases with them whenever they are on duty. The purpose of these briefcases is to make crime prevention support material available to the uniformed officer at the time he or she needs it most--while on patrol.

VII. Criminal Investigations

One of the primary objectives of Directed Patrol is that of improved criminal investigation efforts. Traditionally, uniformed police officers complete criminal reports at the scene of a criminal incident and conduct, to varying degrees, initial investigation of the incident. If the criminal incident is not solved through initial investigation and there are either leads or information requiring follow-up or the incident is serious enough to warrant such follow-up, a specialized plain clothes investigator will be assigned to the case. In most instances, the uniformed officer who responded to the incident and completed the initial report loses contact with the victim and the incident.

Through Directed Patrol, we hope to expand the investigative efforts and involvement of uniformed police officers. Effective immediately, the following guidelines will be followed concerning criminal investigations:

1. Uniformed officers will be permitted, whenever possible, to conduct follow-up investigations of those criminal incidents to which they initially responded. Such investigations may be conducted independently or in conjunction with the department's investigator. Follow-up investigations may entail a changing of shifts, a plain clothes assignment, a stake-out, etc. Follow-up investigations by uniformed patrol officers should be coordinated through the Assistant Director and the appropriate Shift Commander.

2. Whenever a member of the university community is a victim of a criminal incident, a special effort should be made by the initial investigating officer to maintain or restablish contact. The primary purpose of this procedure is to reassure the victim of the officer's interest and concern about the criminal incident. A secondary benefit of such contact is that new or revised information concerning the incident often comes to light.

The anticipated results of these new procedures are numerous. Patrol officers should have a greater degree of self actual-

ization from being able to carry a criminal incident through from its beginning to some type of conclusion. Since the cases investigated will be their own, patrol officers can be expected to do a more thorough and complete job in the initial phases of the criminal investigation and preparation of preliminary reports. Hopefully, such procedures will result in higher clearance rates for criminal offenses. Finally, more positive public relations with the university community should be established by officer's follow-up contact with victims of criminal incidents.

VIII. Criminal Complaint Procedures

A flow chart, depicting the criminal complaint procedure a uniformed patrol officers should follow may be found on the following page. This chart illustrates the following steps that should be taken whenever a criminal complaint is received:

1. A complaint is initiated by either the officer or someone else.

2. The officer arrives at the scene.

3. A decision point is reached - "is immediate action on the scene necessary?"

4. If the answer to question 3 is yes, seriously injured persons should be attended to.

5. If the arrest of a criminal offender is possible at the scene, it should be affected next (step 4 and 5 may be reversed, depending on the circumstances involved).

6. The following step is to secure the scene for witnesses, information and evidence.

7. A decision point is again reached - "are technical persons required?"

8. If the answer to question 7 is no, the officer should then gather his or her information and begin preparing the Incident Report.

9. If the answer to question 7 is yes, the appropriate interdepartmental or intradepartmental technician(s) should be called.

10. Whether the answer to question 7 was yes or no, the

preparation of the Incident Report should logically follow.

11. If the answer to question 3 was no, the Incident Report should be initiated as soon as possible.

12. After the Incident Report has been written and filed, the next decision point is reached - "is follow-up investigation possible?"

13. Regardless of the answer to question 12, positive crime prevention measures should be discussed with the victim and/or others, whenever possible.

14. If the answer to question 12 is yes, follow-up investigation should be coordinated with the Assistant Director and I-Section.

15. The results of such a follow-up investigation will then render the case either "cleared" or "inactive". In either event, the victim of the crime should be recontacted by the uniformed officer who initially responded to the complaint.

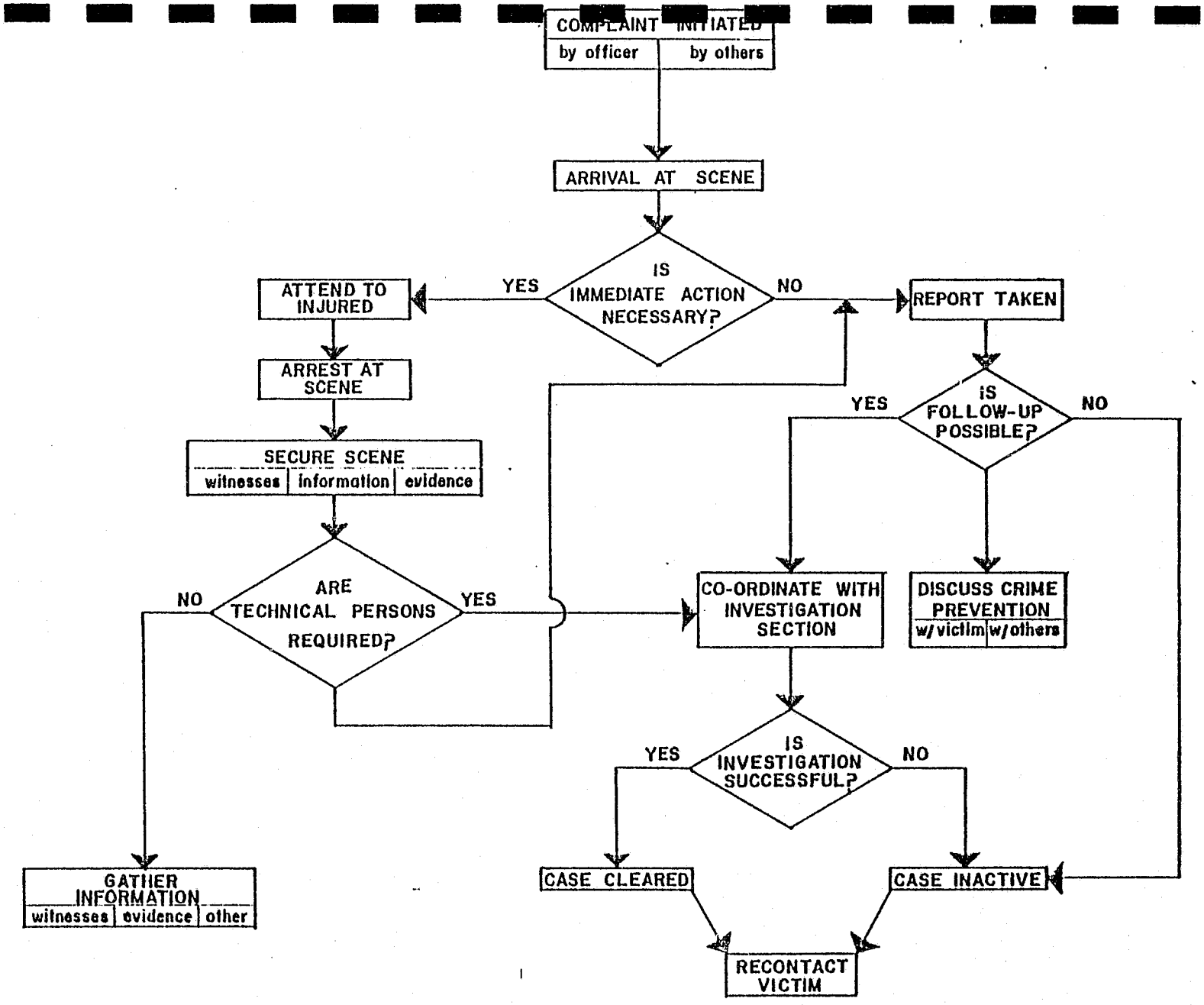
16. If the answer to question 12 was no and further investigation was not possible or practical, the case would be considered "inactive". The last step involves recontacting the victim to advise him or her of any progress made. Such contact should be made by the officer who initially responded to the incident.

As indicated by this flow chart, there are at least three major steps that should be taken in the response to and reporting of all criminal incidents:

- The collecting of information and the taking of the initial Incident Report.

- The discussion of crime prevention measures, whenever possible, with the victim or others involved.

- The recontacting of the victim by the reporting officer.

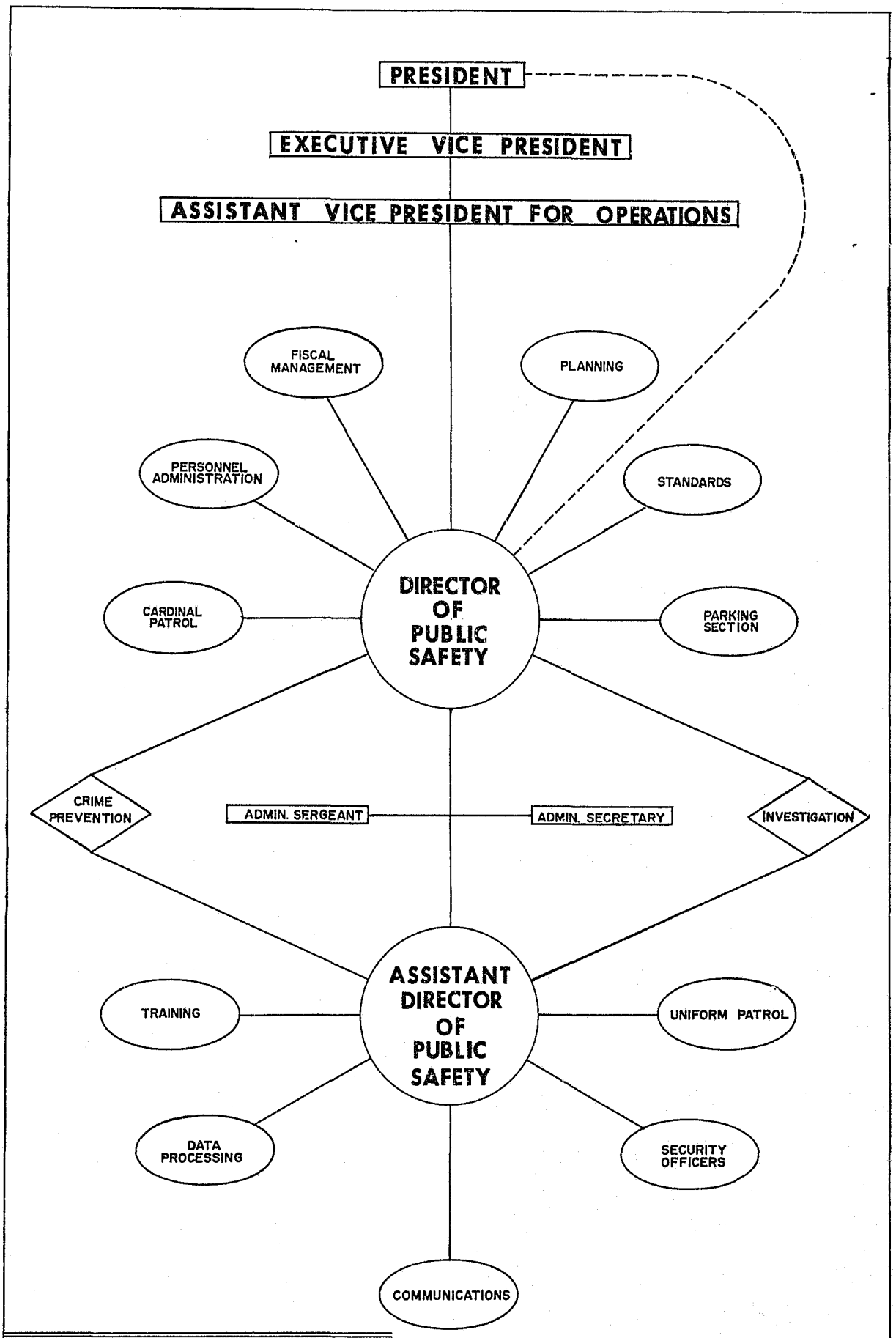


CRIMINAL COMPLAINT PROCEDURE

JGE

SUMMARY

Directed Patrol is designed as a program to fully utilize the resources of the department in its crime control activities. Rather than relying solely or even primarily on the traditional concepts of preventive patrol, Directed Patrol gives us the opportunity to take the initiative and employ a comprehensive attack against crime. We have a fine department with excellent personnel. Directed Patrol allows us to more fully make use of the education, training and skills of our officers to the greatest advantage for the protection of the university community.



UNIVERSITY OF LOUISVILLE
DEPARTMENT OF PUBLIC SAFETY
FUNCTIONAL ORGANIZATIONAL DIAGRAM

UNIVERSITY OF LOUISVILLE
Department of Public Safety

PUBLIC SERVICE QUESTIONNAIRE

1. Were you accommodated promptly and without unnecessary delay? Yes_____ No_____

2. To what degree was competence in evidence on the part of the police officer(s) with whom you had contact? Excellent_____ Good_____ Fair_____ Poor_____

3. How would you evaluate the element of courtesy in your contact?
Excellent_____ Good_____ Fair_____ Poor _____

4. Did the officer discuss positive crime prevention techniques with you?
Yes_____ No_____

5. Based upon your observations and contact with our Department, would you say, in general, that the Department of Public Safety is doing a good job, an average job or a poor job?

Good Job	( )	Poor Job	( )
Average Job	( )	Don't Know	( )

6. How much confidence do you have in the Department of Public Safety?

A Great Deal	( )	None at All	( )
Some	( )	No Opinion	( )
Very Little	( )		

7. How much confidence do you have in police departments, in general?

A Great Deal	( )	None at All	( )
Some	( )	No Opinion	( )
Very Little	( )		

8. What additional comments or recommendations for improvement would you care to suggest?

_____

_____

_____

_____

THANK YOU FOR YOUR ASSISTANCE...

Name_____

UNIVERSITY OF LOUISVILLE
Department of Public Safety

COMPREHENSIVE UNIVERSITY CRIME PREVENTION PROGRAM

Introduction

To be effective, a crime prevention program should be systematic and comprehensive in nature. It should not consist of isolated or fragmented one-shot projects directed solely at the current crime program. Instead, an effective crime prevention program will incompass a wide range of projects aimed at the overall crime problems of the jurisdiction for which it is designed.

Two direct results of a successful crime prevention program which should be anticipated are an increased reporting of crime and the displacement of crime. Crime prevention awareness usually stimulates victims of crime, especially victims of petty or minor crimes, to increase their reporting of such offenses to the police. As they become more conscious of crime prevention measures, people also become more aware of criminal activity. Offenses that they might otherwise take for granted or ignore are then often reported. Thus, the end result of a good crime prevention program may well be an initial increase in crime reporting.

