SECURITY FOR SMALL BUSINESSES

David L. Berger

SECURITY FOR SMALL BUSINESSES

DAVID L. BERGER

BUTTERWORTH PUBLISHERS INC.
Boston London

To Julie

Copyright © 1981 by Butterworth (Publishers) Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

All references in this book to personnel of male gender are used for convenience only and shall be regarded as including both males and females.

Library of Congress Cataloging in Publication Data

Berger, David L., 1929-
Security for small businesses.

Bibliography: p.
Includes index.
1. Small business—Security measures.
I. Title.
HV8290.B48 658.4'7 81-12311
ISBN 0-409-95037-8 AACR2

Published by Butterworth (Publishers) Inc.
10 Tower Office Park
Woburn, MA 01801

Printed in the United States of America

INTRODUCTION

In preparing this book, the author attempted to learn the total amount of small businesses in the United States and possibly some breakdown, by category. Surprisingly, the Department of Commerce, Census Bureau, and even the Small Business Administration could offer no statistics providing information on all concerns considered "small businesses" in the United States. There are statistics relative to payroll taxes paid by the employer, but even then, thousands are unaccounted for. The best we could do is estimate that there are "about" 3,648,513 businesses of less than twenty employees.[1]

Businesses with one hundred or more employees, more able to afford the services of a resident Security Officer, and many companies with as few as ten employees, are utilizing one of the many contract services available within the security field, the cost of that contract security being tax deductible and both a legitimate and necessary expense. But what of the millions of small businesses that cannot afford those services: The so-called "mom and pop" stores, gas stations, repair shops, medical and dental offices, law firms, movie houses, real-estate offices, body shops, hardware stores, etc. It would be difficult just to list all the different types of small businesses, manufacturing firms and professional offices. To determine just how many exist is virtually impossible.

It is those millions of small businessmen — not the giants of industry — who are the very backbone of our country and economy. And they are the ones who suffer the most at the hands of an ever-increasing crime rate. Losses rooted in criminal activity are absorbed by the "majors," who simply collect insurance and raise prices, transferring the burden to the consumer. The small business operator is usually expected to "eat" his loss, collect a meager insurance payment (if he is covered), and attempt to recover . . . "somehow."

For the purpose of this book, "small business" can run anywhere from a sole proprietor to a couple of hundred employees. The small business that we are concerned with here is any business that does not feel it is large enough to

[1]County Business Patterns 1976, United States CPB-76-1, U.S. Department of Commerce, Bureau of the Census.

be able to afford a formal security program built into the company staff and is either unaware of, or unable to afford, one of the many contract services available to the business. This book is intended to advise that businessman of the proper precautions and deterrent measures he can adapt to insure his own protection. In many cases, the precautionary measures described here will not only cost very little, if anything, but may substantially reduce the cost of liability insurance, thereby actually saving money that can be counted. The savings that cannot be counted are those losses that will not be suffered because the proper precautions were taken.

Most people think of the recent surge of the security industry as a modern advance toward the fight against a sudden increase in the crime rate. In the past few years, security guards across the United States have, remarkably, outnumbered law enforcement officials, many times over. Closed circuit television, types of new alarms, computerized access controls, lasers, tasers, bugging devices, counterbugging devices, electronic locks—all of the technology and publicity about "protection" — have given rise to the myth that "security" is something new. Actually, archaeologists have traced intelligent security "planning" back to the earliest inhabited caves, populated by man even prior to forming into social groups of more than just two, three, or four of our ancestors. Even those earliest men assigned "guards" to stand vigils and keep watch for wild beasts or other human intruders. The first access control was probably a fire placed at the entrance of some cave, again designed to ward off intruders or wild beasts. Think of the magnificent perimeter protection devised by the ancient Egyptians in building the pyramids. If they had only had the steel construction materials of today instead of the simple stone and masonry, the graverobbers would certainly have been thwarted, and those priceless treasures would have been preserved for the modern world to enjoy. But one must admit that they were on the right track, for we in modern security use many of the same methods as those ancient designers.

