

HOW TO BE YOUR COMPANY'S SECURITY DIRECTOR



ABOUT THE AUTHOR

Keith S. Shannon has over 24 years experience in the field of law enforcement and corporate security starting his career as a police officer, before moving to manage the corporate security organization of a large public utility. He now works as a consultant and instructor to businesses on asset protection topics.

He graduated from the University of North Carolina at Charlotte and the Charlotte Police Academy. He is a Certified Protection Professional (ASIS), a Certified Fraud Examiner (ACFE) and licensed Private Investigator (NCPPSB). His public service includes: member of the NC Private Protective Services Board, former Chair of the Charlotte, NC Police and Firefighter Civil Service Board and other professional organizations. He holds the Advanced Law Enforcement Certification from the NC Criminal Justice Education and Training Standards Commission and was a commissioned police officer in NC for 23 years before obtaining his private investigator's license.

HOW TO BE YOUR COMPANY'S SECURITY DIRECTOR

*A Quick Reference Business Resource of Major
Corporate Security Issues and Protection
Strategies for Management Professionals*

By

KEITH SMITH SHANNON



Charles C Thomas
P U B L I S H E R • L T D.
SPRINGFIELD • ILLINOIS • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

This book is protected by copyright. No part of
it may be reproduced in any manner without
written permission from the publisher.

© 1999 by CHARLES C THOMAS • PUBLISHER, LTD.

ISBN 0-398-06937-9 spiral (paper)

Library of Congress Catalog Card Number: 98-53171

*With THOMAS BOOKS careful attention is given to all details of manufacturing
and design. It is the Publisher's desire to present books that are satisfactory as to their
physical qualities and artistic possibilities and appropriate for their particular use.
THOMAS BOOKS will be true to those laws of quality that assure a good name
and good will.*

*Printed in the United States of America
SM-R-3*

Library of Congress Cataloging-in-Publication Data

Shannon, Keith Smith.

How to be your company's security director : a quick reference
business resource of major corporate security issues and protection
strategies for management professionals / by Keith Smith Shannon.

p. cm.

ISBN 0-398-06937-9 (spiral pbk.)

1. Corporations--Security measures. 2. Industries--Security mea-
sures. I. Title.

HV8290.S48 1999

658.4'7--dc21

98-53171

CIP

This work and all my work is dedicated to Patty

PREFACE

The intent of this book is to give a working business professional a realistic review of security issues a business may have to deal with on an every day level. Many texts have been written discussing these issues in great detail, and offering solutions. While the value of these presentations is very worthwhile for the security professional, most management professionals need a more simple and workable way to deal with security problems. This presentation endeavors to outline security remedies and options on a level most useful for the average business professional.

In many businesses, security management is assigned to administrative personnel not familiar with protection topics. This book will give those individuals a working knowledge of security issues and practices. This guide can be used as an informed starting point with which to deal with a security situation completely, or at best, give some general knowledge of the field if security professionals have to be called. This basic information can save the company money, and the person assigned the task can feel some level of comfort in dealing with the topic.

In my experience of over 24 years in the field, the best methods for dealing with security problems are the simplest. Management desires a list of options from the security professional and then the best course of action has to be factored into the business life of the firm. Often, the best absolute security remedy will not be the best overall action for the company. A combination of steps may have to be taken in order to address the problem.

This work in no way minimizes the professional expertise required of security professionals today. In fact, it will demonstrate the increasing complexity of providing security and asset protection services to organizations. The work is intended to give those nonsecurity professionals a basic frame of reference in order to begin the task of solving their security problem.

The information presented here is from an asset protection viewpoint. No legal or human resources recommendations are made.

Competent legal and personnel interaction are a part of any security plan, and information should be obtained from those professionals as well.

Keith Smith Shannon

CONTENTS

<i>Preface</i>		<i>Page</i>
		vii
<i>Chapter</i>		
1. BOMB THREATS AND ACTIONS		3
Possible Message Carriers		3
Periodic Business Operation Review		4
Police Action and Fire Department Response		4
Evacuation Planning and Administration		4
Date and Time of Threat		5
Possible Suspects		5
Bomb Device		5
Search Techniques		5
2. BUSINESS TRAVEL PROTECTION		8
3. CARGO AND SHIPPING THEFT		11
4. CONTRACT SECURITY OFFICERS		13
Registration		15
Wages		16
Turnover		16
Benefits		16
Post Instructions		17
Staffing		17
Legal Authority		17
Drug Testing		18
Physical and Psychological Testing		18
Daily Management		19
5. CUSTOMER SERVICE AND EXPECTATIONS		20
Office Thefts		20
Parking Lot Security		22
Uniformed Security Staff		22
Image		23
Response		23
Cooperation		23
Effectiveness		24

