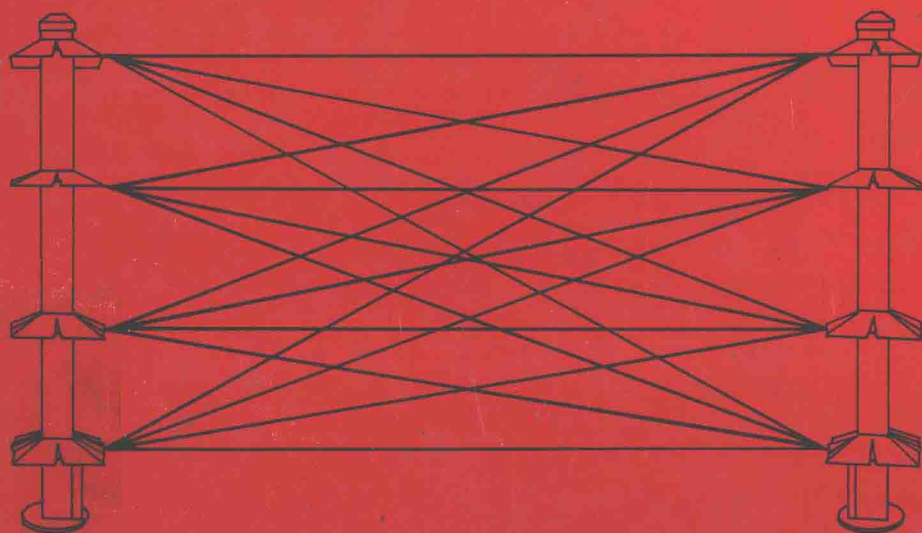


Crime Prevention Through Physical Security



Walter M. Strobl

Crime Prevention Through Physical Security

WALTER M. STROBL, CPP

President

Strobl Security Service, Inc.

Memphis, Tennessee

MARCEL DEKKER, INC. New York and Basel

Library of Congress Cataloging in Publication Data

Strobl, Walter M.[Date]

Crime prevention through physical security.

(Occupational safety and health ; v. 2).

Bibliography: p.

Includes index.

1. Industry--Security measures. 2. Retail trade--Security measures. 3. Public institutions--Security measures. 4. Crime prevention and architectural design.

I. Title. II. Series: Occupational safety and health (New York) ; v. 2.

HV8290.S84

364.4

78-15329

ISBN 0-8247-6722-5

COPYRIGHT © 1978 by MARCEL DEKKER, INC. ALL RIGHTS RESERVED

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage and retrieval system, without permission in writing from the publisher.

MARCEL DEKKER, INC.

270 Madison Avenue, New York, New York 10016

Current printing (last digit):

10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

For my wife, Carolyn

Foreword

Crime Prevention Through Physical Security is a unique combination of technical information and professional experiences that will be valuable to a broad range of security interests. The book will be valuable to the security generalist who needs a solid introduction or review of the technical aspects of security hardware and will be a practical guide to the analysis of security problems and the application of solutions.

Mr. Strobl's extensive use of personal experiences lends credibility to his recommendations and instructs through example how initiative, innovation, and pragmatism are required to construct workable security programs.

But the author does not treat only practical matters in this volume. He also addresses an issue that must be faced by private and public decision makers—the right of privacy versus the right to protect company and personal assets.

In encouraging police crime prevention personnel to acquaint themselves with fire prevention activities, the author has helped close a communications gap that sometimes exists between police and fire services.

Crime Prevention Through Physical Security is required reading for newly appointed security directors. It is a solid review for the experienced and could serve as a textbook for practice-oriented college and university security courses.

Wilbur Rykert
Executive Director
National Crime Prevention Association
Washington, D.C.

Preface

During the past 2 years, I have had numerous discussions with professional security experts and police officers assigned to crime prevention units concerning the need for a comprehensive book on establishing security programs for specific facilities and situations. The majority of these conversations inevitably led to discussions about the need for a sophisticated reference book on the subject of physical security. Specifically, more detailed information is needed by the security professional in the security industry, the police officer assigned to a crime prevention unit, and those individuals employed at different facilities who may "wear many hats," one of which is to ensure that the facility's physical security program is adequate and regularly updated to meet changing requirements.