In a campus environment, we have a unique opportunity to displace crime. Generally, we do not have the type of crime targets that attract the interest of "career" or "professional" criminals. Most of the criminal offenses committed on a college campus (especially crimes against property) are committed by juveniles, opportunistic thieves, and lower-level criminals (this is a general statement and certainly not always the case). If crime risks on campus are identified and either reduced or eliminated, these criminal elements will often look elsewhere for easier opportunities of prey. Since an institution of higher education is usually a rather well-defined location, such criminals become displaced by effective crime prevention activities.

Strategic Goals

The following are the strategic goals of the Department of Public Safety's comprehensive university crime prevention program.

1. The first priority of the Department of Public Safety is to minimize the occurrence of determinable crimes.

2. An additional goal is to provide for the academic community an environment of both actual and perceived safety and security.

3. The fostering of positive public relations with the university community is a third goal of the department's crime prevention program.

4. Finally, it is a stated goal of the Department of Public Safety to develop the finest comprehensive campus crime prevention program in the country.

Crime Prevention Projects

1. Operation Identification

a. Crime Prevention specialist to coordinate.
b. Priorities:
   (1) University dormitories and apartments - students
   (2) Personal property of staff and faculty at the university
   (3) The homes and property of faculty and staff
c. To be assigned to Shift Commanders and Post Commander as objectives.
d. Periodic ads in Potential and Cardinal.
e. Ads on FM radio station.
f. Poster campaign.
g. Coordinate for employees with State Office of Crime Prevention.

2. Dormitory Security

a. Crime prevention decals for dormitory and apartment doors.
b. Operation Identification.
c. Alarming of vending machines.
d. Alarming of exterior dormitory doors.
e. Packets of crime prevention brochures.
f. Telephone decals.
g. Rape prevention sessions.

3. New Student Orientation

a. Crime prevention packets for Belknap Campus - 2,000
b. Crime prevention packets for HSC Campus - 350
c. Slide presentation for Belknap Campus
d. Slide presentation for HSC Campus
e. Article in orientation booklet.

4. New Faculty & Staff Orientation

a. Packets of Crime Prevention Brochures - 750
b. Slide presentations for Belknap & HSC Campuses.

5. Female Safety and Security

a. Police Officer to coordinate.
b. Use State Office of Crime Prevention brochures and films
c. Coordinate with Director of Housing.
d. Training bulletin for DPS.
e. In-service training for DPS.
f. Priorities:
   (1) Dormitories
   (2) Student organizations
   (3) Open sessions
   (4) Faculty & staff

6. Office & Classroom Security

   a. Operation Identification
   b. Articles - Potential (staff newspaper)
   c. "Crime Line"
   d. Brochure - "Message to University Employees
   e. Security surveys
   f. Posters
   g. Brochure displays
   h. "Crime Specific"
   i. Crime Prevention Building Committees
   j. Security Advisory Reports
   k. "Rip Off" cards

7. Vending Machine Security

   a. Concentration of machines
   b. Alarming of vending machines
   c. Protected vending areas (hardware)
   d. Improved random patrolling - route

8. Security Project Library - crime prevention specialist to maintain.

9. Architectural & Environmental Security Recommendations

   a. Crime Prevention Specialists
   b. Technical Advisory Group to Office of Facilities Management
   c. "General Architectural and Environmental Security Recommendations for Institutional Facilities."

10. Security Surveys

    a. Crime prevention specialists to coordinate
    b. "Security Survey Format for Patrol Officers"

11. Displays

    a. Big portable display
    b. Bicentennial displays
    c. Bicycle display
    d. Bulletin board displays
    e. Styrofoam display

12. Posters

    a. Permanent posters
    b. Poster series
    c. Operation Identification

13. Bi-Monthly Management Report - To be prepared by Crime Prevention Section.

14. Crime Prevention Workshop - To be coordinated by the Director

15. "Crime Line"

    a. To be prepared by Crime Prevention Section
    b. To be sent to media, administrators, faculty & staff organizations, student leaders, etc.

16. Motor Vehicle Security

    a. Posters
    b. Big portable display
    c. State Office of Crime Prevention brochure
    d. "Insecure Vehicle Notification" - To be developed
    e. Brochure handed out at vehicle registration

17. Emergency Telephones

    a. Program to improve
    b. Brochure

18. Bicycle Security

    a. Emphasize at dormitories
    b. Future theme of big portable display
    c. DPS brochure

19. Alarm Systems - Electronic Monitoring System

    a. Crime Prevention Section responsible for design, installation & supervision of alarms
    b. Alarming of vending machines
    c. Development of Electronic Monitoring System.

20. Media

    a. Spots on FM radio station.
    b. Classified ads in Cardinal.
    c. Crime prevention fillers for Cardinal and Potential
    d. Articles in local newspapers - Courier-Journal and Louisville Times.
    e. Articles in national publications.
    f. Miscellaneous campus publications
    g. Articles in Cardinal and Potential.

21. Statistical Analysis of Crime

    a. Responsibility of Crime Prevention Section
    b. "Crime Line"
    c. UCR's
    d. Crime Specific
    e. Pin Maps

22. Exterior Campus Lighting

a. Identifying of Standards
b. Thorough survey every three months by Crime Prevention Section
c. "Corridors of Security

23. Public Speaking & Contact

a. Freshman Orientation
b. New faculty & staff orientation
c. Officer's Speakers Bureau
d. Homecoming Festival
e. Registration
f. Oxmoor Display
g. Random Displays - UC / Strickler / HSC
h. Dormitory floor meetings

24. Miscellaneous

a. Bookstore theft program
b. Crime prevention tips for faculty/deans

INTRODUCTION TO SECURITY AND RISK MANAGEMENT

From your knowledge of the university community, you are already aware that college and university campuses represent tremendous expenditures for equipment and facilities. As a member of the Department of Public Safety, it is important that you recognize that your primary function is to prevent crime. Therefore, you should be cognizant of the potential for property loss from university facilities. The concepts of (1) risk management, (2) the systematic approach to the appraisal and evaluation of facilities, and (3) methods for effecting change are presented herein to enable you, as a crime prevention practitioner, to recognize, evaluate and attempt to correct deficiencies in physical and functional security. In addition, these theories should permit you to discuss reasonable and effective loss prevention measures with other members of the university community.

I. Risk Management

Risk management is defined as the "anticipation, recognition, and appraisal of a crime risk and the initiation of some action to remove or reduce a potential loss to an acceptable level." Risk, or the potential for loss, can be divided into two broad categories. The first is dynamic risk or the potential for loss due to some normal business operation (i.e., a merchant who accepts personal checks knowing the possible loss will be overcome by increased sales). Dynamic risk exists only in limited amounts on college campuses. Pure risk, on the other hand, does apply to an academic setting. This type of risk involves the potential for loss because of ignorance or the inability of the potential victim to protect his property. The crime prevention practitioner's function for the institution is to anticipate the potential for loss, recognize the deficiencies contributing to the risk, appraise the potential loss, and initiate some action to reduce or remove the risk.

There are five approaches to risk management that can be used singularly or in combination with one another to remove or reduce risk. The first approach, risk avoidance is defined as analyzing the situation to determine if the risk can be removed by eliminating the criminal opportunity. The second method, risk reduction, can be used when avoiding or eliminating the criminal opportunity conflicts with the ability to carry on normal operations. The third alternative, risk spreading, suggests that by dispersing the potential loss over a wider area the exposure for the perpetrator of a criminal act is increased thus, the probability of apprehension before completion of the act is increased. This can be accomplished by locating valuables throughout an area and improving physical barriers and detection systems. The fourth and fifth alternatives are risk transfer and risk acceptance. Risk transfer involves passing the potential for loss to someone else.

The two most common methods are insurance or raising prices of marketable goodsto cover losses. Risk acceptance is the assumption of all remaining risks by the operation. Risk transfer is usually not acceptable to academic institutions because of the large premiums (i.e., insurance) involved. Risk acceptance should only be used as a last resort.

II. Evaluating the Potential for Loss

For our purposes a "high risk area" may be defined as a room, office or other area containing tangible or intangible property of sufficient value (value need not be defined in terms of dollars) to warrant special consideration because: (1) the risk of theft is great, or (2) the loss, theft or destruction of said property, even though unlikely, would result in irreplacable loss to the owner/user.

Some items, such as office equipment, stereos, tape recorders and the like may be considered high risk because they are readily fenced and in great demand. With such property, value may be expressed by a figure; therefore, such items can be replaced assuming, of course, necessary funds are available. Cash is also included in this category. Unfinished research papers, or personal photographs or mementos, on the other hand, may hold a special significance for the owner, yet no value can be assigned. The actual theft of such property in unlikely. However, should it be destroyed by fire or vandalism or stolen by a thief who mistakenly believes the items are valuable, replacement value would be impossible to assess.

A third type of property should also be considered. Such property consists of items to which a value may be assigned. In this instance values are usually assigned for insurance and procurement purposes only since the item, once stolen, cannot be replaced. Included in this property category are valuable art objects, rare books, historic documents, and the like. When such items are stolen they are usually held for ransom or sold to dishonest private collectors for their exclusive viewing.

Within each category a degree of criminal risk exists. To determine the extent of this risk it becomes necessary to evaluate the loss potential based upon a number of considerations.

First among these is the degree of perceived risk. Perceived risk simply stated involves the owner or person(s) responsible for the property and his perception as to risk of loss or theft. Often, however, the owner's perception of risk is not based upon an objective assessment of all the factors. In most cases the potential for loss is over or underestimated depending upon the circumstances and experiences of the owner or responsible individual. Since one objective of crime prevention is a heightened

sense of safety and well being, however, the owner's opinions cannot be overlooked. Conversely, the owner of the property may be more aware of the risks than others attempting an assessment of loss potential. This is especially true where the property involved falls within the second and third category (research papers, art objects, etc.). The owner may, for example, be aware of the market potential for the items once stolen.

A second consideration in evaluating risk or loss potential is the probability of apprehension. Risk of theft increases as the risk of detection and apprehension decreases. In this context, the probability of detection and subsequent apprehension is directly related to the level or amount of security, either mechanical (real) or psychological (perceived) existing at the time of evaluation. Thus, we may assume, for the most part, increased security will engender less risk.

Offsetting this balance, however, is the next consideration, the value of the target to the criminal. Property categories and the definition of values have already been discussed. Various types of property possess different value characteristics depending primarily upon the motives or needs of the criminal contemplating theft or in some cases, destruction. Generally, however, it can be assumed that the risk of loss increases as the value of the target increase. To determine this value, one should place himself in the shoes of the criminal. Are the items in demand? Is there a readily available market for the property? And what monetary consideration can be expected? These are a few of the questions that should be answered before proper evaluation of risk potential can be determined.

To a great degree, the environment wherein the risk situation is located also has a discernable effect upon the evaluation of loss potential. The criminal climate, population, income and housing of the local non-university populace are, among others, those environmental factors which influence risk. Sound risk management principles dictate, more simply that buildings should not be constructed in areas experiencing an elevated degree of criminal activity. In a university environment, however, structures must be errected contiguous to existing facilities. Thus, the selection of their location is dependent upon the availability of suitable land within the campus bourdries. The degree of criminal risk can seldom be considered as a yardstick for measuring the suitability of a building site.

When considering security measures, the existance and degree of risk is the major determining factor in the selection, installation, and amount of security hardware and procedural controls. Because of its stated importance, it is necessary to determine the physical location of areas wherein this risk is greatest and to design a security "system" that is suited to the risks involved.

Once these risks have been defined the cost of the protection applied must also be considered. This factor is almost always involved, since few institutional organizations can afford to provide a "blank check" for security. Cost of security should not be confused with cost effectiveness. The former can be defined in strict monetary terms only or, more specifically, the availability of funds to accomplish the security objective. Cost effectiveness, on the other hand, concerns itself with striking the proper balance between the cost of security and the potential for loss.

To exemplify this notion, consider that a particular small department involved in teaching foreign languages receives a grant to purchase a large quantity of tape recording and video equipment costing $250,000. Upon inspection several security deficiencies are noted. This, coupled with the high risk nature of the equipment contained in the area leads the surveying officer to recommend a security system costing $2,500. However, the department's annual operating budget is a mere $20,000 from which all departmental expenses must be payed. While $2,500 expended for adequate security is indeed cost effective when weighed against the potential for loss of $250,000, the probability of freeing the necessary funds is remote. It therefore becomes necessary to adjust the security recommendations to fit the financial capabilities of the department. Another alternative may be to devise a list of security priorities based upon cost and degree of importance. This alternative, however, usually falls victim to the waining interest of the administrator responsible for the department.

When deciding the amount and type of protection necessary, the maintenance of the security system must also be considered. Complex systems result in complicated operating procedures, and an increased probability that the system will break down at some point. Again, a balance point must be determined; this time between the potential for loss and the complexity of the system designed. None-the-less, the security system must be designed such that its operation and maintenance are as simple and inexpensive as possible.

Finally, aesthetics, to some degree, must also be considered when designing security recommendations. Obviously, in extremely high risk areas appearances play a lesser role. Moreover, the condition, age and location of the building or areas, the nature of the operations, and the number of persons frequenting the area also determine the importance placed upon appearance.

If, for example, a high risk area were located in a remote corner of a building, attaching bars to the area's windows may be an acceptable method of protection. If this same area were located near the front lobby, another form of protection, such as burglary resistant glass, may be a better choice.

In summary then, it can be seen that defining a high risk area and designing a compatable security system is not a simple clear cut accomplishment. To design an effective system the officer must develop a methodology involving a mirad of interrelated internal and external considerations. The risk or the potential for loss must be assessed employing many factors in order to develop workable, cost effective security measures to remove or reduce the potential for loss.

III. Lines of Defense Theory

In order to effectively recognize and appraise crime risks, the practitioner must develop a systematic approach for evaluating facilities with a potential for loss. The "Lines of Defense Theory" has proven to be very effective for this purpose.