6.	DOMESTIC VIOLENCE	25
	Child Safety	28
	Financial Resources Set-Aside for the Emergency	28
	Location to Which the Abused Party May Relocate in an Emergency	28
	A Home Evacuation Plan	28
	Legal Documents and Power of Attorney	29
	Details and Copies of Any Restraining Orders or Judgements	29
	Emergency Telephone Numbers	29
	Security of The Employee on The Job	29
7.	EMERGENCY PLANNING	31
8.	EXECUTIVE PROTECTION	33
9.	FACILITY SECURITY ASSESSMENT	37
	The Owner Controlled Area: Outermost Perimeter	37
	Parking Lot Security and Ease of Visibility Around the Area	37
	Perimeter Lighting and Ongoing Maintenance	38
	Landscaping: Areas to Hide	39
	Hidden Access Areas: Below Ground Doors and Windows	39
	Garbage Dumpsters	39
	Fences	39
	Loading Docks	39
	The Protected Area: The Facility Buildings	40
	Locks and Key Control: Issued, Changed, etc.	40
	Hidden Closets, Stairwells, etc.	40
	Interior Lighting	41
	Personnel Access Control: Visitor and Employee Traffic	41
	Restricted Access Areas: How is this Accomplished?	41
	Isolated Work Areas	41
	Package Controls and Mail Delivery	41
	Shipping and Receiving Controls	42
	Appropriate Security and Fire Alarms	42
	Bomb Threat Procedures	42
	Security Force Procedures if Security Officers Are Used at the Site	43
	Duress Alarms at Certain Locations	43
	The Vital Area: Most Sensitive Work Places	43
	Lock and Key Control for These Areas	43
	Trade Secret and Confidential Information Protection	43
	Executive Protection Areas	44
	Wage and Salary Data Locations	44

Contents

xi

	Personnel Information Repositories	44
	Client Contracts and Bid Proposals	44
10.	FRAUD	46
	Embezzlement	47
	False Pretenses	47
	Forgery	47
	Extortion	47
	Worthless Checks	47
	Assessment	49
	Rationalization	50
	Permission	50
	Client Case Review	50
11.	INVESTIGATIONS	55
12.	INTERNATIONAL SECURITY	63
	Pre-Travel Planning	63
	Review These Topics Before Travel	64
	Detailed Emergency Plans	66
13.	KIDNAP AND RANSOM INSURANCE	71
	Determine from the KR Carrier	72
14.	OFFICE THEFTS	73
15.	PERSONAL PROTECTION PLANNING	77
	Personal Protection Planning: Reduce Your Vulnerability	78
16.	POLICE LIAISON	80
17.	PREEMPLOYMENT BACKGROUND INVESTIGATIONS	82
18.	PREPARING COMPANY CASE FOR COURT	85
19.	RETAIL SECURITY AND LOSS PREVENTION	91
20.	ROBBERY POTENTIAL AND PREVENTION	96
	Your Robbery Prevention Program Should Cover:	97
	Know That the Robbery Suspect Will:	97
21.	SECURITY LIABILITY AND REPORTING	100
	Security Professionals Will Recommend a Close	
	Examination of the Following	100
22.	SECURITY SYSTEM PURCHASE	102
23.	SECURITY CONTRACT BID SPECIFICATIONS	106
	General Presentation Format	107
	General Proposal Outline	107
24.	USE OF NONEMPLOYEE SERVICE CONTRACTORS	114
25.	WORKPLACE VIOLENCE	117
26.	WORKSITE WEAPONS-ARMED PERSONNEL	123

HOW TO BE YOUR COMPANY'S SECURITY DIRECTOR

Chapter 1

BOMB THREATS AND ACTIONS

At some point in the life of the company, a bomb threat may be received placing the employees and company assets at risk. Having a general knowledge of how to address a threat is very important to protect the business. Management must devise at minimum a simple plan to deal with these threats.

A bomb threat is usually made to disrupt business operations. No other such incident can so thoroughly disrupt a business except a bomb threat. The motive is to disrupt and cause chaos at the business. Bombers hide behind a cloak of sinister disguise and take pride in their hidden act. The disruption may be planned to impact the ability of the company to operate and make money, gain news media attention for the bomber's cause or take revenge for a company action. Understanding that the bomb motive is disruption is a key issue to understanding how to minimize the act and thus the bomb threat's impact.

Proper planning inside company management, along with a few calls to the local police is the first step in dealing with a potential bomber. Remember that the local police are always the first responder to any bomb threat or explosion; federal or state agencies will be called in later by the local police if needed.