Although this book will go into some detail regarding sophisticated electronic devices available on the market, should the reader desire to purchase those items, it is primarily a set of instructions of the practical and functional methods that can be applied toward securing businesses — techniques and procedures that anyone can apply, common-sense methods which, when properly coordinated with a few professional "tips," can be most effective. It will also describe the many services available and, contrary to popular belief, are practical from a financial standpoint; for, not only are they tax deductible, but they are also specifically designed to minimize losses and increase profits.

Let us decide now to force the criminal, who also operates both large and small businesses, into bankruptcy.

此为试读,需要完整PDF请访问: www.ertongbook.com

CONTENTS

I. PROTECTING THE BUSINESS: SECURITY EQUIPMENT AND METHODS

Chapter 1

PERIMETER CONTROL

Regardless of whether the business is housed in an office building or shopping center, or whether it occupies a single structure bordered by other buildings or surrounded by open areas (parking lot, lawn, etc.), the first line of defense against intrusion is the extreme outward perimeter. This perimeter can be the exterior walls of the building (or office) or a fence somewhat distant from the exterior walls. The first consideration, therefore, is establishing deterrent measures designed to discourage an intruder from penetrating to the interior of the business. Bearing in mind that most individuals are conscious of the appearance of the business, it should be noted that most of the measures discussed here can be designed, with a little imagination, to be aesthetically acceptable.

BARRIER PROTECTION

This section contains information for those small businesses, possibly small to medium outside manufacturing firms or businesses, that are housed in private dwellings where the installation of a fence or other barrier may be deemed appropriate.

Fences and other physical barriers serve to define the perimeter of a facility. Their fundamental purpose is to deny or impede access by unauthorized persons. Almost any barrier can be climbed or otherwise penetrated by a determined intruder, but the presence of the barrier provides both a delaying factor (making entry more difficult) and a psychological deterrent.

In some situations design and construction of a facility will take advantage of natural barriers such as rivers or other bodies of water, cliffs, canyons, and other physical obstructions. These may make access control easier, elimin-

ating the need for some other types of barriers. It is a mistake, however, to rely too much on natural barriers. Most are overcome relatively easily and must be supplemented by other protection.

Fences, block walls, building perimeter walls, and other structural barriers commonly form the basis of perimeter protection — supplemented by some form of surveillance (guards, CCTV and alarm systems) and security lighting.

Fences

The most common type of security fence is the chain-link design. It should be made of at least 11-gauge wire with mesh openings not larger than two inches square. The chain link should extend to within two inches of the ground or, if the soil is soft and easily moved, the mesh should be extended below the surface. The mesh should be tightly drawn and secured to rigid metal posts set in concrete. Although many existing industrial fences are six feet in height, security fencing should be a minimum of eight feet high overall, including seven feet of chain-link mesh extended another foot by three or four strands of barbed wire angled outward at the top.

A more recent addition to barbed-wire topping is coiled barbed tape, or razor ribbon (see Figure 1-1). It consists of a single helical coil of stainless-steel barbed tape, eighteen inches in diameter, which is mounted on top of the fence, attached to the top strand and leaning away from pedestrian traffic. While this barbed tape significantly extends the delay time in attempts to climb the fence, it should be noted that many penetrations involve cutting, breaching, or going under the fence.

It is also possible to alarm a fence so that any attempt to scale or penetrate it would be detected immediately at a central security control station.

The fence should be lighted at night to make the areas both inside and outside, as well as the barrier itself, visible to roving patrols, and to act as a deterrent.

Masonry walls

Masonry walls should also be an overall minimum of eight feet high in perimeter barrier configuration, with a barbed-wire top guard or broken glass or pointed barbs embedded on top of the wall (see Figures 1-2 and 1-3). While such barrier walls deny the opportunity for an outsider to look into the protected property, they also provide cover for a potential intruder. In this respect, the chain-link fence offers better opportunity for passersby or police patrols to observe any external approach to the perimeter.