The first line of defense is the perimeter or exterior surroundings of a facility. Many times this is considered to be only perimeter barriers such as fencing, walls, thick hedgerows, etc. This should correctly include any perimeter barriers, landscaping, the position of the facility in relation to others, and psychological barriers such as walls of light, short parapet walls, etc. For example, recommending improvements in exterior lighting and not being able to see the facility because of a tall perimeter wall is not a cost effective security improvement.

The second line of defense is the building perimeter itself (walls, doors, windows). When evaluating the facility, officers should direct attention to door and window locations, hardware (locks, hinges, glazing, etc.), light levels, and the outline (shape) of the building perimeter itself. Ease of access, positions of concealment, and durability against criminal attack are all important considerations. The third line of defense is the identification and protection of specific risk areas within a facility. Officers should evaluate the potential for loss from specific rooms or groups of rooms or areas, and then consider physical protection methods such as door and window hardware, ceiling construction, and equipment locking devices. Operational security procedures such as inventory and key control, equipment identification, and lock-up responsibility are also important.

IV. Initiating Change

Once the officer has completed his evaluation of the building, the next step is to initiate change. The findings of a physical security survey should be prepared in a clear and concise manner. The officer may also wish to include some suggestions to improve the security of the facility. He/she should keep the concepts of

of good cost effective risk management in mind. Officers must remember academic institutions have limited budgets and changes must be possible within the budgetary restraints.

Officers will find many losses are attributable to ignorance or inability to understand sound operating procedures. Therefore, many security deficiencies can be corrected through education. This method usually has significant impact and should not be overlooked by the practitioner. Usually public education is accomplished by groups speaking or massive campaigns. Many times, however, one-on-one encounters are more productive than group audiences and should not be overlooked.

Finally, the practitioner must remember that he/she is not, nor could be expected to keep abreast of the rapidly advancing field of loss prevention. The crime prevention specialist is available to assist the officer in dealing with special problems he/she is likely to encounter. The specialist will handle situations much too time consuming for the practitioner. Communication, however, is imperative. The specialist and practitioner should maintain open lines to check progress in problem areas as well as the maintenance of attained levels of security.

PERIMETER ENTRANCE PROTECTION

I. INTRODUCTION

From a practical point of view, a building's perimeter represents the criminal's first real encounter witn barriers which physically retard attempts to enter. Often, he must resort to brute force or the use of a tool to affect entry. In the institutional situation, all too often such means are unnecessary... for the objective of entry might be more easily achieved simply by "trying" doors until one is located which requires little or no force to open, or a window may be found ajar.

A common retort to this problem would suggest that such entry methods are easily prevented simply by the adoption of a firm operational security policy. Employees should be educated in the correct methods of property protection, responsibility for security should be assigned and these individuals held accountable for breaches of security. This policy should be enforceable and authority to take action against rule violators should be mandated by the administration.

Most certainly,these idealistic and simplistic approaches are a part of a well rounded security program. However, such an undertaking is most difficult if not impossible to implement on a college campus.

This is due, in part, to the lack of a proprietary relationship between the individual and the institution of which he is a part. Often, this individual will insure the security of property for which he is directly accountable. His home will be locked, his vehicle will be secure and, in most instances, steps will be taken to insure the safety of his office and its contents (at least to the extent of his knowledge of security and his perception of the criminal risk). In these examples, the proprietary relationship is prevalent. Work and property are directly associated with the individual and its protection is paramount.

This same individual will seldom insure the doors to the building, of which his office or classroom is a part, are locked upon leaving. In most cases, this lack of attention to security is simply the result of forgetfulness; while in others, convenience, or the lack of it plays a major role.

Secondly, and perhaps most important, is the inability of the university administration to legitimately assign responsibility for security to any one individual. A given building,

for example, may house many departments or organizations; after hours access may be granted to a number of individuals normally assigned to other buildings (i.e., to use specialized auditoriums); graduate students may be allowed access to conduct research or oversee experiments; and other university departments must enter for purposes of building and equipment maintenance.

Thus, many must be allowed access to the building; assigning security accountability to one individual within the building would be unfair and extremely difficult to administrate. This is especially true when the scope of this individual's responsibility extends to areas common to a number of departments (such as those containing perimeter barriers).

It therefore becomes necessary to place emphasis upon those building and barrier design techniques which will reduce the need for reliance upon the individual by designing a system that is both intrinsically secure, and requires little human involvement to insure this security.

For the most part, this section deals with mechanical barriers as they apply to entrance security. In this context, recommendations are offered to deter attack on the structure by providing physical barriers through which the intruder must pass to affect entry. Though psychological barriers are not discussed specifically, the fact that mechanical barriers provide a psychological response cannot be overlooked.. It should be noted, however, that the degree to which psychological barriers are effective is largely dependent upon the relationship of the criminal's exposure time to the ability to be detected.

Thus, by installing a formidable locking device on a door the time of penetration increases. Increase exposure time through better lighting or locating the opening in an area of high visibility and the risk of apprehension increases until a point is reached where the intruder becomes discouraged.

The degree of skill possessed by the intruder also influences the time of barrier penetration. Obviously, the more sophisticated or complex lock and alarm systems become, more time is required for defeat; unless the intruder is knowledgeable in the methods of attack - in which case the time diminishes in proportion to the skill level possessed.

Another influence on exposure time (or risk of detection) is the value of the target or objective to the criminal. For the most part, the prime motivating factor can be expressed in terms of expected monetary profit.* Thus, it can be assumed,

---

*This is not true in all instances. Sexual gratification, extreme political beliefs, and personal agrandizement are, among many others, motivations not involving monetary gain.

some certainty, that the time allowed by the intruder for penetration of the barrier will increase as the value of the target becomes greater. For this reason, a greater degree of protection is required for areas containing items of higher value.

Figure 1 illustrates the effects these factors have on the probability of barrier penetration.

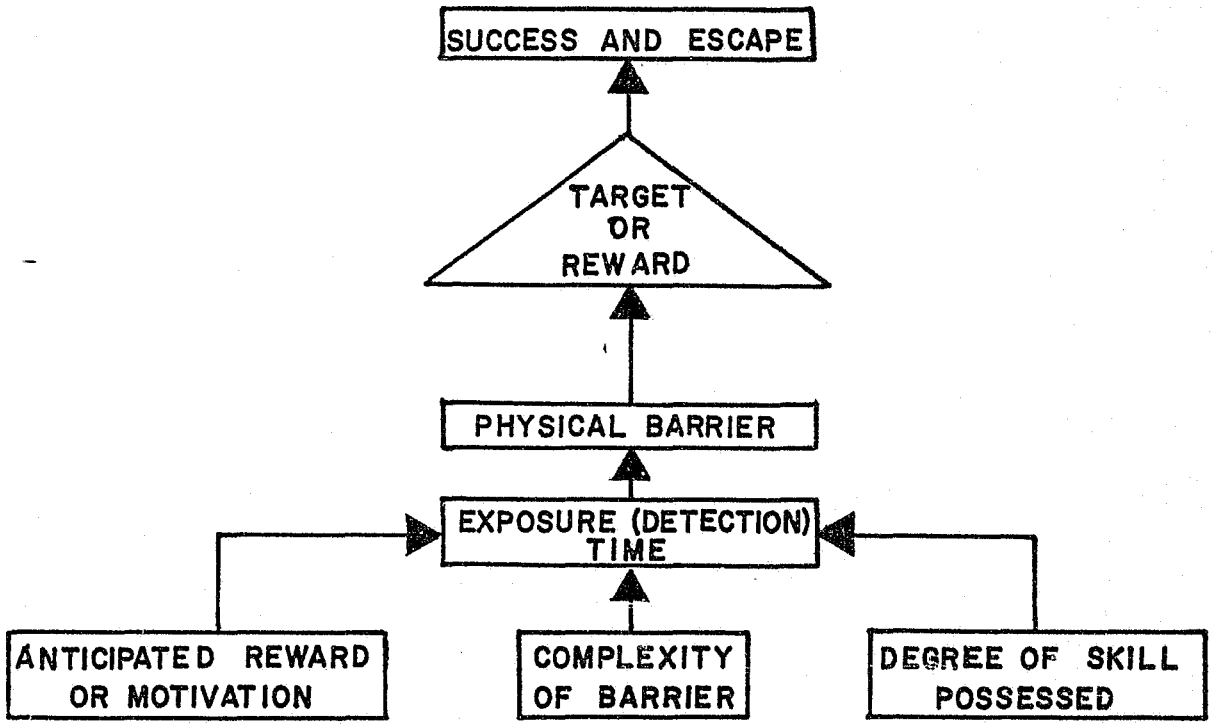


FIG.1

From the points noted above a number of assumptions regarding barrier penetration can be made and techniques of risk reduction can be developed from them:

1. Avoidance of detection and apprehension is usually uppermost in the mind of the criminal;

2. An increase in exposure time results from:

   a. enhanced barrier protection (difficulty of barrier penetration).

   b. an increase of skill required to penetrate the barriers.

c. an increase of barrier exposure.

3. If the anticipated rewards are great, the criminal will be willing to take greater risks. Thus, exposure time will be greater. It then becomes necessary to strengthen the barriers so that the risk of detection becomes greater.

4. Anticipated rewards also influence the degree of skill required to overcome the barrier. Added protection should thus be afforded to items of high value.

In the following sections, this concept is applied primarily in terms of asset protection. It should be noted, however, that many of the recommendations apply equally as well in the area of personal safety.

II. SCOPE OF THE PROBLEM

By far, the most common point of burglarious entry is the facilities' perimeter doors. Virtually all available findings indicate this fact both in residential and commercial buildings. A 1973 publication, Patterns of Burglary, noted that of all burglaries studied during the three year period, doors were the point of entry in over 56 percent of the cases (average for period). That same year the California Crime Specific Program indicated that the point of entry most preferred by the burglar was the door in 59.6 percent of the residential, 57.7 percent of the commercial/industrial, and 50.9 percent of the public (schools, churches, etc.) facilities.

Because burglars (as well as other types of criminals) seem to prefer doors as their major point of entry, common sense dictates that such points should receive a high priority when determining security needs.

In most burglary attempts, the success or failure of the attack depends upon the weaknesses or strengths of a number of components associated with the particular opening. One attack may center on the lock or its parts; while in another, the frame is forceably spread to allow passage of the locking bolt. In another instance, entry may be accomplished simply by breaking a window and stepping through the opening.

Thus, a door allowing entry into the facility cannot be considered simply in terms of its locking hardware. From this then, arises the notion of "door systems or assemblies" which

can be defined as "a unit composed of a group of parts or components making up a closure for a passageway through a wall."

When a layman thinks of security, his first consideration usually involves the strength of the lock applied to the door. While this is obviously an important consideration, other door parts require equal attention. The door itself, its frame, hinges, contact devices, anchoring methods and even the area or wall surrounding the door are (among others) interrelated and subject to attack. Only one need fail to provide the burglar with initial entry into the facility.

Another popular misconception is the notion that secure doors are unsightly in appearance. Historically, security meant massive locks, steel bars, or extremely cumbersome doors and frames. Today, however, the demand for improved security has given rise to a mirid of door hardware that is both secure and, at the same time, attractively designed to accomplish the architect's artistic and utilitarian objectives.

The selection of such devices should be predicated upon at least five considerations:

1. The door components should be intrinsically secure to resist or deter acts of burglary and vandalism;

2. The components should be designed such that, when installed, the intruder is substantially delayed before entry is accomplished; thus, increasing the probability of detection and apprehension;

3. A successful or attempted entry into a facility should be indicated at the point of entry by physical damage to the door or its parts. This is necessary to pinpoint the location of initial entry so that security may be improved when repairs are made, to establish the crime of burglary, rather than simple theft and to locate a productive source of physical evidence;

4. All components, especially those which affect security should be of the highest quality to insure proper operation at all times. Of primary concern are door closures, locking bolts, strike units, and other components which allow the door to close and relock.

5. Doors and associated components should blend aesthetically with the structure and the surrounding environment.

With these criterion in mind, the following suggestions for improved security of door components are presented.

III. GENERAL CONSIDERATIONS - DOOR ASSEMBLIES

A. All perimeter door frames should be constructed of 14 gauge steel or heavy gauge aluminum. When installed this frame should be completely filled or grouted with concrete on both sides.

This recommendation is made to increase the door frame's resistance to jamb peeling or spreading to allow passage of the lock bolt or defeat of any deadlatching mechanisms that might be employed.

Both sides of the frame should receive this treatment as pressure applied between the lock side of the frame and the door will be transmitted through the door to the hinge side.

If for some reason frames cannot be properly filled, additional support is necessary at the hinge and strike locations. This may be accomplished by welding 1/4 inch stiffners edgewise in these areas so that outward force is distributed to the masonry walls.

B. All exteriorly exposed butt hinges should be of the non-removable pin type (NRP).

C. All door windows and/or side lites should be glazed with burglary resistant glass or polycarbonate material. Special attention should be afforded to those windows 40 inches or less from a door opening device (i.e., panic bar, thumb turn, etc.).

In terms of burglary resistive glazing, several products exist which provide excellent protective qualities to the window opening.

Perhaps the most widely used material is polycarbonate sheet. Similar in appearance to acrylic and available in a wide variety of colors, this material is virtually indestructible, resisting repeated blows with baseball bats, sledge hammers, and thrown missiles. Additionally, because of its indestructibility and light weight, polycarbonate is not as susceptable to breakage during shipping and handling.

The material has some disadvantages, however. In addition to cost, polycarbonate sheet, even with the "mar resistant"

film is more susceptable to scratching than glass and special care must be exercised during installation to insure adequate allowance for expansion and contraction. Despite these drawbacks, however, polycarbonate is an excellent choice in windows not subject to a great degree of handling. The mar resistant material chould be installed in moderately high use areas. Though this material is substantially more resistant to scratching than its regular counterpart, abrasions could occur in high use areas resulting in decreased light transmission and optical clearity. For these areas or where the appearance of glass is desired, a second type of glazing material, burglary resistant glass, should be used. "B R" glass consists of two or more plies of glass with a layer of transparent plastic sandwiched between. While the outer layers will fracture when impacted, the inner plastic material will remain to resist penetration. BR glass possesses all the characteristic appearance of standard plate or float glass. In addition, it is not susceptible to abrasion through normal use and cleaning which makes it ideally suited to high traffic areas. Among its disadvantages are cost (though somewhat less than polycarbonate) and need for replacement should the material ever become broken.

