Security Executive Council

RISK MANAGEMENT PORTFOLIO

Workplace Security Playbook

The New Manager's Guide to Security Risk

Bob Hayes, Contributing Editor

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals

The first step is an assessment of your current environment. What needs improving? What are Security's fixed conditions? What recent changes have impacted Security, such as new business directions, new stakeholders, or a merger or acquisition?

An SEC team made up of former CSOs will engage with you to identify the key risks and determine the continuum of desired outcomes depending on your conditions. We map the solution to your C4R – current circumstances, conditions, culture and resources.

Once we understand the issues and potential barriers, we search our extensive security knowledge base for resources or research data that can be used as a base or to kickstart direction ideas.

Next, our subject matter experts bring their varied experiences and knowledge together to create a plan to help you reach your desired outcome. We call this Collective Knowledge™.

We help determine which other functions the plan should touch and align with. We use the SEC's Unified Risk Oversight™ model to help plan and communicate the value of cross-functional collaboration.

We assist in communicating the value of the project to the business leader accountable for Security's new vision. This in turn assists in communicating the strategy to senior executives from other functions.

Business value metrics are developed for the client team to measure and determine project success for the organization, including key stakeholders.

Last, clients can either take the SEC deliverables and run with them, or we can guide you through the implementation of your plan. At the end of the day, **the SEC is here to help you succeed.**

The SEC Process Outcome: Security Leader and Program Success

Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

First published 2013

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-417245-6

CONTENTS

Executive Summary vii
Introduction ix

Chapter 1 Security Performance Guidelines 1
1.1 Performance Guidelines vs. Standards 1
1.2 Three-Step Decision-Making Process 2
1.3 Performance Guidelines 3

Chapter 2 Elements of a Facility Security Program 9
2.1 Employee Awareness 9
2.2 Security Coordinator 11
2.3 Security Committee 12

Chapter 3 Surveys and Validations 15
3.1 Security Surveys 15
3.2 Validation Testing 16
3.3 Types of Validations 17

Chapter 4 Investigation Guidelines 19
4.1 Goals of an Investigation 19
4.2 Reporting to Law Enforcement 19
4.3 Document All Information 20
4.4 Legal Rights 21
4.5 Investigative Records and Evidence 21
4.6 Investigative Resources 22
4.7 Voluntary Statements 22
4.8 Surveillance 24
4.9 Warrants and Subpoenas 24
4.10 Polygraphs 25

Chapter 5 Inspection Guidelines 27
5.1 General Inspection Guidelines 28
5.2 Inspections Based on Reasonable Suspicion 32
5.3 Inspections Based on Generalized Suspicion 36
5.4 Refusal to Cooperate in an Inspection 44

Chapter 6 Emergency Procedures 47
6.1 Types of Emergencies 47
6.2 Security Concerns 47
6.3 Managing with a Plan 48
6.4 Reporting 49
6.5 Evacuation 49
6.6 Bomb Threats 50
6.7 Civil Disturbances and Demonstrations 52
6.8 Natural Disasters 57
6.9 Strikes and Labor Disturbances 60
6.10 Medical Emergencies 63

Chapter 7 Special Security Situations 65
7.1 Contractors, Vendors, Temporary Employees, and Interns 65
7.2 Construction Security 67
7.3 Vacant Properties 70
7.4 Special Events 73

Chapter 8 Security Management Resources 75
8.1 Training and Education 75
8.2 Professional Associations 76
8.3 Trade Publications 76
8.4 Books 77

Chapter 9 Implementing Your Security Program 79
9.1 Coordinators 79
9.2 Security Committee 79
9.3 Employee Awareness 80
9.4 Information Security 80
9.5 Access Controls 80
9.6 Security Officers 82
9.7 Security Surveys 83
9.8 Reporting 84
9.9 Investigations and Inspections 84
9.10 Emergency Plans and Contacts 85
9.11 Special Security Requirements 87

About the Contributing Editor 89
About Elsevier's Security Executive Council Risk Management Portfolio 91

CHAPTER 6

Emergency Procedures

The effectiveness of your actions in an emergency depends on how well you have developed emergency plans. Your plans should cover three phases:

1. Responding immediately
2. Controlling the situation and finding a remedy for it
3. Returning to normal business operations

6.1 TYPES OF EMERGENCIES

An emergency is any situation that could result in an immediate safety or health threat to a person, or in damage to property or the environment. This situation can result from a variety of accidental or intentional causes:

- Criminal and security-related incidents that escalate to a local emergency, such as bomb threats, arson, sabotage, civil strife, or property destruction
- Serious injury or illness
- Property damage from fire or explosion
- Environmental discharge accidents, such as chemical spills or leaks
- Natural disasters, such as floods, tornadoes, earthquakes, and winter storms
- Conditions that require a shutdown of operations, such as a roof collapse
- Incidents of potentially high community interest

6.2 SECURITY CONCERNS

Safety is a primary concern in emergencies, but these situations also raise immediate security issues, including the following:

- Appropriate staffing of security officers
- Alarm service and emergency response
- Site and scene protection

- Property and information protection
- Law enforcement contact and coordination
- Emergency vehicle access
- Crowd control
- Special access controls for extended situations

6.3 MANAGING WITH A PLAN

A formal plan can help you manage and control emergency situations. Much of your plan may focus on safety issues, but there will also be some important security components (which your corporate security department could help you with, if applicable). Emergency planning is a seven-step process, as described below.

6.3.1 Step 1: Examine Your Vulnerability

Examine the likelihood of various emergencies and your vulnerability to them. Identify the situations that could have a sudden and negative impact on your operations.

6.3.2 Step 2: Prepare Your Plans

Plan for the emergencies that are most likely to occur.

If possible, reduce the probability that the emergencies will occur. Determine who will make what decisions under what circumstances. Establish an emergency center or other location where information will be channeled and decisions made.

Train an emergency response team appropriate to each emergency:

- Spill team
- First responders
- CPR units
- Computer and data recovery team
- Written records recovery team
- Boiler recovery team

Identify alternate means of communication, and define the conditions that will require evacuation or relocation of your operations.

6.3.3 Step 3: Ensure Recovery of Operations

An organized recovery of operations depends on continuity of management and critical functions. Identify your primary and alternate

sources for critical materials and spare parts. Plan for the preservation and recovery of essential records.

6.3.4 Step 4: Coordinate the Plan

Discuss the plans with all concerned groups in your facility, and with any outside agencies you may need to call on to help verify your assumptions. If your plan depends on police and fire support, contact them to make sure of their cooperation.

6.3.5 Step 5: Test the Plan

Testing your plan will help you sort out any problems and will also prepare your employees for a real emergency. You can test your plan in stages or through a full participation exercise.

6.3.6 Step 6: Implement the Plan

In an actual emergency, stick to your plans as closely as possible. It is especially important that decision makers get timely and accurate information in order to assess the situation. Contain the situation as quickly as possible, and begin recovery operations as soon as the emergency is under control.

6.3.7 Step 7: Evaluate the Plan

Evaluate your plans thoroughly and objectively after each test. After a real emergency, perform an evaluation as soon as possible after you resume normal operations.

6.4 REPORTING

When an emergency arises, notify your company's management team as soon as possible. After the emergency has been handled, you should write a formal written report. After completing the report, be sure to forward it to management for their records. Some of the forms you also may need to complete are: injury reports, fatality reports, and Environmental Protection Agency (EPA) reports.

6.5 EVACUATION

Emergencies may sometimes require an evacuation of your facility. It's important that you identify the circumstances that will require an evacuation, and that you establish and practice evacuation procedures.

Specific evacuation procedures may differ in various emergencies, but your planning should consider these general guidelines:

- Determine who can order an evacuation. Public authorities such as police, fire, health, civil, and EPA officials always have this authority, but you should determine which members of your management may declare an evacuation.
- Determine in advance what circumstances or conditions would require an immediate evacuation.
- Determine the evacuation signals and other means of communications you will use.
- Plan evacuation routes carefully so that employees are not directed through or near hazardous areas.
- Prominently display evacuation routes and instructions throughout your facility. Mark emergency exits clearly.
- Post warnings on elevators advising that they should not be used during an evacuation.
- Designate employees to monitor specific posts in the facility, guide employees, and make final sweeps to ensure that their areas are clear. Select people who are generally available, and who can provide calm, authoritative leadership. Designate alternates, and update the monitor rosters frequently.
- Establish waiting areas outside the facility. This will help you account for all people and keep employees at a safe distance from the facility and out of the way of emergency equipment and personnel. Designated waiting areas are also useful when you need to communicate further instructions to the employees.
- Do not allow employees to re-enter the site for any reason until management or the public authorities determine it is safe.

6.6 BOMB THREATS

Awareness and planning can do much to reduce the tension and confusion that accompany a bomb threat. According to the Federal Bureau of Investigation (FBI), in 95 percent of bomb threats no device is ever found. On the other hand, most actual bombing incidents are not preceded by any type of warning. Despite these statistics, you should make plans to deal with bomb threats on a case-by-case basis.