此为试读,需要完整PDF请访问: www.ertongbook.com

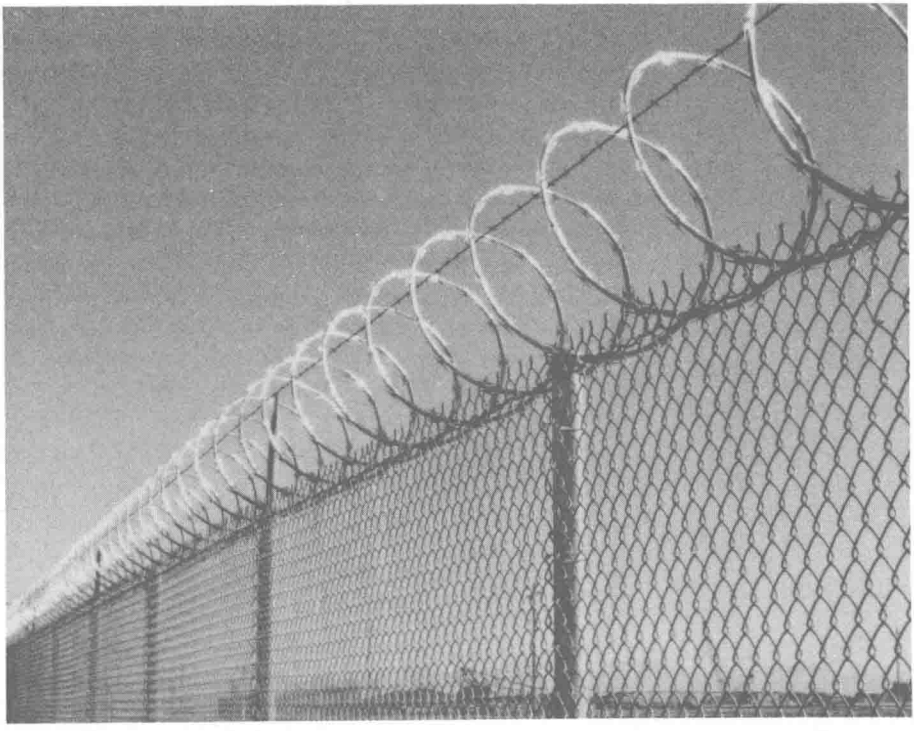

Figure 1-1. Standard chain link fence. (Courtesy of American Security Fence Corporation.)

Openings in Perimeter

Openings in any perimeter fence or wall should be kept to the minimum necessary for carrying out the business of the facility efficiently. All openings should be guarded, locked, or secured in some other fashion. Gates and doors not in use should be locked. Windows and all other openings in exterior perimeter walls of buildings should be covered in such a way as to deny entry, by means of bars, grills, or other barriers. This includes vents, pipes, conduits, and any other openings.

Clear Zones

Clear zones should be maintained on both sides of the perimeter barrier. Shrubbery and weeds that could provide cover for any intruder, or for the hid-