Both the burglary resistive glass and polycarbonate material provide excellent security for windowed doors, while maintaining aesthetic appearances. Bars, protective grill work and the like also afford protection, and in limited application may even be employed to enhance appearances of certain structures. Such protective measures may also be applied inexpensively to door windows in obscure, secluded areas where appearances are less important.

For the most part, however, bars and other such methods of securing windows are unthinkable in an university environment, creating a "prison-like" appearance totally unacceptable to the academic community.

Burglary resistive glass or polycarbonate is usually the best choice for secure door window glazing. Other less expensive material may be developed in the future. However, before any of these products are considered, architects should insure that the material is rated "Burglary Resistive" as set forth by Underwriters Laboratories, Standards for Safety, Burglary Resistant Glazing Material, UL 972.

D. At no time should the latch bolt be visible between the lock stile of the door and the frame.

Such a condition is conducive to prying attempts, most of which are successful, since the deadlatching mechanism is

seldom reliable or sturdy enough to resist the simple force of a screwdriver. A more common attack method involves a prying force applied between the door and frame separating the two enough to allow passage of the latchbolt or defeat of the deadlatch (sometimes referred to as "anti-shim device"). Such methods are extremely effective where multiple door sets are employed since the prying force is transmitted from one door to another. The normal clearance between all doors is reduced allowing the clearance between the door and frame of the door under attack to become greater.

When the clearance expands to a certain point a small screwdriver, coat hanger or other instruments can then be inserted to depress the latchbolt and open the door.

If, for some reason the latchbolt exposure is necessary, the space between the door and frame should be covered with a "tee" extrusion, 1/8" steel strip, or applied bolt protectors.

E. Lock cylinders should be protected against attempts to pull or wrench cylinders from their mounted position.

Reasonable protection should be afforded to lock cylinders to prevent removal of the entire unit. Such protection is necessary to prevent a single intrusion into the facility or multiple intrusions carried out by individuals who have managed to decode the master combination and cut their own grand master key.

Protection of lock cylinders is accomplished by equipping the cylinders with hardened free spinning tapered guards, recessing into the frame, or by applying special steel covers over the cylinders.

At least one manufacturer offers a complete door assembly equipped with a special pull handle which encloses the cylinder. If this product is selected additional cylinder protection is unnecessary.

F. No exterior doors should be equipped with cylindrical (key-in-knob) lock sets.

Experience has shown that this type of locking hardware is easily compromised. Instead mortise locks should be installed. Moreover, cylindrical locksets are usually equipped with latch bolts with deadlatching features. On perimeter entrances opening outward this would necessitate exposing the latchbolt between the frame and door edge.

IV. MULTIPLE DOOR SETS - CRASH BAR EQUIPPED

A. All multiple door sets should be equipped with center mullions or mounted singularly or in such a manner or with such locking equipment as to prevent the use of coat hangers or other devices to pull the crash bar and open the door.

Several methods are available to prevent this type of attack: Center mullions of the movable or fixed type may be installed to cover the space between the meeting edges of the two doors; special panic hardware equipped with crash bars or paddles which open the door only when interior force is applied directly forward as opposed to downward; or a door assembly constructed especially to prevent this type of attack may be installed. Whatever the method used, it is only necessary that the panic device not be activated from the exterior.

B. All multiple panic door sets should be secured with concealed or rim vertical rod panic devices.

This is one of the most effective methods of securing panic doors. When installed and undogged, two bolts secure the door at both the head and sill or threshold. This locking method is extremely resistant to attempts at prying and should be employed wherever panic devices are installed.

V. SINGLE DOOR SETS - CRASH BAR EQUIPPED

A. All crash-bar equipped single doors should be secured to the door frame with concealed or rim vertical lock bolt devices.

Mortise locking hardware using a single latchbolt and strike should be avoided as the space between the door and frame is conducive to successful prying attempts. If, for some reason, a single latchbolt device must be used, a rim type panic device is preferred because the locking bolt is not exposed and thereby less susceptible to prying.

Single latch bolt panic devices are less secure than the concealed or rim vertical rod type, and are, therefore, only recommended in applications where electronic control of locking and unlocking mandates their use or in single door applications where both the hinge and lock sides of the frame are solidly filled with concrete. In both cases, the bolt should be protected from prying attempts by a extruded tee or some other bolt guard device.

Single latchbolt devices should not be employed in conjunction with movable or fixed center mullions as mullions tend to give slightly when placed under inordinate lateral load allowing the door to be jerked open.

VI. SINGLE DOORS - NON PANIC

A. Single doors not designated as fire exits should be equipped with double cylinder deadbolt locking devices of the rim, mortise, or tubular type. Projection of the bolt should be a minimum of one inch and the bolt, if exposed between the frame and door should be protected by armored strike reinforcement and extruded tee, steel strip, or bolt guards.

Doors classified as non-panic are those which are not mandated by fire codes to serve as fire or emergency exits. Most often such doors function as service or loading dock doors and are therefore easier to secure. Because these doors are usually located in more secluded sections of the building they are often used by dishonest employees to secretly remove items from the building to nearby vehicles or trash recepticles. (In the latter method, the employee returns later to remove the merchandise.)

Burglars also prefer these secluded entrances to those more visible and highly used. Often poorly lighted and visually obscured, such doors may be penetrated quite easily by the intruder because the possibility or fear of detection is substantially reduced.

Service or loading dock doors are also a convenient means of removing bulky or a quantity of items from the building to an awaiting vehicle.

For these reasons non-panic service-type doors should receive protection to prevent their opening from both the interior and exterior.

VII. DOUBLE DOOR - NON PANIC

A. Double door non-panic or service entrances should be double cylinder deadbolt equipped as noted above (VI-A). Flush bolt latching levers securing the inactive leaf should be located along the meeting edge of the door.

For reasons mentioned previously, double door service entrances should be protected from both sides. In addition

to the double cylinder deadbolt locking devices, the inactive leaf should also be protected. In most instances, this is accomplished by the installation of flush bolts occasionally, a security deficiency results when the levers used to throw these bolts are located on the interior surface of the door. When this occurs the door may be opened even though the locking device is engaged. To prevent this the actuating levers should be located along the meeting edge of the inactive leaf. When installed in this manner, the active leaf when closed physically covers the levers making their operation impossible from either side of the door.

VIII. OVERHEAD DOORS

A. All overhead perimeter doors should be equipped with a provision for interior padlocking (in addition to the conventional locking device). Once locked the padlock should serve as a positive stop allowing the door to open no more than three inches (if at all).

A small chain should be attached to the lock to insure the device will not be misplaced.

Securing overhead doors is usually simply a matter of drilling a hole in the track slightly above one of the track rollers. A padlock is then inserted and the door is secured. Trackless doors (roll-type) may be secured with a conventional or modified hasp and staple arrangement.

BIBLIOGRAPHY

System Development Corp., Crime Specific, Burglary Prevention Handbook, Office of Criminal Justice Planning, State of California. May, 1974. p.56

U.S. Department of Justice, LEAA, NILE & CJ, Physical Security of Door Assemblies and Components, U.S. Government Printing Office, Washington. May, 1976. p.3

U.S. Department of Justice, LEAA, Patterns of Burglary, 2nd Ed., U.S. Government Printing Offiee. 1973. p.135

GLOSSARY OF LOCK TERMINOLOGY

Active Door: First operating door of a pair. Usually the door with the lock installed.

Anti-Friction Latch: A device incorporated into a latch bolt to reduce the closing pressure required.

Astragal: A molding to cover an opening between two meeting doors. Protects the latchbolt so it can't be slipped.

Backset: The distance from the edge of the door to the center of the lock.

Bolt: The part of the lock which is moved into the locked or unlocked position, mechanically or electrically.

Change Key: A key for operating a specific lock or a group of locks having the same planned bitting. (Lowest level master key).

Cuts: The indentation made in a key to make it fit the tumblers of a lock.

Cylinder Guard: A device used to protect the cylinder of a lock. So the cylinder cannot be wrenched from the door.

Cylinder Housing: The external case of a lock cylinder. (shell)

Cylinder Core: The tumbler section of cylinder.

Cylindrical Lock: A lockset with the cylinder in the knob. Lock-in-knob.

Dead Locking Latch: A latch, when in a closed position resists the latch from being retracted by pressure being applied to it. (Also called a springbolt with an anti-shim device.)

Double Bitted Key: A key having cuts on two sides to activate the tumblers of a lock.

Escutcheon Plate: A plate, either protective or ornamental, containing openings for knob, handle, cylinder and keyhold.

Face Plate: The part of a mortise lock through which the bolt protrudes.

Grand Master Key: A key designed to operate all locks under several master keys in a system.

Heel of a Padlock: The end of the shackle on a padlock which is not removable from the case.

Jimmy Resistant: Lock type that has a vertical bolt to resist prying the door away from the jamb to bypass the bolt.

Key Way: The longitudinal cut in the cylinder plug.

Laminated Padlock: The body of a padlock consists of a number of plates.

Lip of Strike: The projecting part of a strike plate which guides the spring bolt to the latch point.

Lock: A lock is a device for fastening, joining or engaging two or more objects, and in a locked or fastened condition limits, and in an unlocked condition permits, relative movement or separation of the objects, and includes a means to operate the device into the locked or unlocked position.

Locking Dog of a Padlock: The part of the padlock that engages the shackle and holds it in the locked position.

Lock Picking: The process of operating a lock by means other than the specifically planned key.

Master Key: (See Grand Master)

Mortise: A cavity made to receive a lock or other hardware.

Mortise Cylinder: The pin or disc tumbler type used with mortise lock.

Mortise Lock: A lock with a bolt made for installing in a hole cut in the edge of the door.

Mushroom Tumbler: A special tumbler used to resist picking.

Padlock: A detachable and portable lock with a hinged or sliding shackle or bolt.

Panic Bolts: A horizontal bar inside a door that retracts the bolt in case of panic - used on fire doors.

Pin Tumblers: Round pins designed to fit the bitting on a key. Length varies to determine the combination of the cylinder.

Plug Cylinder: The round core of the lock that receives the key.

Rim Lock: A lock designed to be used on the surface of a door.

Rose: The part of the lock used as an ornament or bearing surface - normally placed against the surface of the door.

Shackle: The hinge or sliding portion of a padlock that does the fastening.

Shearline: The area between the housing and the plug, normally obstructed by tumblers.

Spring Bolt: It is a bolt which may be withdrawn by a knob inside and a key outside. When the door is closed the springbolt automatically retracts upon contact with the lip of the strike and then extends into the hole of the strike securing the door in a closed position.

Spring Bolt with an Anti Shim Device: Same as above, but has a small device normally adjacent to the spring bolt which, when the door is closed, prevents the spring bolt from being depressed or forced with a flat object. (Also called a dead locking latch)

Dead Bolt - Generally a rectangular bolt that is not spring operated but is moved by either the key or inside knob.

Strike: A metal plate installed on or in a door jamb, with one or more bolt holes into which the bolt of a lock or latch can be thrown.

Tail Piece: The unit on the cylinder of a lock which in effect, activates the lock.

Tension Wrench: An instrument used in picking locks - it applies tension to the cylinder plug while lining up the tumblers.

Throw: The outward movement of the bolt and the distance the bolt travels.

Tumbler: Any moveable or variable device in or attached to a lock upon which security against unauthorized entry depends.

INTRUSION DETECTION SYSTEMS

INTRODUCTION AND ORGANIZATION OF THE SYSTEM

I. INTRODUCTION

As police officers working toward the goal of crime prevention, we should exercise care when making recommendations concerning the installation of intrusion detection equipment, for such equipment is not a "panacia" for security; rather, it is only one element in a systems approach to prevention. Locks, lighting and public awareness are a few other elements involved in this approach to the reduction of crime.

Electronic protection is, however, a major factor in crime prevention and the reduction of risk. But, before we go any further, you must be satisfied in your own mind that such protection is not only usefull for purposes of apprehension of intruders, but it is also an excellent tool for the prevention of criminal incidents.

In a research paper on burglary prevention, Dean John C. Klotter noted that, "In those cities where burglary alarms were most evident, the burglary rate was without question lower."

More recently, the Burns Security Institute, a private research unit that studies and reports on crime related matters in the private and institutional areas, conducted a seminar on school security. During the proceedings, some rather startling statistics came to light;

- Prince George County, Maryland school system's recently installed intrusion detection system for 234 schools and ten administration buildings and warehouses, cut breaking and entering by more than one half and saved an estimated $178,000 in the first six months of operation;

- In Alexandria, Virginia, electronic protection systems have been credited with reducing lossess from theft and vandalism by 890 percent, from $178,000 to $20,000 per year.

Another study in Cedar Rapids, Iowa on installation, test and evaluation of a large scale burglary alarm system for a municipal police department also found that burglar alarms are effective. The study determined that if an alarm is present the chances of an arrest at the scene are five times as great even though the alarm may not have been activated. Additional findings noted that if clearances based on captures, confessions, or discovery of stolen goods is considered in all burglary cases, the clearance rate for locations with alarms was 46 percent and 27 percent for those without alarms. If there was no capture at the scene, there was no loss by theft in 63 percent of the locations with alarms, more than twice the 31 percent rate at locations without alarms.

As indicated by these statistics, alarm systems can and do play an important role in crime prevention. However, as mentioned previously, they are not the only tool through which this goal may be achieved. In fact, sometimes such systems may engender a false sense of security in the mind of the property owner, a condition which may well enhance the opportunity for a crime to occur.

A major problem with the deployment of electronic protection is the extremely high incidence of false alarms. But before we as police officers condemn alarm systems, let's look at some facts. From the police point of view any time we respond to a call and find neither burglars or robbers, nor any evidence of an attempted entry, the alarm is false. At first glance such an outlook seems to provide a straightforward enough definition; but there are still some problems. For example, the burglars may have been frightened off by the audible portion of an alarm or by the sudden arrival of police units prior to successful entry. In some instances burglars may have deliberately set off an alarm one or more times as a part of a plan for a later break-in or to decoy police away from the scene of an actual crime. While such occurrences are quite rare, they should be noted when considering the overall false alarm rate.