6.6.1 Planning

An important part of planning is to contact your local police department (and your local military resources if that is recommended or if no local police are available). Determine the conditions under which your local police or military resources will help you search the facility. They may be able to provide you with dogs trained in such searches, as well as expert help in identifying and removing devices.

6.6.2 Phone Threats

Because most bomb threats are received by phone, the people who handle your incoming calls should be instructed to do the following:

- Remain calm.
- Ask what particular facility is being threatened.
- Ask what time the device is set for.
- Ask specifically where the bomb is located.
- Ask why the caller is taking this action.
- Record any background noise, unusual voice characteristics, or speech mannerisms.
- Record the date and time of the call and which phone number it came in on.
- Tell only designated managers about the call.

6.6.3 Assess Credibility

When there is a bomb threat, the first thing you need to do is assess the threat's credibility and determine whether further action is needed. Calls that are short and nonspecific generally do not have sufficient credibility to merit an extraordinary response on your part, but you should always document the incident and report it to management or your corporate security department.

Calls that are long, contain specific about the type of device, and touch on specific grievances deserve further consideration.

You should also consider whether the caller could have gained access to place the device, and if conditions in the facility or the surrounding community are likely to produce an actual bombing.

If you determine the threat is credible, you may need to consider several additional factors. Do you have the time and resources to conduct a search first? Does the nature of your business include any critical

operations (handling hazardous chemicals, for example) that would require immediate evacuation? The credibility of the threat and your assessment of these issues will help you determine whether evacuation is necessary.

In addition to whatever assistance your local law enforcement and military resources can provide, you may also have to form volunteer employee search teams. Volunteers should be assigned to search areas they are familiar with, beginning with the most accessible areas and ending with the least accessible.

If a suspicious device is found, search team members must not touch it, but should contact management and report its location and appearance. They should then shut down any machinery in the area and depart immediately. Notify the authorities if they are not already on the scene. Do not let anyone reenter the building until authorities consider it safe.

For a visual summary of the information in this section, see the model for responding to bomb threats (Figure 6.1).

6.6.4 Bomb Threat Search Diagrams

In Figure 6.2, you'll see that bomb searches should be conducted according to specific procedures to ensure thorough and accurate coverage of all locations in your company's building(s). The top diagram illustrates the pattern with which each room should be swept: search teams should be broken up, and then cover the room in two groups. The bottom diagram illustrates the three levels of search that should be performed in each room:

- Level One: the area from the floor to the searcher's waist
- Level Two: the area starting at the searcher's waist and ending at the top of the searcher's head
- Level Three: the area from the top of the searcher's head to the ceiling

6.7 CIVIL DISTURBANCES AND DEMONSTRATIONS

Frequently viewed as a product of 1960s and 1970s social movements, demonstrations continue to be a means of expression about any number of valid issues, such as abortion, apartheid, the environment, and nuclear weapons. The primary objective of demonstrators is usually media