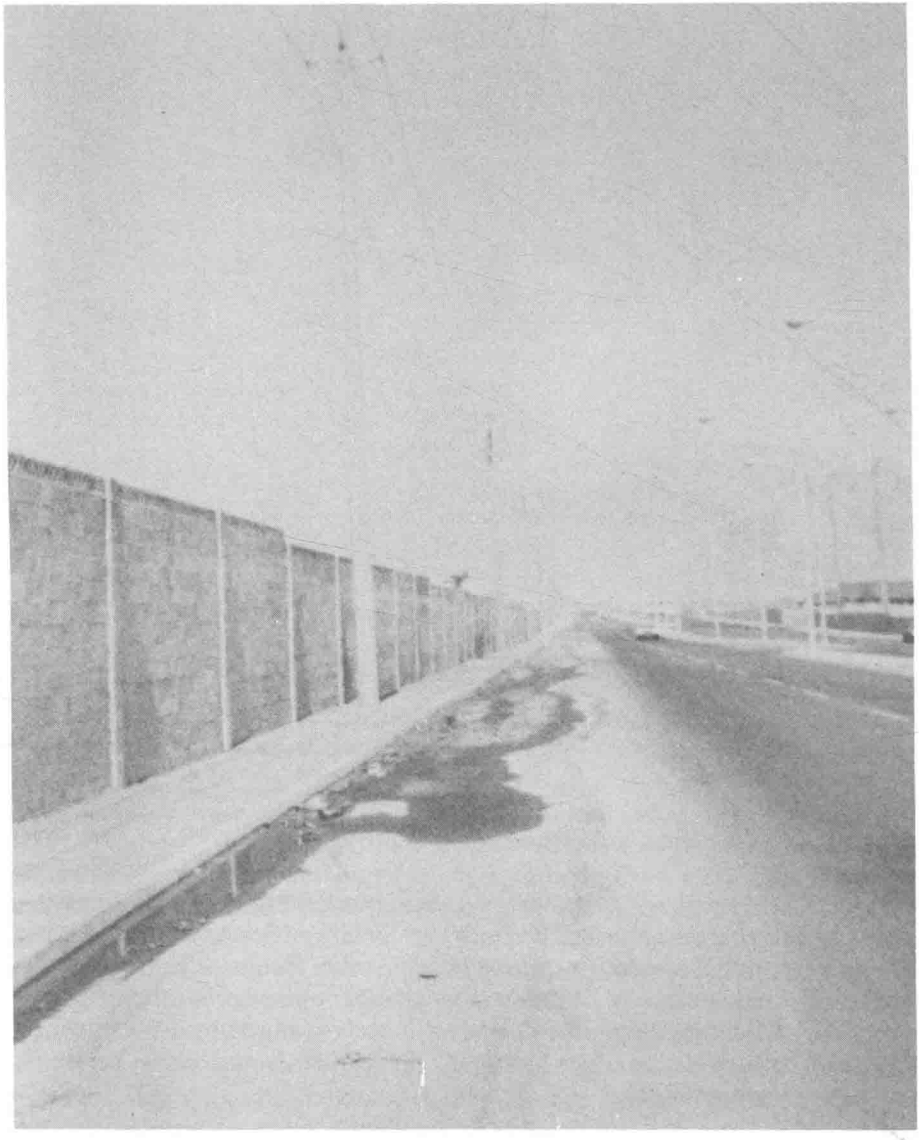

Figure 1-2. Concrete block wall. (From Eugene D. Finneran, *Security Supervision: A Handbook for Supervisors and Managers,* Butterworth Publishers, Inc., 1981.)