Often we hear of false alarm rates expressed in terms of an extremely high percentage. In fact, as presently computed, the national false alarm rate is somewhere around 97 percent. But if we look closer at the methods of computation, this percentage does not accurately reflect a true picture of the false alarm problem. The customary procedure is to compute the figure based upon the total numbers of system activations (alarms) versus the number of actual or attempted burglaries into an alarmed premise. Thus, if a particular jurisdiction responds to 100 alarm system activations of which 97 are false, the false alarm rate would be 97 percent.

No consideration is given to the number of systems in operation at the time. If we assume for example, that a small city has only 10 systems from which these 97 false alarms are generated, one can easily understand why such figures are not a true representation of the efficiency of the systems. Conversely, if a large city with 1000 systems recorded only 100 activations, 97 of which were false, the rate is still 97 percent, but with one unmentioned difference; there are 100 times as many systems as in the small community.

In a recent survey conducted by the Alarm Industry Committee for Combating Crime, it was determined that it required about 30,000 hours of police time to respond to the 38,898 alarms investigated by the committee. However, this expenditure of police time resulted in the capture of 634 criminals or one criminal for every 48 hours of response time spent by law enforcement officials. Extrapolation of these survey findings on a national basis would suggest that alarms were responsible for the apprehension of at least 10,000 criminals annually. Moreover, the conviction rates for all criminals thus apprehended was substantially higher than the conviction ratio for all criminals caught by police.

Alarm systems, the survey went on to say, for all their difficulties as far as false alarms are concerned, are one of the principle labor-saving and crime-preventing tools available to the police. Viewed in this perspective, the 48 hours of police time per criminal arrested turns out to be one of the best investments of police time available.

A certain amount of false alarms are acceptable if the system deters and aids in the apprehension of criminals. Fundamental to a reduction in false alarms is proper design of the system, the use of high quality components and proper installation and maintenance programs. Human error must also be reduced since it is the major cause of false alarms.

II. ORGANIZING AND DEFINING THE SYSTEM*

The historical use of geese as an intrusion detection system led Gordon Hasler, in his "Integrated Alarm Systems," to make physiological analogies to modern systems. The analogies resulted in a breakdown of the system into three fundamental parts. These simple analogies as applied to electrical or electronic systems were not dependent on the extent of security. These fundamental breakdowns were adopted and defined as follows:

A) SENSOR: That function of the intrusion detection system which detects or senses a condition that exists or changes, be it authorized or unauthorized. This definition can be related directly to the animal senses of touch, hearing, sight, smell and taste.

The above definition includes all actions that occur since the senses have no means of distinguishing authorized or unauthorized actions. This is easily pointed out in one of the most common and simplest sensory devices - the magnetic contact on a door. The device is activated each time the door is operated and has no means of determining whether the operation of the door is authorized. That function is assigned to the next fundamental part.

B) CONTROL: That function of the intrusion detection system which provides the power, receives the information from the sensors, evaluates the information and transmits the required information to the annunciation function.

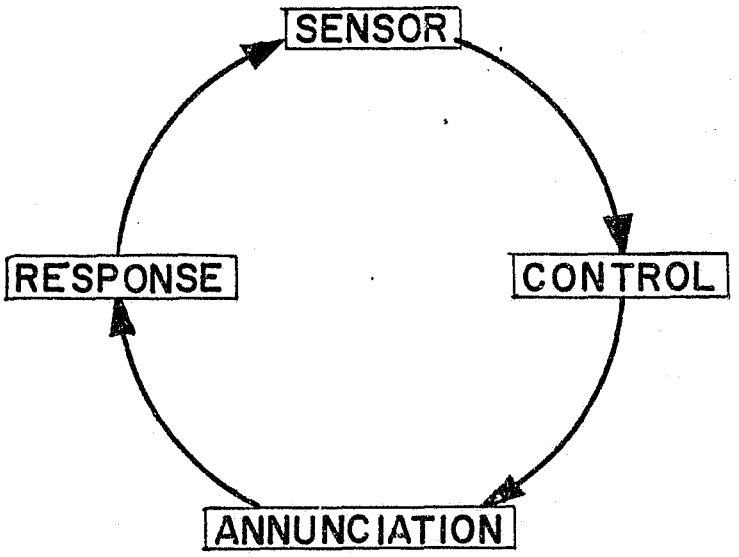
The annunciation function is related directly to the physiological functions of the brain and nervous system and also to the circulatory system. The nervous system collects and evaluates information from the various senses and transmits signals to the muscles for appropriate action. The circulatory system provides the power source (i.e., nutrients and oxygen from the blood) to maintain the ability of the system to function.

* Adapted from handout material developed by Carl Kellum, National Crime Prevention Institute.

C) ANNUNCIATION: That function of the intrusion detection system which alerts the human to initiate a response that will result in an investigation of the sensor environment.

This could be bell, buzzer, light flashing, etc. This function is analogous to the squawking of geese, the barking of dogs, or a man calling for help.

To complete a cyclic flow of information, the response to the alarm must be included. The nature of this response must be considered in designing a system. The cyclic flow of information may be illustrated as follows:



It is easy to demonstrate that a flaw in this flow at any point may prove to be a point of vulnerability to the criminal, so that not only the design of the three fundamental parts of the intrusion detection system must be equally strong, but the response must be adequate and appropriate.

To enable an individual to design the three fundamental parts with equal strength, each is broken down into functional elements.

REFERENCES

1. Burns Security Institute, A Panel Discussion on Campus Crime and Security, Burns Security Institute, Briarcliff Manor, New York. 1973.

2. Cedar Rapids, Iowa Police Department, Installation, Test and Evaluation of a Large Scale Burglar Alarm System for a Municipal Police Department, Final Report, National Technical Information Service, Springfield, Virginia. 1972.

3. Kellem, Carl, Lecture Outlines, Intrusion Detection Systems, National Crime Prevention Institute, Louisville, Kentucky.

4. National Burglar and Fire Alarm Association, "An Analysis of False Alarms," NBFAA Signal, Washington, D.C. (January 1974).

5. National Bureau of Standards, Terms and Definitions for Intrusion Alarm Systems, Law Enforcement Standards Program, National Institute of Law Enforcement and Criminal Justice, LEAA, U.S. Government Printing Office, Washington, D.C. (1974).

SENSORS

I. FUNCTIONAL ELEMENTS - GENERAL

Functional elements in the sensor may be considered from two approaches -- first, from their physiological relationships to the human senses; and secondly, from the application to the security needs. Both divisions are utilized in the instruction process, but in the design of a system, the applications are used as the functional elements.

In the adoption of the concept of DEFENSE IN DEPTH there are various established means of applying sensors starting at the high value targets and working out to the most remote points. By combining various concepts of what is considered to cover all possibilities in applying sensors, the following functional elements and definitions are used:

A. Point Protection - the application of sensory devices to the high value target (monetary or other) which can be the objective of an unauthorized intrusion.

B. Trap Protection - the application of sensory devices in the interior of a premises in a manner or location that will not normally be expected.

C. Space Protection - the application of sensory devices in the interior of a premises which detect the presence of an individual within a defined volume - whether COMPLETE or PARTIAL - of the premises.

D. Perimeter Protection - the application of the sensory devices, completely or partially enclosing the protected area within a shell which may be exterior to, interior to, or at the physical barriers that enclose the secured premises.

In viewing a premises with these functional elements in mind, a person may conceive a system by identifying the high value targets (this enables him to establish one of the primary considerations of crime risk management -- the probable maximum loss). He then may determine the depth of defense necessaryrfor each individual premises, selecting the most applicable elements of the sensors. The highest risks would demand all elements, whereas lesser risks could be adequately protected with partial perimeter.

II. TYPES OF SENSORS

After the applicable functional elements are decided upon, various devices must be selected to fill each function. The understanding of the capabilities and limitations of all sensory devices will enable the selection of those that will best be suited for each individual premises considering risk management principles.

The sensor devices available are grouped with analogies to the human senses with the intention of simplifying the selection of devices to fill functional elements. If the need exists for devices to fulfill the perimeter function for a particular premise, is it best to "look" at the perimeter with a photoelectric device in front of a series of doors or "feel" the position of each door with an electromechanical device? These analogies are made as follows:

A. Sense of Touch or Feeling

This analogy is developed to cover more common electromechanical devices and a few electronic devices that function by breaking a conductor, moving an object, vibrating, applying pressure and sensing temperature.

1. Foil Tape - A high lead content tape which is stretched and attached to a surface (usually a window) and protected with a coat of varnish. A small electrical current is passed through the tape and if broken or fractured, the electrical current ceases causing the alarm. Foil tape, when customarily applied as perimeter protection to windows, serves as a visible deterrant.

   Installation in terms of labor alone is time consuming and expensive. Maintenance is also a problem, especially on doors or windows handled frequently.

2. Open Wiring or Lacing - Employs the same principle as foil except that wire made of semi-brittle copper is used instead of tape. Such wire is simply attached to the protected surface. Breaking the wire causes the alarm. Seldom used in visible locations because of unsightly appearances. Most often used to protect walls and ceilings from penetration.

3. Grooved Stripping - Same principle as open wiring except that the wire is encased in grooved wood

strips and dowels. The entire assembly, similar in appearance to jail bars, is then attached to a surface (usually a window or door). If any of the dowels are broken an alarm condition results. Can be wired so that defeat is most difficult. Good protection for skylight windows and walls, but limited in uses because of unsightly appearance and extreme cost.

4. Alarm Screens - An insulated wire is incorporated into a material resembling common fly screen. The screen is mounted in an aluminum frame and attached to the protected opening. Provides reasonable security if properly wired. Relatively expensive. Used in openings (primarily windows) where ventilation is required. May be equipped with magnetic reed switch to further protect against complete removal.

5. Wire Traps or Trap Clips - A wire, permanently mounted at one end, is stretched across an area. To the other end a clip or "spoon" is attached and inserted into a receiver. Removing the spoon causes the alarm.

   a. live traps - current flows through the trap wire. More secure because wire cannot be cut to defeat the device.

   b. dead trap - no current flows through the trap wire or the wire is replace by a string.

   Inexpensive form of trap protection. Best used on stairs or in hallways. May also be used to protect doors or windows in unique applications. May be easily defeated simply by stepping over trap wire. Must be set by subscriber each day and may therefore be undesirable except in locations not requiring daily settings (i.e., staircases leading to roof access or to protect removable ceiling panels). Should be installed in unlighted areas.

6. Plunger Contacts - Springloaded pushbutton switch similar in appearance to those found on car or refrigerator doors. Commonly employed to protect bell housings, control cabinets, and other alarm equipment against tampering by unauthorized persons. Often mounted in door frames to signal opening.

May also be used to protect casement windows or objects from being lifted. Undesirable in high use areas because of mechanical failure and contact oxidation. Other forms of switches preferable except in tamper applications.

7. Mercury Contact - Consist of a small glass tube containing small amounts of mercury. Electrical contacts are contained in and at one end of the tube. The device is attached to windows or other openings hinged at top or bottom and is designed to detect the tilting action occurring when the window is opened.

   Excellent protection for hatch doors to roofs, some overhead doors and other top or bottom hinged openings where magnetic contacts cannot be used.

   May be adjusted too sensitive such that the mercury reacts to vibrations such as thunder or passing trains (false alarms).

8. Magnetic Contact - Most common, most preferable method of movable opening protection. Commonly consist of two parts; a magnet mounted on the movable part of the opening and a switch installed on the jamb or frame. As the magnet is brought in close proximity to the switch (door closed) the contacts react. Removing the magnetic influence (door open) sounds the alarm.

   A multitude of various switching configurations, styles, and sizes are available for most applications. Also available are devices which can be completely or partially concealed in the door and its frame. For high security applications a "balanced magnetic contact" may be used. This device reacts (sets) only when the exact amount of magnetic influence is introduced. Any more, any less, or influence introduced from any other direction will trigger the alarm.

   Another form of higher security magnetic contact employs two magnets, one in the switch section; the other mounted in the movable part of the opening, at opposing polarity. The repelling action of the two magnets causes the contacts to close. Both the balanced and repelling magnetic switches are difficult to defeat by introducing extraneous magnetism.

Most other types of magnetic contacts are easily defeated if the wire terminals are accessible simply by attaching a jumper wire. A substitute magnet may also be used.

9. Vibration Contact - Two types, both designed to detect vibration.

   a. mechanical - responds indiscriminately to vibrations. Utilizes a contact with a tensioned spring holding it against another contact. Shocks or vibrations cause momentary breaking of the contacts causing the alarm condition. Highly susceptible to false alarms if adjusted incorrectly or mounted on resonate surfaces (i.e., drywall).

      Inexpensive protection for block or concrete walls or heavy safes where extraneous vibration is not a problem.

   b. crystal or frequency controlled - utilizes crystals oscillating "tuning fork" or other electronic circuitry designed to respond to a specific range of frequencies.

      Less susceptible to vibrations from low frequency sources such as thunder, passing trucks, etc. Used primarily as a method of protecting glass surfaces.

10. Weight Activated Devices - Consists of a number of types of devices, all designed to detect pressure or weight among which are the following:

   a. mat switch - a sensory device employing two pieces of conductive material separated by an insulator. Sufficient weight placed upon the mat causes the conductors to touch, initiating the alarm. May be obtained in quantity and cut to any length. Reasonably good protection. Should be concealed under carpet. Well suited for halls, aisles and stair steps. May also be used on floors in front of windows or doors to protect against perimeter entry. Should not be used in high traffic areas (unless specially designed), on wet floors, or in areas where corrosive or other types of destructive chemicals are stored or used.

When installed the mat should be of sufficient length or installed in such a manner as to prevent the intruder from jumping over or maneuvering around it. May be used to detect lifting of an object.

b. stress sensor - an adaptation of the strain gauge. Sensors attached to any building member subject to minute flexing whenever pressure is applied or removed (i.e., floor joists). Usually consists of a control unit and a number of small sensing elements.

Early models susceptible to false alarms caused by settling of the building. Latest models incorporate circuitry designed to initiate the alarm only when the pressure is applied or removed within a short preset period of time.