On September 16, 1975, Richard Velde, Administrator of the Law Enforcement Assistance Administration, speaking at the annual meeting of the International Association of Chiefs of Police in Denver, declared that America simply cannot afford two competing systems of crime prevention—public and private. He told the gathering of national police chiefs that they should learn to cooperate more fully with the private security industry, which in many metropolitan areas outstripped the police departments in terms of financial and manpower resources.

Most major city police departments have organized or are in the process of organizing crime prevention units. The obvious need for this police service should not be underestimated, because police departments should participate in planning decisions in new construction within their jurisdiction, whether this construction is a high-rise apartment complex, a condominium housing project, a shopping center, or an urban renewal project. I feel there is an obligation on the part of police departments to assist in these areas as well as to survey and give advice to the builders, owners, or operators of all types of business, both government and private, when they are requested to do so. The basic concept of crime prevention must start with the establishment of physical security of the facility or area to be protected.

One need only consider the 18 percent increase nationwide in overall crime that occurred in 1975, remembering that this increase was directed against both persons and property.

Facts are irrefutable. Between December 1973 and February 1974 the Federal Aviation Administration required airport management and airline management to tighten security for the protection of passengers and aircraft crews. It appeared incredible that persons and hand-carried luggage would be subjected to thorough searches before boarding any aircraft departing some 531 airports throughout the United States. The program, as we are now all aware, has been successful within the United States. The search of both persons and baggage is accomplished through the use of electronic devices and physical searches by trained personnel.

The recent increase in kidnappings, bombings, and other terrorist activities in the United States dictates that security personnel review their current programs and expand their protection plans to include executive personnel and their families. There is a need for tighter security in their computer operations and a general tightening of all security measures to ensure adequate protection of property and safety of personnel.

Top management in the private sector and in municipalities and their police departments must take a more realistic look at their protection programs. There is no reason to believe that crimes in the nation will decline appreciably in the next few years. Certainly there is no expectation that crimes against persons will decline in the near future.

With these conditions in mind and in view of the apparent need for more information in developing security programs for specific installations, personnel protection, and the like, I have assembled, in this book, detailed information that will assist individuals in better discharging their security responsibilities.

The need for tighter security on our college campuses, in our high schools, and in our grade schools has increased dramatically in the past couple of years. There is hardly a school district in the nation that has not been plagued with costly vandalism inflicted by the student population and outsiders. Therefore, I have included a chapter that discusses numerous changes in design, material used in building construction, and organization of the complexes' parking lots, sidewalks and athletic fields, which will in many cases deter vandalism or otherwise decrease the cost of damage repair caused by vandals.

To write about or discuss physical security without including a discussion of the basic principles is quite impossible, because these principles apply in all situations to some degree. They are merely tailored to provide the degree of security required in each situation. It is therefore impossible to write a book such as this without discussing these principles and their application in the overall security plan.

I wish to thank all my associates and good friends in the private security industry and police department crime prevention units for encouraging me to undertake this project so that this material can be shared with all who have the responsibility for protecting property, lives, and assets.

Special thanks to my wife, Carolyn, for her inspiration, dedication, and confidence in me. My appreciation also to the many persons and companies who have so generously provided the photographs that appear throughout this book and to Eddie Hamilton, retired fire chief, Memphis, Tennessee, for his assistance with the material in Chapter 10. Thanks also to Caril Magdefrau for contributing his talent in the field of closed-circuit television systems.

Finally, my most sincere appreciation to Kathie Wilson, who, I believe, sometimes neglected her family to spend long hours at her typewriter to complete the manuscript.