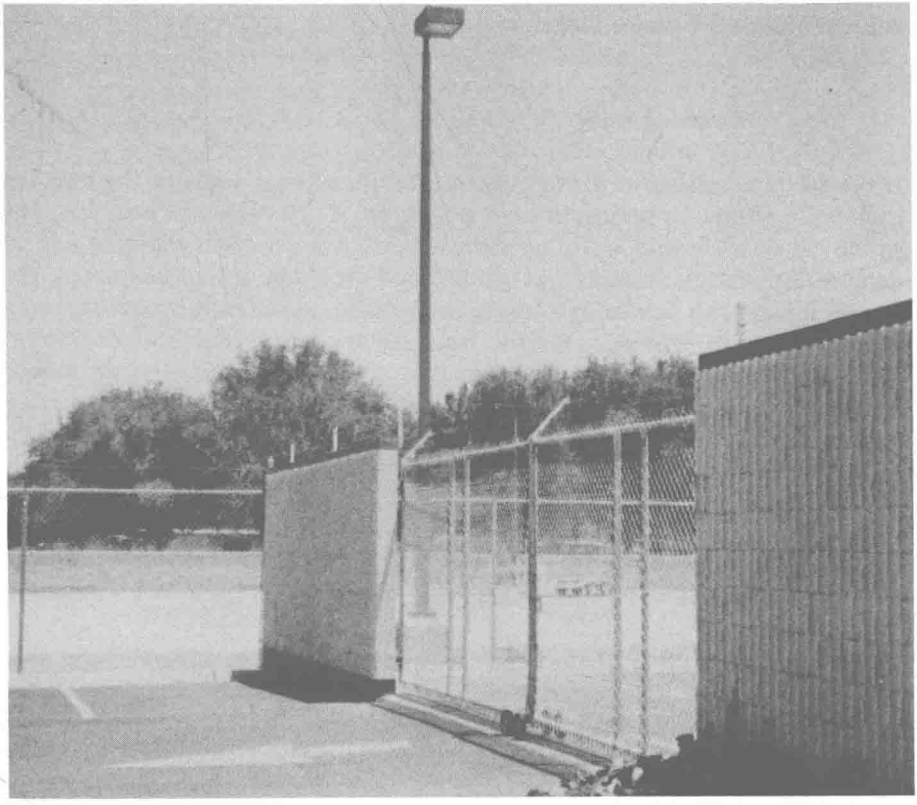

Figure 1-3. Combination block and chain link barrier. (From Eugene D. Finneran, *Security Supervision: A Handbook for Supervisors and Managers,* Butterworth Publishers, Inc., 1981.)

ing of stolen goods, should be cut away, preferably for a distance of fifteen to twenty feet. Stored materials, boxes, or trash of any kind should not be allowed to pile up near the barrier, offering places of concealment. Particular attention should be given to neighboring structures, trees, utility poles, or other elements that might make it easier for an intruder to circumvent the perimeter barrier.

Signs

The fence should also be posted approximately every thirty feet, with a sign indicating that the property is private and that trespassers will be prosecuted.

The sign could also state that other measures are present, such as armed guards, alarms, or guard dogs.

Building walls

If the facility consists of a single structure, the exterior walls of the building itself will become the perimeter to be protected. It is those walls, including any windows, doors, vents, or other openings, that must form the first line of defense. Any burglar alarms that are installed should be at that perimeter. The strongest locks, all deadbolts, should be installed on the exterior doors, and a greater degree of protection on the windows and vents could be considered. There are a number of manufacturers that now make extremely safe and attractive window grills and bars intended to defeat any illegal entry. In retail establishments, the grills are made to fold back during the hours the establishment is open so as not to impair the view of window displays when customers are shopping.

ALARM PERIMETER PROTECTION

There are various types of electronic sensors on the market to detect the presence of an intruder in an exterior area. Not all are applicable to all situations, and each facility will have to be evaluated individually. For example, nearby vehicle traffic may cause false alarming in microwave detectors. Heavy fog, rain, snow, or dust may interfere with the operation of infrared systems.

Fence disturbance sensors detect an intruder climbing over, cutting through, or lifting up a chain-link fence (see Figure 1-4). The sensors are designed to discriminate between the higher-frequency vibrations caused by an intruder and the lower-frequency vibrations caused by wind.

Microwave or infrared systems send an invisible beam of microwave or infrared energy from a transmitter to a receiver and detect an intruder moving through the beam (Figure 1-5).

Buried pressure sensors detect the pressure of an intruder passing over a buried cable.

Electrostatic fences utilize an electric field generated along a series of wires that comprise a fence. When an intruder's body changes the electric field level to a certain degree, an alarm is activated.

Ultrasonic systems emit patterns of radio frequency (RF) waves, and alarm when the signals are altered by the presence of an intruder.

Ferrous metal detectors are sometimes used in high-security government installations within an "inside" perimeter where metallic objects are not permitted. Buried in the ground, the detectors react to metal objects carried by an intruder.

Figure 1-4. Fence disturbance sensor. (From Robert L. Barnard, *Intrusion Detection Systems*, Butterworth Publishers, Inc., 1981.)