Relatively expensive when compared to other forms of protection. Environmental conditions may limit use in certain areas.

c. buried line intrusion detection or seismic sensor - a sophisticated, extremely expensive type of detection system primarily for outdoor perimeter applications. One type detects pressure differential between two lines buried in the ground as the intruder approaches. Another type employs pressure sensors spaced at intervals along a single line.

This type of device, because of expense, is limited to extremely high risk areas such as nuclear and government installations.

d. fence detection system - a device employing small sensors spaced at intervals along a perimeter fence. A tension wire is attached to the fence and sensor and when pressure is removed from or applied to the fence (climbing) the alarm is initiated.

Some types extremely sensitive and producers of false alarms caused by wind or other environmental conditions. Relatively inexpensive when compared with other forms of fence protection.

11. Heat Sensors - A device designed to detect a change in ambient temperature. May be constructed of a fusable link (when temperature reaches a certain point, the link melts causing the alarm) or an expanding metal alloy. The alloy type may be a fixed temperature device (as the fusable link type) or a rate of rise device, or a combination. The rate of rise function detects a change in ambient temperature when such change occurs within a preset time interval.

    While the heat sensor is primarily used in fire detection systems, it may be employed in burglary protection systems to detect torches or burning bar attacks on safes and vaults.

B. Sense of Smell

This analogy is developed to cover those devices that sense ionized particles, or products of combustion. Like the heat sensors, these devices are used primarily in fire systems, but find limited uses in safe and vault protection.

1. Ionization or Product of Combustion Detectors - a smoke detector employing minute quantities of radioactive material which ionizes the air in a sensing chamber, thus rendering it conductive and permitting a current to flow through the air between two charged electrodes. When smoke particles enter the ionized area, they decrease the conductance of the air. When the conductance is less than a predetermined level, the detector circuit responds.

2. Photo-Electric Detectors - A type of smoke detector employing a sensitive photo cell and light source. Smoke entering a chamber reduces the level of light received by the photocell from the light source initiating the alarm. Another type uses the same components but the photocell and light source are separated by a boffet. Smoke entering the chamber reflects the light into the photocell initiating the alarm.

C. Sense of Hearing

This analogy is developed to cover those devices which use airborne sound in its sensing medium. This includes

devices that transmit sound and listen for reflected sound or those that just receive the sound.

1. Sound Monitoring - Uses microphones to passively listen-in to the protected area. When an intrusion occurs, an alarm is received at the remote receiving station. The central station operator then increases the volume on the monitoring receiver allowing him to listen to the remote protected area. Excellent method of protection when used in conjunction with other conventional sensors. False alarms reduced due to listen-in feature.

   Audio output may (and should) be channeled into a recorder for later use in court.

   Large area of coverage. May be attached to existing building P.A. system to reduce installation cost.

2. Sound Sensing Detection System - Detects audible sound caused by an attempted forcible entry into a protected structure. Consists of microphones and a control unit containing, in addition to other electronics, an accumulator which sums the amplitude of a series of noise pulses. Noises above a preset level or a sufficient accumulation of impulses will initiate the alarm.

   Adjustments and installation methods and locations are critical. May generate false alarms from environmental noises (noisy steam pipes, running water, thunder, passing vehicles). However, such noise sources may be eliminated by placement of special noise canceling microphones near noise sources.

   May use existing building P.A. system.

3. Sonic Motion Detection - Form of space detection sensor which detects the motion of an intruder by his disturbance of an audible sound pattern generated within the protected area. Operates on doppler principle (see ultrasonic). Frequency of sound waves lower, thus audible to persons outside protected area. Manufacturer claims that this audible sound has preventive effect on person considering forced entry. Installation precautions similar to ultrasonic.

4. Ultrasonic - Consists of a transmitter, receiver, and processing electronics which may or may not be housed seperately. The transmitter emits ultrasonic sound energy (20 to 46,000 cycles, above human hearing range)

into the protected area. This energy is reflected from the various surfaces contained in the protected area back to the receiver. Enter an intruder and the received frequency differs from the established pattern (higher or lower) and the alarm is initiated.

Selection of mounting location is critical. Because sound energy is a movement of air, the ultrasonic device should not be located near sources of strong air drafts (i.e., fans, cold air returns, heat vents, etc.). Hissing sound such as steam leaks, should also be avoided as these are likely sources of ultrasonic energy which may trigger false alarms.

More modern devices are equipped with circuitry to minimize problems caused from these noise sources.

Radio frequency interference will seldom cause false triggering unless the units are improperly shielded.

Occasionally environmental noise such as telephones, buzzers, etc. may cause false alarms depending upon the frequency of the noise producer, locations of sensors, etc.

Relatively large moving objects (object size and its effect upon the sensor is largely dependant upon the proximity of the object to the sensor) such as hanging signs and displays extremely loose fitting and large overhead doors, etc. may also become a problem.

D. Sense of Sight

This analogy is developed to cover sensors using electromagnetic radiation regardless of frequency. This includes all photoelectric, microwave, electrical field, and magnetic field devices.

Just as the human ear is limited in the range of sounds it can hear, human sight is even more limited. What the eye sees is only a small portion of the electromagnetic spectrum which includes radio waves, x-rays, and light.

1. Microwave - Except in outdoor perimeter systems, microwave sensors employ the same operating principle (doppler) as ultrasonic devices except that instead of high frequency sound, microwave units use transmitted radio frequency energy (12.5-40.5 Ghz).

Being radio waves, microwave energy will readily penetrate such building materials as wood, plastic, drywall, and glass.

Additionally, metal acts as an excellent reflector for microwaves. Care must be exercised to insure the energy is contained within the protected area or false alarms will result. Avoid mounting where energy will be reflected by metal objects out through a window or door.

Microwave devices protect a much larger area with a single unit than ultrasonic -- (up to 10 times more).

Florescent lights may trigger false alarms if mounted within approximately 10 ft. of sensor.

Devices using microwave energy are also available for outdoor perimeter applications. Such devices consist of a transmitter which projects microwave energy to a receiver located, in some cases, 1000 ft. away. The receiver then responds when the received energy is reduced to some specific point as occurs when an intruder approaches. More aptly called a "presence detector". Best used inside a perimeter fence.

2. Active Photo-Electric - Consists of a light beam transmitter and a photo-electric receiving element. A beam of light is transmitted across the protected area to the receiver. Breaking the beam causes the alarm. Light beam may be visible or invisible (infra-red) to the human eye. Latest devices employ infra-red beams which pulsate to prevent defeat by inserting substitute light source. Available in ranges from 15 to several thousand feet depending upon the manufacturer. May be stacked to provide a beam "fence" making it most difficult to jump over or crawl under.

   May use mirrors to turn corners for added coverage; however, for each mirror used, effective range is reduced by 25% and alignment becomes more difficult. Units must be mounted on ridged surfaces and in such a manner as to prevent their being bumped and thus misaligned.

   May be purchased with transmitter and receiver housed in one unit. Reflective disk(s) then placed on wall opposite unit and beam is reflected to receiver.

3. Passive Photo-Electric - Consists of primarily two types of devices both of which are "passive" in the senses that they transmit no form of energy. Rather, the device simply remains inactive (normal) until an outside energy source (human) appears.

   a. light intensity or ambient light detector - "looks" at the protected area in terms of the existing (ambient) light levels and establishes a reference point. As an intruder enters, these levels change. Once these changes exceed the reference point, an alarm is initiated.

      Should not be used in totally dark areas because detection will not occur unless intruder uses flashlights or turns on interior fixtures.

      False alarm problems may occur when outside light sources are introduced into protected area (i.e., lightning, vehicle headlights).

   b. passive infrared - sensitive to infrared energy radiated by the human body (any warm object radiates infrared energy due to molecular activity). Sensor looks at protected area in terms of ambient infrared energy. Intruder's presence changes the amount of energy received and an alarm is initiated.

      Passive IR sensors very stable; few false alarms. Expensive when compared to other devices with same coverage area. Most IR sonsors can protect a small area (25'x25'). At least one manufacturer offers an IR device with a detection zone of 4 ft. by 70 ft. Should not be aimed at sources of IR energy (i.e., radiators, heat ducts).

4. Active Infrared Intensity - Singularly housed device containing a transmitter and receiver (intensity device). A beam of pulsed infrared energy is projected into the protected area and the receiver "looks" at the beam. Should the reflected energy level change (as occurs when an intruder enters) an alarm is initiated.

5. Capacitance or Proximity - Wired to a metalic item requiring protection (i.e., safe, file cabinet). Item must be well insulated from the ground. Small alternating current is passed through protected item to generate a resonate or balanced condition. As the intruder approaches this balanced condition is upset

and the alarm is initiated.

A variation of this device is employed in outdoor perimeter applications. Instead of a metalic object, the device is connected to a single wire which surrounds the area to be protected.

Sometimes referred to as a "touch switch".

CONTROL FUNCTION

The elements of the control function are generally all required. The sophistication of the devices fulfilling each function determines the level of security attained.

I. CONSISTS OF THE FOLLOWING PARTS:

A. Power Source

B. Protective Circuitry

C. Energizing Technique

D. Signal Transmission

E. Annunciation Circuitry

II. POWER SOURCE

A. Defined

The power source is the functional element of the control function which provides the energy to operate the intrusion detection system.

B. Types of Power Sources (in order of increasing reliability)

1. Public Utility - 110 VAC or house current. Seldom reliable enough to operate the system by itself. Susceptible to power failures.

2. Primary Battery - System is powered solely by batteries which are used once and disgarded. While this power source is more reliable than public utility, batteries are subject to a "shelf life" which requires periodic battery changing. Additionally, if the system is activated more frequently, the life of the battery will diminish.

3. Secondary Battery - A type of storage battery that may be charged and discharged many times. Secondary batteries usually have no shelf life or the life may be

of such length as to render it inconsequential. Major drawback is that the secondary battery's charge may become too low to power the system after long periods of utilization.

4. Public Utility with Primary Battery - Power source employing batteries (usually dry cells) and public utility. When operating normally, the system is powered by the public utility. Should this source fail, the battery then takes over system operation. More reliable than first three power sources because the battery is not used until house current fails. However, battery is still subject to shelf life, and if both battery and public utility fail, system is inoperable.

5. Public Utility with Secondary Battery - Best method of powering system. Public Utility is employed to maintain a continuous charge on the secondary battery. The alarm system draws needed power from the charged battery. Should the public utility fail, the battery will continue to operate the system for several days. Once restored, the public utility will again recharge the battery.

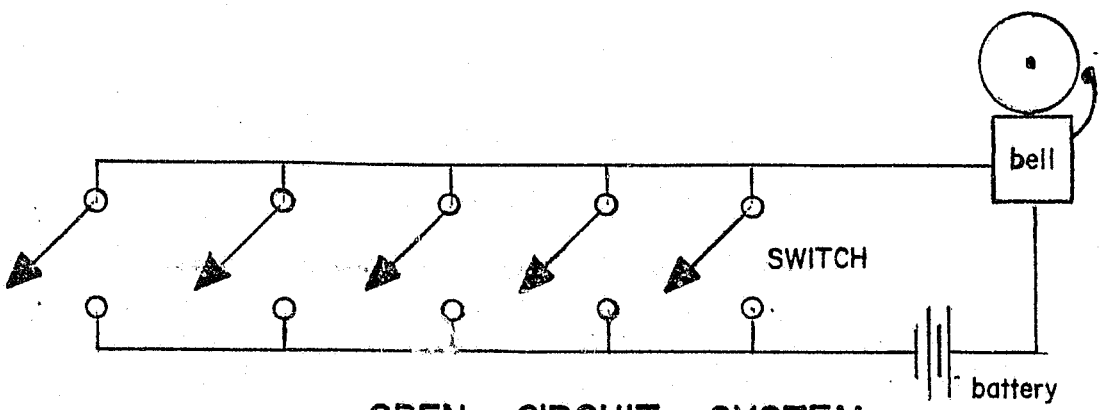
III. PROTECTIVE CIRCUIT

A. Defined

The means by which the "information" from the sensory devices is brought to a common point.

B. Three Basic Types of Protective Circuits (in order of increasing security)

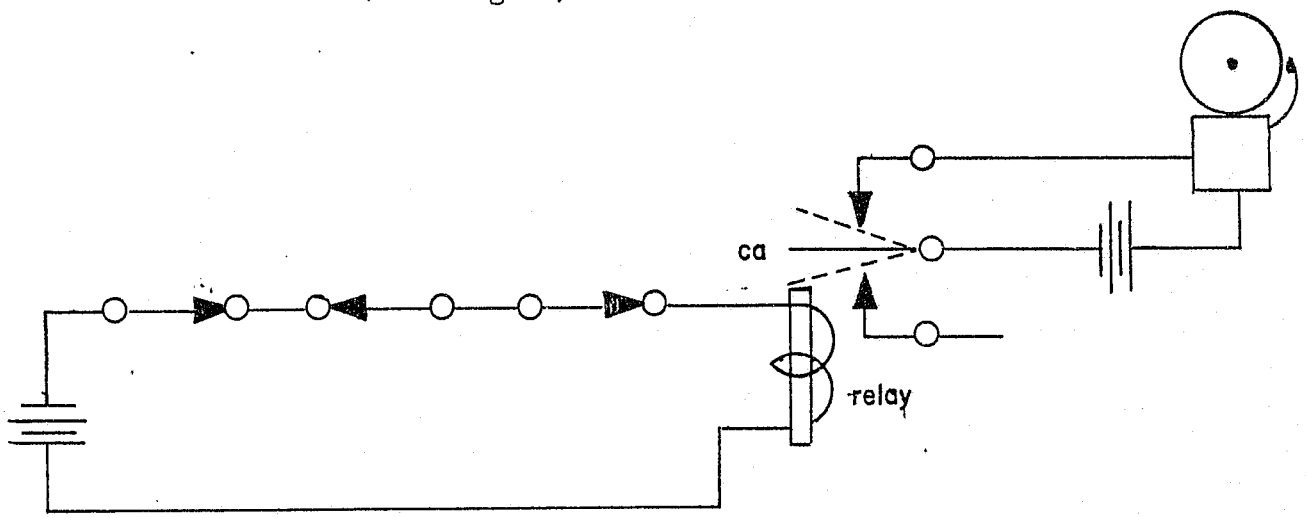
1. Open Circuit - A type of protective circuit wherein the alarm sounds when the switch (sensor) is closed. Switches in an open circuit system are wired in parallel (see diagram).