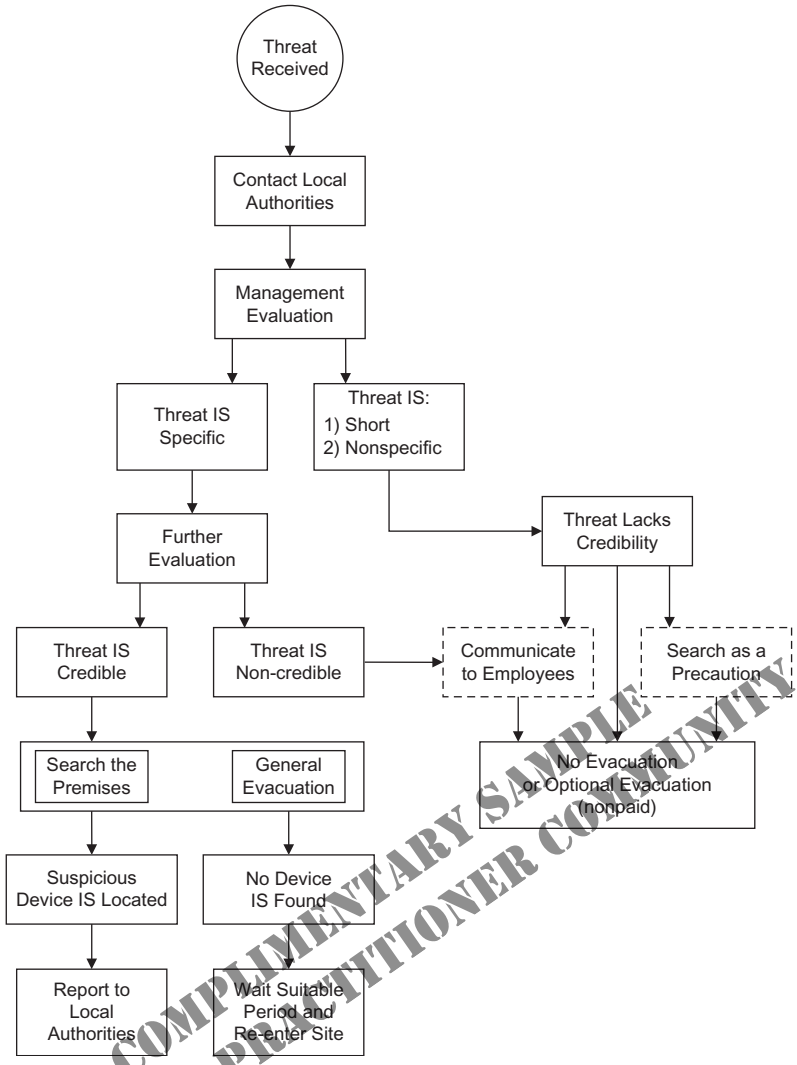

Figure 6.1 This bomb threat response model will help you follow the specific procedures for responding to bomb threats called in to your company, including: notification of appropriate parties (law enforcement, management, employees); determining whether the threat is credible; ordering employee evacuations; and searching company property for the bomb device.

attention; communicating with the company is often secondary. Related objectives may include getting arrested by trespassing on company property, engaging the company in public debate, conveying a message directly to employees, or, occasionally, inciting physical confrontation.

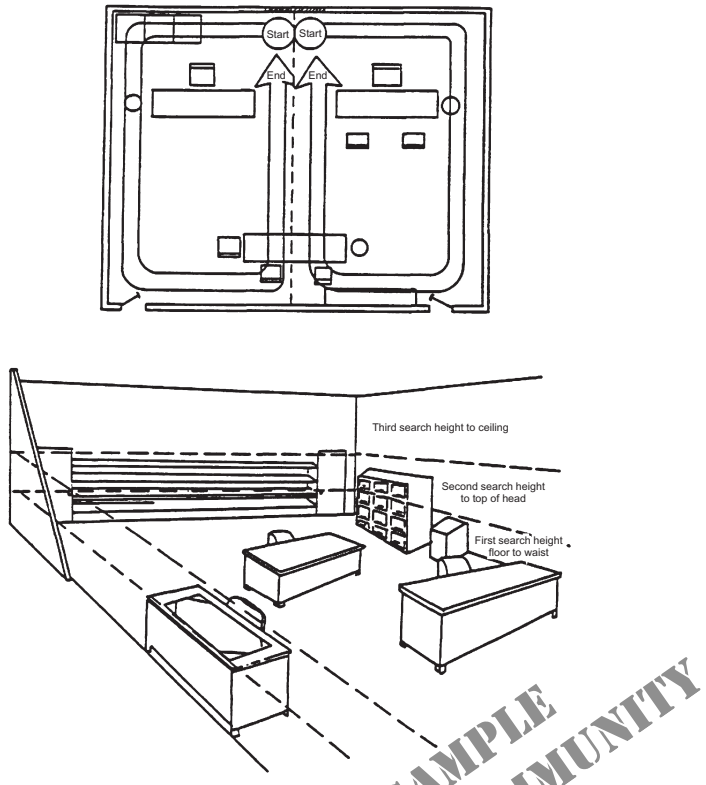

Figure 6.2 The two diagrams in Figure 6.2 demonstrate the procedure for proper bomb searches. Rooms should be divided among the search volunteers (top diagram), and should be searched beginning with the floor and ending with the ceiling (bottom diagram).

Every organization should prepare and implement a demonstration plan (to be incorporated into the overall security plan) for handling demonstrations on or near company property. As the person responsible for the safety of company employees and assets, you should make sure to communicate in your demonstration plan that company grounds are private property maintained for the use of company employees, customers, vendors, and guests. Use of company premises for demonstrations interferes with the normal conduct of business and is, therefore, not allowed.

The best defense in the case of demonstrations is to be aware of conditions in your community and make sure you are notified of any actions that could affect operations. Your public relations department and other governmental and business sources can also keep you informed.