Alarming by the above methods is expensive and is necessary only in companies maintaining maximum-security projects. The alarm products themselves should be examined and rated to determine whether they are applicable to each individual situation. All alarm systems are subject to false alarm potential. The major cause of false alarms is malfunction caused by a mechanical defect in the alarm hardware or wiring itself. The second major cause is use of a system that is not compatible with the environment, such as using certain types of motion detection units in areas where large animals are likely to enter the field, or ultrasonic units in buildings too close to railroad tracks with heavy traffic.

DOORS AND WINDOWS

The exterior doors to any business, whether it be in a single building or office within a multi-storied office building, should be of solid wood construction and not the hollow framed doors commonly used on interior doorways (Figure 1-6). Exterior doors should also be fitted with a good-quality deadbolt lock (described in another chapter). It is also important that all exterior doors be well lighted on the outside, preferably by a light in a tamper-proof housing suspended over the door. Figures 1-7, A through I, illustrate common weak-

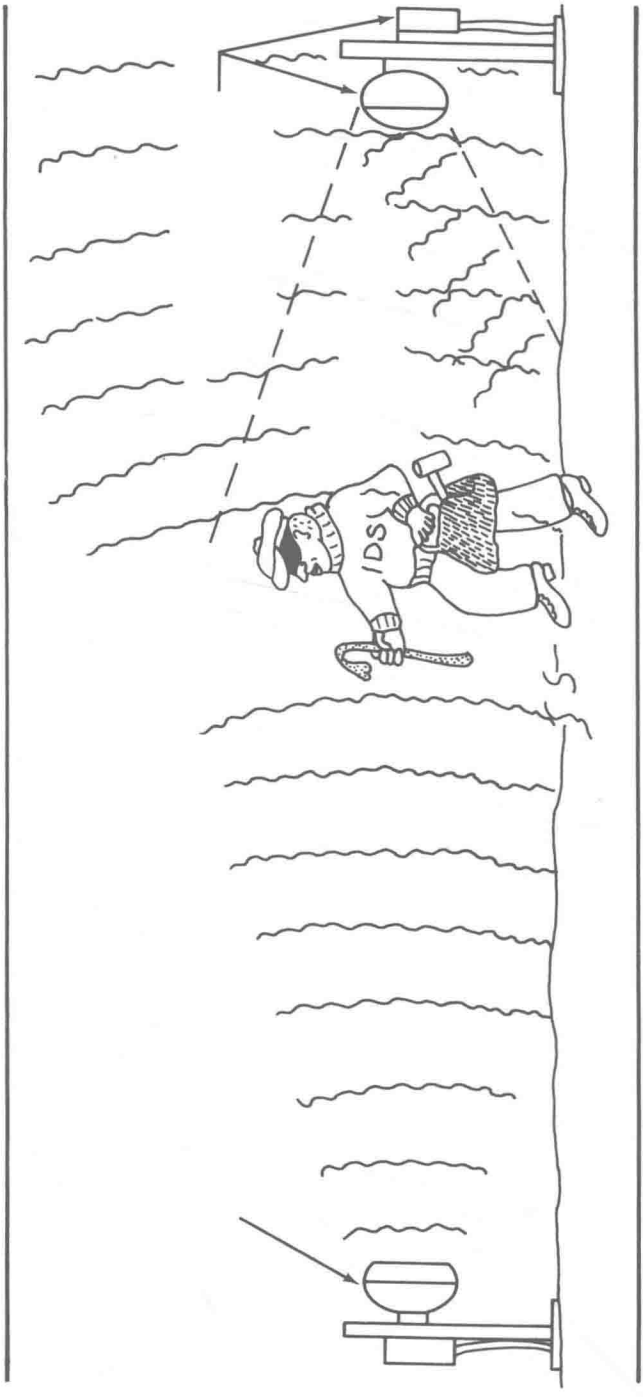

Figure 1-5. Microwave barrier detector. (From Robert L. Barnard, *Intrusion Detection Systems*, Butterworth Publishers, Inc., 1981.)

此为试读,需要完整PDF请访问: www.ertongbook.com