Walter M. Strobl

Contents

FOREWORD	v
PREFACE	vii
1	
EVALUATING THE SECURITY REQUIREMENTS	1
2	
DEFINING AND ANALYZING EXISTING HAZARDS	4
3	
SECURING THE FACILITY'S PERIMETER	25
4	
SECURITY OF OPEN AREAS	45
5	
ILLUMINATION IN THE PROTECTIVE PLAN	53
6	
INDUSTRIAL BUILDING SECURITY	70

7		
DOCK, WAREHOUSE, AND CARGO SECURITY		93
8		
LOCK IDENTIFICATION, KEY SYSTEMS, AND KEY CONTROL		111
9		
IDENTIFICATION AND CONTROL OF PERSONNEL AND VEHICLES		147
10		
THE FIRE PROTECTION PLAN		175
11		
SECURITY THROUGH ELECTRONICS		214
12		
SURVEILLANCE THROUGH CLOSED CIRCUIT TELEVISION SYSTEMS		237
13		
PHYSICAL SECURITY OF A COMPUTER AREA		256
14		
HIGH-RISE BUILDING SECURITY		269
15		
HOSPITAL AND HEALTH CARE SECURITY		286
16		
BANK AND FINANCIAL INSTITUTION SECURITY		312

17		
THE RETAIL INDUSTRY PROTECTION PLAN		331
18		
REDUCING VULNERABILITY OF THE CONSTRUCTION SITE TO THEFTS		356
19		
INDIVIDUAL AND GROUP THEFT CONTROLS		365
20		
MINIMIZE THE BOMB THREAT—PLAN AHEAD		379
21		
THE EMERGENCY CONTROL PLAN		388
22		
THE EMPLOYEE SECURITY EDUCATION PROGRAM		399
23		
DESIGN TO REDUCE SCHOOL PROPERTY LOSS		403
24		
THE EXECUTIVE PROTECTION PLAN		414
BIBLIOGRAPHY		419
INDEX		425

Evaluating the Security Requirements

To establish an economical, workable, and effective security program at any type of facility requires first that an in-depth study of the facility be conducted. This study must then be analyzed and a determination made of the degree of security that is required for the protection of property, lives, and assets.

It is not difficult to determine whether protection of property and assets must be increased. High losses and depressed profits indicate that either internal or external thefts are being committed or perhaps a combination of both. In order to reduce these losses and increase the organization's profits, it is essential that a security study be conducted.

Depending on the type of commodity being handled, the high public visibility of the organization, and the notoriety that chief executives may be creating for whatever reason, protecting the life safety of management personnel and their families may become increasingly more important. The fact that the company may have multinational operations adds to the possibility of attempted attacks and most certainly tends to make assets more vulnerable.

Initially, a number of assessments must be considered in developing an overall security program. Generally, those assessments fall into ten basic categories.

1. Surrounding terrain. This is of particular importance when the facility is located in suburban or rural areas, where special precautions must be taken or where existing conditions may be used to the advantage of the security planner. If the surrounding terrain is unlikely to affect the overall protection of the facility, then disregard it. However, in most instances, particularly in the industrial sector, surrounding terrain will present the security planner with areas that require special treatment.

2. Economic status of the area. This requires careful study, particularly in urban areas where crime rates are high. In these areas, unemployment, inadequate education, and other unstable conditions are likely to result in overt or covert attacks against the facility being protected.

3. Sociological conditions and psychological outlook. Unfavorable social conditions and psychological outlook of the surrounding community can present special problems and may already have had some effect on existing

operations, because local residents probably are a substantial part of the work force. When planning new construction, site-selection teams must fairly evaluate sociological and psychological conditions, because they will have a definite bearing on the security of future operations. Therefore, any organization planning construction of a facility at a new location would be well advised to include a security representative as a member of the site-selection team.

4. Labor conditions. Labor conditions in the community as well as conditions in established facilities may well dictate the degree of security that will be acceptable. Planners must give consideration to employee-management relations, union agreements, and the severity of violence that may have occurred in past labor disputes. Perhaps now is the time to effect greater protection for the transformer banks, gas metering equipment, or other critical equipment that suffered physical damage in past disputes because of the vulnerability of its location.

5. Location of fire and police departments. The size and proficiency of these departments and the response time when summoned will certainly influence the security plan. For example, if the fire department is made up entirely of volunteers, surely the fire-protection plan of the facility will need to be strengthened by an increase in manpower, by better training, and, in all probability, by the purchase of fire-fighting equipment that ordinarily would not be required.