POSSIBLE MESSAGE CARRIERS

Bomb threats normally are made to the company over the telephone, but any message carrier such as e-mail, fax or letter should be considered. Have discussions with employees at these message center locations. Instruct them on passing the message to the appropriate person named in the bomb threat procedure. If incoming telephone calls are recorded, or numbers of the caller identified, be certain to

save that data. If not, message operators should be instructed to be observant for any recognizable evidence associated with the threat such as background noises, e-mail addresses, etc. All this data should immediately be given to the company contact named in the bomb threat procedure.

PERIODIC BUSINESS OPERATION REVIEW

If the business is involved with issues concerning activities aligned with some group's social or political agendas such as nuclear power, abortion, the environment, etc., management should address in the threat procedure how to review the threat potential when business operations may be targeted by action groups. Often, business operations at particular times of the year will be more visible and thus the threat potential higher.

Disgruntled employees or activities affecting management and labor such as union organizing, layoffs, work reductions, etc., may also produce bomb threat motives and potential. Examine these key elements and how to deal with them in the plan.

POLICE ACTION AND FIRE DEPARTMENT RESPONSE

Meet with the local police crime prevention officer. Determine in advance the police response. Plan for this response. Also, contact the local fire marshal at the fire department and ask what response they will provide when called. Emergency telephone numbers should be available to all applicable persons and be kept current.

EVACUATION PLANNING AND ADMINISTRATION

Evacuation routes out of the company facility should be pre-planned and marked. Periodic evacuation drills should be conducted at least annually; coordinate with the police and fire departments. Assembly points outside the facility should be varied and searched for

potential secondary bomb devices planted to harm employees after building evacuation; secondary devices are becoming a large problem. Also, check areas where emergency vehicles will park upon arrival. Secondary devices may harm those vehicles as well.

Management review of the threat potential is very important. If the bomber knows a bogus threat will disrupt the company each time they call, then more calls may be made. A chain-of-command to review the threat should be established, with the final approval to evacuate all or part of the facility made at a senior management level. This review and approval process will be clearly delineated before any threat. Management will consider:

Date and Time of Threat

Does facility evacuation coincide with a holiday, anniversary of a political event, recent employee action, etc.

Possible Suspects

Are disgruntled employees likely to be the cause and if so, what is the real bomb potential? Check with the police and find out if other companies are having similar threats if time permits. A known bomb threat suspect may be contacting several firms in the area. Analyze the possible suspects with real threat potential.

Bomb Device

If a bomb device is mentioned in the threat, does the device appear to have a potential to be real, and if so, what collateral damage could occur to company property causing functional damage, i.e., a bomb exploding in a chemical plant? Also review how any mentioned bomb devices could be hidden.

Search Techniques

Police and fire departments will usually ask for assistance in searching the areas for suspect devices. Employees know best what items

appear out of place, or foreign. The facility rooms and area should be mentally divided into 3 distinct sections, (1) floor to knee level (2) knee to shoulder level and (3) shoulder and above. Search areas starting with the floor and continue overhead. Following the designated 3-step pattern will help avoid missing sections of rooms. If suspect packages or devices are found, DO NOT MOVE them. Call for emergency personnel to evaluate. Remember that a bomb can be placed or built into almost any configuration. Employees conducting the search should be volunteers and have clear instructions from management and emergency agencies before beginning; this is no game.

Remember bombs and bomb threats are used to disrupt the company and work force. Their immediate impact lasts only a few seconds or hours. Human damage may last a lifetime. The bomber will be observing how the incident was managed. How management reacts to the situation will be a major factor in what future threats occur. A clear management decision chain should be used to specify the ultimate decision-maker. Thousands of dollars of company profits are at stake if evacuations are held without good justification. This must be weighed against the potential for human tragedy if the worst happens.

A bomb threat plan does not have to be elaborate. Certain key elements do need consideration and review beforehand. Management support of this planning is essential. If company operations are associated with social and political agendas, management must take greater care in addressing bomb contingencies.

Some companies will use electrical or X-ray equipment to scan executive mail for possible devices. This equipment has been reduced in size and cost over the years. Mail personnel can receive free and valuable training from the local police crime prevention officer about how to deal with package and letter bombs. If scan equipment is used, it needs to be positioned in a location that if damaged by a possible explosion, will not cause heavy collateral damage to other areas. Access to the equipment by emergency response agencies should be quick and easy. Meet with emergency agencies to establish these procedures. Train designated mail and security people in every phase of mail processing, delivery and emergency contact methods. If possible, make emergency calls with special telephone numbers to avoid traffic interception of 911 calls by the news media and others who may be lis-