OPEN CIRCUIT SYSTEM

Easily defeated by cutting the wire at any point. Not suitable for most alarm applications.

2. Closed Circuit - Type of protective circuit utilizing a constant flow of electrical energy. Break the flow, and the alarm sounds. Uses series switching technique (see diagram).

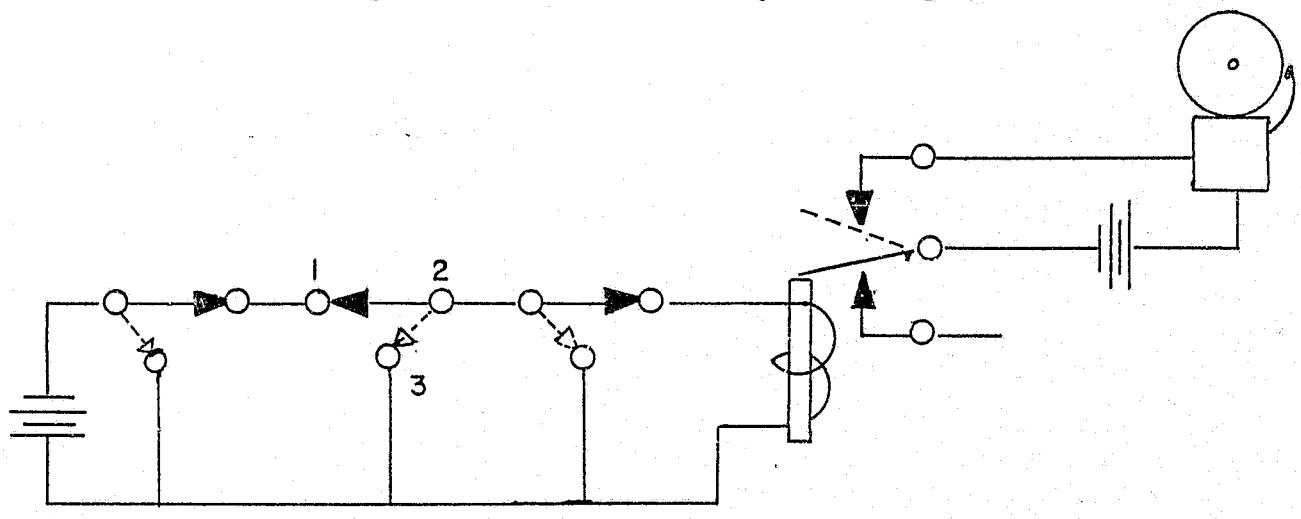


CLOSED CIRCUIT SYSTEM

In the above diagram, the relay contact arm (ca) is held down. Should one of the switches open, the contact arm will spring up and energize the bell.

More difficult to defeat than open circuit technique. Jumper wires must be used.

3. Combination Open and Closed Circuit - Type of circuit wherein both features of open and closed circuits are utilized. Uses series/parallel switching to achieve optimum levels of security (see diagram).



COMBINATION OPEN / CLOSED CIRCUIT SYSTEM

Most difficult type of circuitry to defeat. Requires that one side of the switch be jumped and the other broken.

In the diagram above, if only a jumper wire were attached at points one and two, the sensor would still not be defeated. As the switch opens the contactor will make contact at point three causing a dead short which de-energizes the relay causing the alarm.

C. Protective Circuit Transmission Technique

There are several types of techniques used to transmit the protective circuit information. Among them are the following:

1. Hardwire - Each of the sensors is physically attached to a wire. The wire is then connected to the control panel. Most reliable. Most secure because if circuit fails, alarm will sound (supervision).

2. Non-Wire - Three types.

   a. line carrier - sensory devices connected to a transmitter and plugged into a 110 volt wall receptical. When activated a signal from the transmitter is superimposed on the existing electrical wiring. A remotely located receiver receives the signal and initiates the alarm.

      Transmitter and receiver must be operated by house current supplied by same electrical transformer.

      Operates on public utility only and is therefore less reliable. No supervision.

   b. FM-wireless - utilizes a small battery powered short range transmitter to broadcast a coded signal to the receiver located at the control where the alarm is initiated.

      Batteries may become discharged and the system will not function. Supervision limited.

   c. light - utilizes flashes of light (flash cubes) to signal the control when sensory devices are activated. No supervision. System will not function if door is closed between protected area and control.

IV. ENERGIZING TECHNIQUE

A. Defined

Those actions or procedures that must be performed to set the intrusion detection system in the active or on state to detect and annunciate unauthorized intrusion, but still permit authorized exit and entry without alerting authorities.

B. Types of Energizing Techniques

1. Shunt Lock - A portion of the protective circuit is removed from the system by a key switch mounted outside the protected area. The authorized individual then enters the area and de-energizes the remaining portion of the system (usually by deactivating the control panel).

2. Local Remote Control - Entire system is deactivated from a key station mounted outside the protected area. Used primarily in residential applications. Less secure because entire system may be defeated at the key station.

3. Magnetic Shunt Switch Contact - A single door is designated as the entry/exit point. A special magnetic switch equipped with a button is attached to the door. To energize the system, the subscriber activates the control panel, depresses the button on the magnetic contact and exits. The system is now armed.

   An entry timer is incorporated into the control panel which allows the entrant 30 seconds to one minute (in some cases more or less) to enter and de-energize the control before the alarm is activated.

4. Entry/Exit Delay - Two timers are incorporated into the control panel. When the subscriber energizes the control he has a period of from 30 seconds to two minutes to exit before the system becomes armed. To de-energize the system another timer begins a cycle (from 15 seconds to one minute) before which the control must be de-energized or the alarm will sound.

5. Remote Signalling - Used with systems reporting remotely (i.e., central stations), this technique involves the actual triggering of the alarm by the subscriber at known times (opening and closing). The

subscriber may also achieve access by telephone. In both cases the central station operator activates and deactivates the system.

6. Combination - Any or all of the above techniques may be employed in combination to meet some requirements unique to the particular system.

V. REMOTE SIGNAL TRANSMISSION AND ANNUNCIATION CIRCUITRY

A. Defined

1. Remote Signal Transmission - Element by which the information received from the protective circuit is routed and incoded for annunciation.

2. Annunciation Circuitry - Element by which the information is communicated from the control function to the annunciation function.

B. Three Categories

1. Direct Wire - Each protected premise is connected to the remote station by wire that is dedicated to that premise and connected to one monitoring position.

2. Shared Wire - Signals transmitted over wire but the wire serves several premises, (includes telephone dialers, Multiplexing equipment, etc.).

3. Other - Includes other transmission techniques not mentioned above, such as radio transmission or transmission over cable or video lines.

ANNUNCIATION

The annunciation function must provide for the reception of the signal from the control and the initiation of the appropriate response. Since the receiving devices are determined by the signal transmission and annunciation circuit of the control function, the functional elements of the annunciation concentrate on the ability to initiate response.

I. TYPES OF ANNUNCIATION

A. Local Alarm

Devices utilized at the secured premises, interior and/or exterior to induce a psychological response from the unauthorized intruder and to alert other responsible persons in the vicinity.

It should be noted that the absence of responsible persons in the vicinity will terminate the Intrusion Detection System information cycle since there is no available means for the required investigation of the environment in which the sensory devices are placed.

B. Proprietary Alarm

The functional element of the annunciation function in which the annunciation devices are utilized in a monitoring facility that is maintained by the owner of the protected premises and is manned by a private force which may respond to any alarm.

This is readily adaptable to large institutions which maintain several buildings in a small geographical area such as colleges, universities, medical centers, etc. The force would naturally have access to the interior of all spaces with intimate knowledge of the layout of the premises.

C. Central Station

The functional element of the annunciation function in which the annunciation devices are utilized in a specially designed monitoring facility offering services to individual subscribers such as police notification of unauthorized entry, records of openings and closings, guard response and key access. Charges are commensurate with those services provided.

D. Police Department Alarm

The functional element of the annunciation function in which the annunciation devices are utilized in a nearby law enforcement agency which initiates direct police response.

Services are limited to police response. Other arrangements must be made to gain access into the premises to complete a search and to check the intrusion detection system.

E. Other Alarms

The functional element of the annunciation function in which the annunciation devices are utilized in any manner other than local, proprietary, central station or police.

With the variety of equipment that is available today, annunciation may be located almost anywhere. This includes monitoring services only, such as telephone answering service and trusted neighbors and relatives.

II. SELECTION OF ANNUNCIATION

All the functional elements of annunciation contain the ability to initiate the response to the alarm in varying degrees. The following is a list of factors of the response which must be considered in order to select the appropriate annunciation functional elements.

A. Speed and training of armed response.

B. Access into premises (availability of keys).

C. Familiarity of intrusion detection equipment.

D. Familiarity of premises.

E. Security of monitoring facilities.

F. Records of openings and closings, as to date, time and person.

G. Psychological deterrant to the criminal from completing the criminal act.

H. Safety to innocent bystanders, employees and police.

I. Reasonable or feasible cost.

The selection of that annunciation element, or a combination of elements, which produce(s) the best results for each individual situation considering good risk management principles must be done with great care. The essential result of annunciation should be to initiate the appropriate response. If the full services of a central station are out of the financial grasp of an individual, other alternatives must be sought to fulfill the need to investigate the environment of the sensors.

SECURITY LIGHTING

SECURITY LIGHTING

The Miracle of Light

The idea that lighting can provide improved protection for people and facilities is as old as civilization. Equally old, however, is the problem of providing good lighting. Babylon dealt with the situation by ". . . burning thick wicks in bowls of fat during crowded festival times". Other approaches included those used in 4th century Jerusalem where crossroads were illuminated with wood dires; and, in the 10th century when the Arabs paved and lighted miles of streets in Cordova. These efforts improved throughout the years when, by the 17th century, both London and Paris made attempts to provide effective street lighting. In England, for example, street lights were provided at public expense where individual citizen action could not be expected; while in France, a program was initiated involving a system of guides with lanterns which the night traveller would pay a small fee for the privilege of being protected by the light.

Over the years, protective lighting evolved from candle and wood power to more sophisticated gas lights, with the first systems installed by the early 1800's. Finally, with the perfection and expanded use of electricity, the first electric filament street lights began appearing during the 1870's, increasing visibility and providing communities with a feeling of security.

As police officers you are, of course, aware of the effect that lighting has in reducing criminal opportunity. Nonetheless, it is interesting to note that a variety of studies and experiments have recently been conducted that have documented this fact. For example, in December, 1973, in response to national appeals for energy conservation a small town in Indiana turned off its street lights. An immediate outbreak of vandalism and petty thefts occurred. The outbreak peaked with four firms in a commercial district being burglarized in a single evening. As a result, the conservationists' ideas were replaced by the realities of the community with public demand forcing a return to the properly lighted street.

Clearly, this example is extreme. However, experience has shown the close relationship between illumination and crime. In fact, installation of improved, brighter street lighting in a number of cities has resulted in the following reported effects:

City	Reported Effect in Areas of City Receiving Improved Lighting
St. Louis, Missouri	A 40 percent reduction in stranger to stranger crime; a 29 percent drop in auto theft; and, a 13 percent reduction in commercial burglaries.

New York, New York (Public Parks)	A 50 to 30 percent decrease in vandalism.
Detroit, Michigan	A 55 percent decrease in street crimes.
Washington, D. C.	A 25 percent decrease in robbery, compared with an 8 percent decrease citywide.
Chicago, Illinois	A 85 percent decrease in robbery; a 10 percent decline in auto theft; and, a 30 percent reduction in purse snatching.

It is because of this clear relationship that street lighting intensity has been increased in many communities well above standards required for traffic safety. Street lights, however, are not the only type of lighting important to crime prevention and security. Other types of illuminating devices such as flood lights, search lights, and fresnel units can also be used to increase security around homes, businesses and industrial complexes. The discussion presented below will review the various types of equipment that might be used for security lighting, but we'll first discuss lighting terminology; and, techniques that can be used in the placement and dispersal of lights. The discussion will conclude with the subject of light and the energy crisis.

What is Good Lighting?

Good lighting is the single most cost effective deterrent to crime, but what is good lighting? Ideally, a good lighting system would be reproduced daylight. Realistically, however, the system must furnish a high level of visibility and at the same time a low level of glare. One of the most critical problems that needs to be considered is that the evenness of outdoor light is more important than an absolute level. Too much lighting can actually be a hazard in itself. Outdoor evening activity areas, such as a tennis court or playgrounds, can be hazardous because of the difficulty of seeing clearly into the surrounding area. When an individual leaves a brightly lighted area such as this and walks into a dark area their vision is momentarily reduced and their vulnerability is increased. The opportunity for criminal attack is more of a likelihood when a situation like this exists.

Transitional lighting can be effectively used to minimize this hazard. Transitional lighting merely provides a gradual light level change from a brightly lighted area to a dark area. A lower light level can be employed adjacent to the bright area and this would help to provide a safe transition.

Understanding Lighting Technology: A Definition of Terms

Lighting technology, as you may already have discovered, involves a whole new language. Generally, the terms, definitions and discussions that appear

CONTINUED

1 OF 2

in most texts are designed for the lighting engineer who has a strong foundation in the jargon and specifics of this subject. The terms presented below, although only scratching the surface, provide a point of deparature that you may draw from in developing a better understanding of the subject. In summary, therefore, some of the basic lighting terms that you, as a crime prevention officer, should be familiar with include:

- Watt: A term used to measure the amount of electrical energy consumed.

- Candle Power: The "candela" is the basic unit in lighting. An international condela standard has been established; the National Bureau of Standards is the agency in this country that handles the standardization responsibility. Candle power or the amount of candelas is the luminous intensity of light. As such, the various characteristics of lighting equipment or fixtures are usually defined in terms of candle power distribution curves.

- Lumen: The lamps (light bulbs) used in various lighting equipment are rated in lumens. The lumen is frequently used as a term to express the output of a light source.