6. Operational flow plan. The operational flow plan and the number and category of employees will certainly have an effect on the overall plan. The study of this area must consider density of employee population in the various departments or on various floors. Consideration should also be given to the rate of annual employee turnover in all categories; administrative, hourly, technical, supervisory, and so forth. Any contemplated changes in employee strength usually attributed to seasonal production and the effect of these changes in population density throughout areas is of equal importance. The number of employees on each operational shift and shift-change times must be studied. These conditions will almost always have an effect on the parking plan and the location and number of authorized employee entrances. One can easily see that the size and deployment of the security force may well be determined by this one item alone.

7. Criticality and vulnerability. By criticality we mean the importance of certain functions to the continued successful operation of the organization and the vulnerability of these functions to successful attack. An example might be a computer operation located at ground level on the periphery of the building with expansive plate glass areas that expose the operation unnecessarily. The computer operation is critical, and the location makes the operation quite vulnerable to attack. This type condition may require protecting the window openings or moving the entire operation elsewhere.

8. Natural phenomena. The vulnerability of the facility to damage or destruction by natural phenomena must always be considered, particularly

by those who are selecting sites for new construction. This part of the study will require securing past weather data from the government weather service and local chambers of commerce. Studies of topographical maps are a must when the facility is located in suburban areas. United States Army Engineers can offer much assistance in this area relative to drainage conditions and past flooding conditions. A small stream near an industrial park may become a raging torrent when hurricanes or heavy rains occur. The possibility of such phenomena as tornadoes, hurricanes, earthquakes, and even heavy snows will surely require special training for emergency squads of employees and the security force. An evacuation plan will have to be set up, and special equipment may have to be purchased. Weather conditions will have a direct effect on any plans being formulated. We shall discuss later the effects of heat, cold, and darkness in creating favorable climates for the perpetration of thefts and other crimes against people and property.

9. Vulnerability to theft and pilferage. The security of all entrances to property and buildings and control of personnel and vehicles fall into this category. In a given facility, the product being manufactured and its susceptibility to easy removal, personal use, or quick resale will always dictate the degree of security that must be developed in quality-control operations and in areas where the finished product is stored and displayed.

10. Manpower requirements. Finally, the actual manpower that will be required to execute the security plan that has been formulated will have to be determined. The following items must be considered: (a) the economy of the overall program; (b) the legal aspects of certain restrictions; (c) the effect of the new or revised restrictions on employee morale; and (d) the calculated risk that management is willing to accept in lieu of obtaining maximum security as determined by the study.

After all of the above conditions have been studied, data accumulated, and the analysis of each condition made, how the program will be implemented must be decided upon. Certainly it is human nature to resist changes, particularly when such changes may cause some inconveniences heretofore not encountered. The security planner must, therefore, attempt to anticipate the problems and find means to incorporate the program into the overall operational procedures of the facility so that it is at least reasonably acceptable to the majority of the population affected by it.

The success of the security program is related directly to the employee educational program, which should be started well in advance of inaugurating any changes. The informed employee is a more satisfied, cooperative person. If management is in tune with the spirit of the program, acceptance by the employee is that much more assured.

2

Defining and Analyzing Existing Hazards

The first step in any study is to determine what is to be accomplished, what present conditions are, and how these conditions can be altered to best satisfy requirements.

The same is true of the security study—or survey, as it is normally referred to. However, before starting this study, the surveyor must be able to identify those obstacles, including those that may surface later, that will have to be overcome. The obstacles are security hazards. The degree of danger these security hazards present will depend on numerous factors that are usually grouped under two general terms: criticality and vulnerability.

What, then, is a security hazard, regardless of the type facility or area being surveyed? By definition, the hazard is any act, omission, or condition which would seriously impede continuous successful operations, cause the loss of assets, compromise proprietary information or cause loss of life or serious injury to personnel—either employees or others temporarily on company property.

Industrial complexes, for example, are often the target of attack merely because of the product they manufacture, or the computer complex is attacked merely because of the information stored that pertains to persons. It is likely that attacks will soon be attempted against computer operations involved in the National Crime Information Centers, not necessarily to destroy records, but perhaps to secure information on individuals that would be used for extortion or perhaps merely to distort factual information.

It is a proved fact that it is far more economical to deter or attempt in some manner to prevent illegal and unsafe acts from occurring than it is to apprehend and prosecute individuals after the acts have been committed. Furthermore, it is also a fact that the employee, regardless of his or her rank or category, who feels secure in his or her position, both physically and financially, is a more productive and accurate worker. One must also consider that embarrassing or undesirable notoriety caused by the peers of the employees have a direct effect on the morale of the employees as a group, even though they may not be directly involved.