6.7.1 Building a Demonstration Plan

The objectives of your plan should be to

- Avoid injuries to individuals and damage to property;
- Prevent harassment of employees and interruption of work;
- Minimize the possibility of confrontation and arrest;
- Correctly state your company's position on the issue;
- Maintain effective relations with the news media and public officials; and
- Avoid potential legal problems.

As you build a demonstration plan, remember to perform the following nine steps:

1. Review company policy and applicable local ordinances and laws with local law enforcement officials.
2. Confirm the boundary lines between company and public property.
3. Negotiate with local law enforcement officials for an acceptable public area to allow demonstrations. Try to select an area near a vantage point, such as a window, from which you can photograph the event but not be observed.
4. You might consider purchasing video cameras and recorders to document the entire event. At a minimum, have a camera available.
5. Evaluate perimeter and access controls to the facility, and modify procedures if additional access control is needed.
6. Designate a security coordinator or other manager to be the initial contact with the demonstration leaders.
7. Select a room where company representatives and the demonstration leaders could meet if necessary, and a room for news media briefings.
8. Establish a notification list. This should include anyone who may need to know about potential or actual demonstrations (i.e., business unit managers, company management, or local officials).
9. Make sure that your colleagues involved with security operations are briefed on how to handle demonstrators.

6.7.2 Task Force Responsibilities

If your company is a part of a larger corporation, demonstrations or protests will require a coordinated response by facility management (you), division or subsidiary management, and corporate staff. This coordination is the responsibility of a task force that consists of the

persons in charge of administration, corporate quality and manufacturing services, and public relations. The task force determines policy and provides guidance and any corporate assistance to the facility. Selected representatives of affected staff departments or divisions will advise the task force, implement its policy decision, and act in place of the task force if its members are not immediately available.

6.7.3 Assess Impact

When you hear about a potential disturbance, you must assess its probable impact on operations. Consider these factors:

- How serious or widespread will the disturbance be?
- Will employee access to the facility be hampered? Can you arrange alternate routes and modes of transportation?
- Are perimeter safeguards adequate to protect the facility? What steps can you take to protect vulnerable areas?
- Will supplemental security patrols be needed?

6.7.4 Reporting

Immediately report any warning or actual organizing or gathering of a demonstration to your local management and/or your corporate security department. These groups will notify the appropriate departments, including the office of general counsel. These departments might also send observers or other assistance to the scene if necessary.

6.7.5 Local Management Response and Control

As the company representative at the scene, you should take charge of the situation and be the main contact with demonstrators, the police, and other company groups. Specifically, you should adhere to the following guidelines for responding to a demonstration:

- If applicable, keep corporate security informed.
- Keep local police advised of the situation. Request their assistance to monitor or control the situation if necessary.
- Keep employees informed. Recommend they avoid contact or confrontation with demonstrators.
- Follow the established publicity procedures for emergency situations. If you are contacted by reporters, ask them who they represent and exactly what they need to know, and tell them that you or another qualified person will call them back. Then contact a public relations representative about handling the reply.

- Do not allow the demonstrators to use any company facilities, either buildings or parking.
- No company employee or security manager should physically contact or try to arrest demonstrators. Leave arrests to local law enforcement officers.
- The security coordinator or designated company representative should make sure the event is being videotaped or photographed to supplement written reports. The person with the camera should record the event from a vantage point where it's possible to maintain a low profile.
- Consult with the demonstration task force or designated representatives as appropriate.

Your company's public relations representative or group is responsible for contact with the news media and community officials, and for communications with the demonstrators regarding the company's position on the issue.

Public relations is also responsible for advising and assisting facility management on communications with the news media, employees, demonstrators, and community officials, or sending a representative or arranging public relations assistance for local management as appropriate.

Public relations should also prepare any official company statements to the news media and employees.

6.7.6 Debriefing

In conjunction with other managers and staff departments, always review and evaluate your actions and response with the task force once the demonstration has ended.

6.8 NATURAL DISASTERS

6.8.1 Communications

Communications can be a critical factor in any natural disaster. It's important to be prepared for an interruption of normal lines of communication. For example, if land phone lines are down, you can try using a wireless phone. If neither of those are working, sometimes text messaging or email will still work. In recent years, communication through the use of social media (i.e., Facebook or Twitter) has been a critical way that individuals and companies affected by a natural

To purchase the complete Workplace Security Playbook, visit
https://www.elsevier.com/books/workplace-security-playbook/hayes/978-0-12-417245-6