- Foot Candle: This is another unit of illumination. It is defined as the illumination on a surface one square foot in area on which is uniformly distributed one lumen of light.

- Coverage Factor: The coverage factor is the minimum number of directions from which a point or area should be lighted depending upon the use of the area. For example, a coverage factor of two is required for parking areas and for protective lighting to reduce the effect of shadows between automobiles, piles of materials and similar bulky objects.

- Reflector: A device used to redirect the light by the process of reflection.

- Refractor: A glass band, globe or bowl designed to control the direction of light by the use of prisms.

- Luminaire: A complete lighting device consisting of a light source, together with its globe, reflector, refractor, and housing. The pole, post, or bracket is not considered a part of the luminaire.

- Visibility: This term refers to the ability to be seen or to facilitate seeing or the distinctness with which objects may be observed. There are four visual factors that must be considered in planning effective security lighting--size, brightness, contrast, and time. Size is an important consideration in that larger objects reflect a greater amount of light. The comparative brightness of objects is important in that brightly polished silver reflects a greater intensity of light to an area than tarnished silver with the same lighting source. Contrast is important in that an object placed against a strongly contrasting

background will seem to reflect more light to the eye than when the object and the background are alike. Time is critical because it requires less time to see accurately under good illumination than it does with poor lighting.

GENERAL TYPES OF OUTSIDE SECURITY LIGHTING

There are four general types of outside security lighting. These are: continuous lighting; emergency lighting; movable lighting; and, stand-by lighting. Each is described briefly below.

Continuous Lighting

Continuous lighting, the most familiar type of outdoor security lighting, can be designed to provide two specific results: greater projection or controlled lighting. The glare method of continuous lighting originated in prisons and correctional institutions where it is still used to illuminate walls and outside barriers. It has been described by some security experts as a "barrier of light" and is particularly effective for lighting boundaries around a facility and approaches to the site. This technique is normally used when the glare of lights directed across an area will not annoy or interfere with neighboring or adjacent properties. The utility behind this method is that a potential intruder has difficulty seeing inside an area protected by such a "barrier"; thus, the lighting method creates a strong visual and psychological deterrent. Generally, flood lights are used in this way because the beam, although easy to direct, produces a great deal of glare that a possible intruder must face.

The controlled lighting approach, that is the second type of continuous lighting, is generally employed in situations where due to surrounding property owners, nearby highways, or other limitations, it is necessary for the light to be more precisely focused. For example, the controlled lighting method would be used when the width of the lighted strip outside of an area must be controlled and adjusted to fit a particular need, such as illuminating a wide strip inside a fence and a narrow strip outside, or the lighting of a wall or roof. One of the most popular methods of controlled lighting for industrial and commercial use is the "surface method". This method provides for the complete illumination of a particular area or structure within a defined site; not only are the perimeters of the property lighted, but so are the various parking areas, storage lots, and other locations that require improved security. Another advantage of the surface method is that the lighting units are directed at a building rather than away from it so that its appearance is enhanced at night and this same principle is used in some locations to illuminate the front and surroundings of residential sites.

Stand-By Lighting

A second type of outside lighting is stand-by lighting. Stand-by lighting systems generally consist of continuous systems, but are designed for reserve or stand-by use, or to supplement continuous systems. These systems are engaged

either automatically or manually when the continuous system is inoperative or the need for additional lighting arises. A stand-by system can be most useful to selectively light a particular portion of a site should prowlers or intruders be suspected, or to light an area merely for occasional use.

Movable Lighting

A third type of system uses movable lighting hardware. This system is manually operated and usually is made up of movable search lights that can either be engaged in selected or special locations during hours of darkness or only as needed. The movable system is normally used to supplement continuous or stand-by lighting. This type of system would be particularly useful at a construction site.

Emergency Lighting

The fourth system is emergency lighting. Emergency lights may duplicate any or all of the other three types of lighting. Generally, the emergency lighting system is used in times of power failure or other emergencies when other systems are inoperative. The unique feature of the emergency system is that it is based on an alternative power source such as a gas power generator or batteries. Emergency lighting should not be overlooked when evaluating facilities.

GENERAL TYPES OF LIGHTING SOURCES

Listed below are the five general lighting sources that are mostly used in providing indoor or outdoor lighting. Their characteristics are described and their lumen output is summarized in the chart at the end of this section. The five lighting sources are: Incandescent, Mercury Vapor, Fluorescent, Metal-Halide, and Sodium Vapor.

Incandescent

Incandescent lighting systems have low initial cost and provide good color rendition. However, incandescent lamps are relatively short in life (500-4000 hours) and low in lamp efficiency (17-22 LPW) when compared to other lighting sources.

Mercury Vapor

Mercury vapor lamps emit a purplish white color, caused by an electric current passing through a tube of conducting and luminous gas. This type of light is generally considered more efficient than the incandescent lamp and is also widespread in exterior lighting. Approximately 75% of all street lighting is mercury vapor. Because mercury lamps have a long life (24,000 + hours) and good maintenance characteristics, they are widely used in applications where long burning hours are customary. Color rendition is generally good except in the blue region of the spectrum, and the lumen per watt is 58-63.

Metal-Halide

Similar in physical appearance to mercury vapor, but provides a light source of higher luminous efficiency and better color rendition. The rated life of 6000-7500 hours is short when compared to the 24,000+ of mercury lamps. Used in applications where color rendition is of primary importance and generally where the burning hours per year are low. Rated at 85-95 LPW.

Fluorescent

Provide good color rendition, high lamp efficiency (67-83 LPW) as well as long life (9000-17,000 hours). However, their long length relative to their small diameter, causes luminaires to have very wide horizontal beam spreads. Fluorescent lamps are temperature sensitive and low ambient temperatures can decrease the efficiency.

Sodium Vapor

High Pressure

Constructed on the same principles as mercury vapor lamps, but emit a gold-yellow color. Produces more lumens per watt (105-140) than any other lighting source, is brighter, and provides good color rendition. Lamp life expected is up to 20,000 hours.

Low Pressure

Constructed similar to high pressure sodium and mercury vapor lamps. Low pressure sodium emits a more gold toned light than does high pressure sodium. Low pressure has a high lamp efficiency. The high efficiency is outweighed by poor color rendition, less efficient ballast (or starter) systems, and requires larger and more expensive luminaires.

LIGHTING PHILOSOPHY FOR ACADEMIC INSTITUTIONS

From purely a crime prevention standpoint, the ideal situation would be to bask the entire campus in high intensity lighting. This, however, would serve to destroy the serene academic environment desired by most institutions of higher education. Our philosophy at the University of Louisville, in regards to security lighting, is to provide light in a sufficient quantity to maintain an environment of perceived safety and security while attempting to preserve the traditional academic setting. An excellent example of this approach is the recently-installed pedestrian lighting on the major sidewalks that criss-cross the Belknap Campus. These "corridors of security" provide excellent pedestrian pathways throughout the campus without lighting up the entire area like the proverbial "Roman Candle".

Security lighting generally results in some type of a trade-off. While from our standpoint we are intensely interested in the protection of persons and property, aesthetic values must also be considered. Obviously, one would usually not recommend the same level of light around an academic building that one would hope to have in a parking lot. The primary point within the basis of our security lighting philosophy is that we must endeavor to protect lives and property without destroying the enherent environmental quality of the institution.

GENERAL GUIDELINES FOR LIGHTING LEVELS AROUND BUILDINGS

Generally, the most cost effective way to improve lighting is to include good planning into new or renovated facilities and replace older existing fixtures as funds become available.

The following levels of illumination are recommended for all new exterior lighting installations.

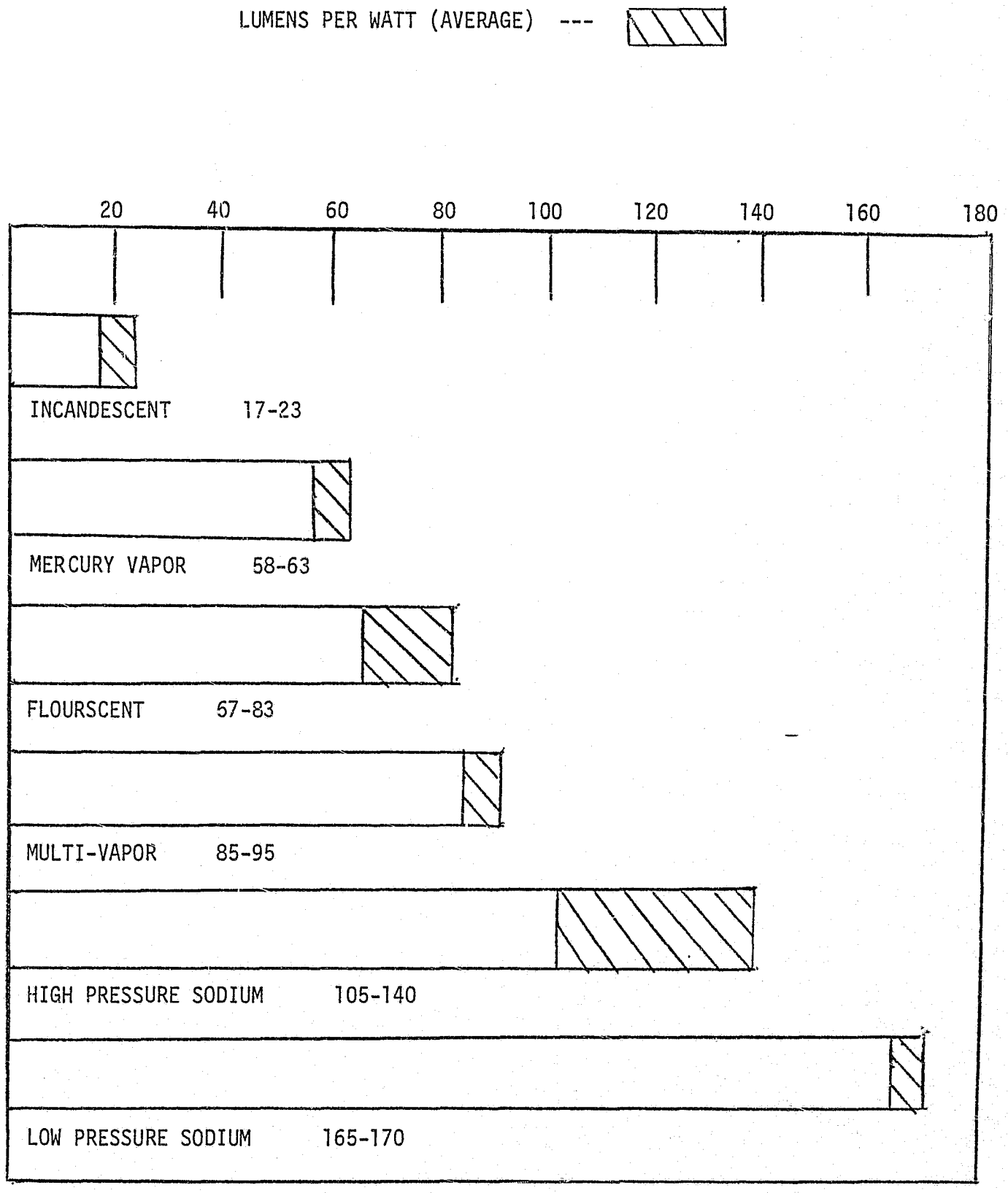
Pedestrian walkways	5 ft. candles
Building entrances and exits	5-8 ft. candles
Building walls w/windows	3-5 ft. candles
Building walls w/o windows	1-2 ft. candles
Pedestrian walkways crossing street	8-10 ft. candles
Parking Lots	3-5 ft. candles

LIGHTING WITH ENERGY CONSERVATION

As we face continuing energy problems, effective steps must be taken to provide sufficient illumination levels without disregard for the amount of energy consumed. The pedestrian walkway lights on the Belknap Campus again provide an excellent example. During high pedestrian traffic volume periods all lights are kept on. However, after these high volume periods are past, every other luminaire is extinguished, thus reducing the level of energy consumption by half. Careful planning should include these necessary provisions.

SUMMARY

Lighting alone is not a cure-all for security deficiencies. Recommendations for improved lighting should be made along with items such as the removal of trees and shrubs that reduce light levels, or improving the reflective surfaces that the lighting illuminates. Changes should be cost effective not only in the amount of light provided but in the type and length time it is necessary.


LUMENS PER WATT (AVERAGE) ---
20
40
60
80
100
120
140
160
180
INCANDESCENT 17-23
MERCURY VAPOR 58-63
FLOURSCENT 67-83
MULTI-VAPOR 85-95
HIGH PRESSURE SODIUM 105-140
LOW PRESSURE SODIUM 165-170

BIBLIOGRAPHY

Callander, Don. "Light, A Weapon In War on Accidents and Crime", American Motorist, reprint. Hendersonville, South Carolina: General Electric, March, 1962.

General Electric. Glossary of Terms Used in Street and Highway Lighting. Hendersonville, South Carolina: General Electric, 1973.

Healy, Richard J. Design for Security. New York: John Wiley and Sons, Inc., 1968.

Hemphill, Charles F., Jr. Security for Business and Industry. Homewood, Illinois: Dow Jones Irwin, Inc., 1971.

Holland, William. "New D. C. Lights Cut Crime", The Evening Star. Washington, D. C., Friday, June 18, 1971.

Landman, Amos. "Lighting for Crime Prevention", Street and Highway Safety Bureau, undated.

LEAA Emergency Energy Committee. Energy Report No. 2: Street Lighting Energy Conservation and Crime. Washington, D. C.: U. S. Government Printing Office, March 1, 1974.

Luedtke, Gerald and Associates. Crime and the Physical City. Detroit: General Luedtke and Associates, June, 1970.

Lurkis, Alexander. "More Lighting and Fewer Juvenile Problems". American City. New York: Department of Water Supply, Gas and Electricity, January, 1962.

Malt, Harold Lewis and Associates, Inc. Tactical Analysis of Street Crime. Washington, D. C.: Harold Lewis Malt and Associates, 1973.

Texas Crime Prevention Institute. "Specialized Crime Prevention Course for University Police". Southwest Texas State University, San Marco, Texas.

END