It is often not possible to eliminate all hazards to security for numerous reasons, but usually because management considers the reduction unwise or unjustifiable economically or because the restrictions on movement of personnel or material would impede operational efficiency and cause the loss of time and money. When this occurs, calculations of the risks involved must be defined, and management will then have to decide the degree of risk it is willing to assume.

One cannot discuss the major hazards to security without examining in some detail the human element. Until quite recently, this aspect of security was concerned almost entirely with the illegal actions of employees alone or in concert with outsiders and fell into the category of "natural hazards" that will always exist to some degree. We now must expand the human category to include the "bomber," the "extortionist," the "kidnapper," the "assassin," and the "terrorist."

NATURAL HAZARDS

Actually, the natural hazards to security are nothing more than acts of nature or natural phenomena that occur and are usually peculiar to a particular area. Weathermen will refer to regions in the United States as the "Hail Belt" or "Tornado Alley," and certain geographical locations are more apt than others to have earthquakes. All of the natural hazards present their own peculiar problems, some more frequent and more severe than others.

Site-selection teams for construction of new facilities or major expansion at present locations must be clearly aware of the local destructive phenomena that could occur. In California, for example, building codes in many localities include specific design to reduce damage should an earthquake occur.

There is little that individuals or groups can do while some of these phenomena—for example, an earthquake—are occurring. The loss of lives and property, however, can be minimized by prior planning, including the preparation of written plans that are tested and updated regularly. There is much that can be accomplished in reducing damage due to natural hazards if the security plan includes a well-organized, trained, and supervised security force whose effectiveness can be measured only by their involvement in the overall disaster or emergency plans that have been formulated.

Natural hazards most often discussed are the following: heat, cold, darkness (these three being by far the most common and troublesome), fires, explosions, floods, hurricanes, tornadoes, and earthquakes. Other less frequently discussed destructive phenomena include hail, ice storms, and the occurrence of "pot holes" in some sections of the country. The largest "pot holes" occur when the surface of the earth caves in as a result of subterranean erosion, the work of underground rivers. However, such

occurrences are unpredictable and infrequent, and so the security analysis rarely, if ever, considers them.

Darkness

It is an old adage that thieves do not like to "work" during the hours of daylight or in areas that are sufficiently illuminated to expose their illegal activity to observation.

Because periods of darkness occur regularly during every 24-hour period with a predictable by-the-minute increase or decrease in duration, the surveyor must be ever mindful of this occurrence. Not only is the engineering and installation of the interior and exterior protective lighting system directly affected, but equally involved are closed circuit television systems, foot and motorized patrols, location of truck parks inside the perimeter, and practically every other item or condition that will be examined in determining and planning the security requirements for any facility.

Although a properly engineered protective lighting system will eliminate many of the hazards that exist, during the hours of darkness one cannot rely entirely upon the system alone. Remember that every physical device designed to increase protection has a certain vulnerability to being defeated. The power lines serving the lighting system and each individual luminaire or group of luminaires are highly vulnerable to successful attack by the very nature of their location. Therefore, the defense of the entire system must be planned in depth. For example, the effectiveness of the chain-link-type perimeter barrier at any facility is immediately reduced when darkness occurs unless it is adequately illuminated. Also, peripheral lighting equipment is extremely vulnerable, and this vulnerability is increased if there is no chain link fence to protect it. Therefore, one technique or device to establish physical security at a facility is compatible with one another, and one will directly affect the effectiveness of another.

The following incident will give you some appreciation for the immense problems that darkness can cause. Recently, I was involved in planning security protection during the construction phase of the trans-Alaska oil pipeline. I had an assistant fly to the Prudoe Bay area installations in the month of January to carry out various tasks, including photographing a typical installation and some typical terrain. The photography part of the mission was a complete flop because during that time of year the area is in almost total darkness 24 hours per day, and only 1 day was scheduled for completion of the mission.

Heat

These hazards to security, like darkness, will vary in severity and duration depending upon the geographical location of the facility to be protected. Protection against the effects of heat, including the high temperatures that