CONTENTS

Preface xxii
Acknowledgments xxv

SECTION I: RISK ANALYSIS

Chapter 1 Risk Analysis — The Basis for Appropriate and Economical Countermeasures 3
Introduction 3
Critical Thinking 5
Qualitative versus Quantitative Analysis 5
Required Skills 6
Tools 8
Theory, Practice, and Tools 8
Theory 12
Practice 13
Tools 15
Organization 16
Summary 17

Chapter 2 Risk Analysis Basics and the Department of Homeland Security—Approved Risk Analysis Methods 19
Introduction 19
Risk Analysis for Facilities and Structures 20
Many Interested Stakeholders and Agendas 22
Commercially Available Software Tools 24
Risk Analysis Basics 25
Risk Assessment Steps 27
DHS–Approved Risk Assessment Methodologies 29
Which Methodology to Use? 31
Community versus Facility Methodologies 31
Strengths and Weaknesses of Major Methodologies 31
Summary
Risk Analysis for Facilities and Structures 33
Many Interested Stakeholders and Agendas 33
Commercially Available Software Tools 34
Risk Analysis Basics 34
Risk Assessment Steps 34
Which Methodology to Use? 35

Chapter 3  Risk Analysis Skills and Tools 37
Introduction 37
Skills 39
Skill #1: Gathering Data 40
Get the Organization’s Mission Statement 41
Understand the Organization’s Programs (Business Units) 41
Assets by Classification 42
Existing Countermeasures 43
Skill #2: Research and Evidence Gathering 44
Interviews 44
Internet Research 46
Telephone Research 49
Records Research 49
Surveys 49
Asset Classifications 50
Historical Data Relating to Security Events 50
Criticalities and Consequences Assessments 51
Bibliography Building 51
Countermeasure Research 52
Skill #3: Critical Thinking in the Risk Analysis Process 53
Skill #4: Quantitative Analysis 53
Skill #5: Qualitative Analysis 54
Converting Quantitative Data into Qualitative Data 55
Skill #6: Countermeasure Selection 55
Countermeasure Selection 55
Cost-Benefit Analysis 56
Skill #7: Report Writing 56
Tools 56
Commercially Available Software Tools 57
Chapter 6  Criticality and Consequence Analysis

Introduction
Twofold Approach
Criticality
Consequence Analysis
Building Your Own Criticality / Consequences Matrix
Criticality / Consequence Matrix Instructions
Summary
   Criticality
   Consequence Analysis

Chapter 7  Threat Analysis

Introduction
Theory
   Threats versus Hazards
   All Hazards Risk Analysis
   Design Basis Threat
Practice
Tools
   Adversary / Means Matrix
Summary
   Design Basis Threat
   Practice
   Tools

Chapter 8  Assessing Vulnerability

Introduction
Review of Vulnerability Assessment Model
Chapter 9  **Estimating Probability**  161

Introduction  161

Basic Risk Formula  161

Likelihood  161

Terrorism Probability Estimates and Surrogates  162

Resources for Likelihood  163

Viewing the Range of Possible Threat Actors  163

Criminal versus Terrorism Likelihood Resources  166

General Comparison for Resources  166

Terrorism Asset Target Value Estimates  166

Criminal Incident Likelihood Estimates  168

Criminal Statistics  168

Economic Crime Asset Target Value Estimate  169
Nonterrorism Violent Crime Asset Target Value Estimate 169
Petty Crimes Asset Target Value Estimate 171
Summary 171
Likelihood 171
Terrorism Asset Target Value Estimates 172
Criminal Incident Likelihood Estimates 173
Criminal Statistics 173
Economic Crime Asset Target Value Estimate 173
Nonterrorism Violent Crime Asset Target Value Estimate 173
Petty Crimes Asset Target Value Estimate 174

Chapter 10 The Risk Analysis Process 175
Introduction 175
Objective 175
Examples 176
Displaying Risk Formula Results 177
The Complete Risk Analysis Process 178
Probability Factors 180
Vulnerability Factors 181
Consequence Factors 181
The Risk Analysis Process 181
Probability Factors 181
Diagram Analysis 183
Asset Target Value Matrices 184
Probability Summary Matrix 186
Vulnerability Components 186
Vulnerability Tools 187
Consequence Components 188
Risk Formulas 189
Risk Results (Unranked) 189
Summary 191
Displaying Risk Formula Results 191
The Complete Risk Analysis Process 191

Chapter 11 Prioritizing Risk 193
Introduction 193
Prioritization Criteria 193
Natural Prioritization (Prioritizing by Formula) 194
SECTION II: POLICY DEVELOPMENT BEFORE COUNTERMEASURES

Chapter 12 Security Policy Introduction

Introduction

The Hierarchy of Security Program Development

What Are Policies, Standards, Guidelines, and Procedures?

Other Key Documents

The Key Role in Policies in the Overall Security Program

Policies Define All Other Countermeasures

Legal Challenges

Challenges by Users

Benefits to Having Proper Policies

Control Factors

Summary

The Hierarchy of Security Program Development

Policies, Standards, Guidelines, and Procedures

The Key Role in Policies in the Overall Security Program

Control Factors
Chapter 13  Security Policy and Countermeasure Goals  215

Introduction  215
Theory  215
The Role of Policies in the Security Program  217
The Role of Countermeasures in the Security Program  217
Why Should Policies Precede Countermeasures?  221
Security Policy Goals  222
Security Countermeasure Goals  223
Policy Support for Countermeasures  224
Key Policies  224
  Authorities and Responsibilities  224
  Protection of Life  225
  Special Countermeasures Example  225
  Crime Prevention  227
  Access Control Program  228
  Asset and Property Protection  229
  Individual Responsibilities for Security  229
  Guards  229
  VIP Protection Program  230
  Emergency Security Plans  231
Summary  231
  The Role of Policies in the Security Program  232
  The Role of Countermeasures in the Security Program  232

Chapter 14  Developing Effective Security Policies  235

Introduction  235
Process for Developing and Introducing Security Policies  235
  Triggers for Policy Changes  235
  Policy Request Review  236
  Policy Impact Statement  236
  Subject Matter Expert and Management Review Process  237
Policy Requirements  238
Basic Security Policies  238
Security Policy Implementation Guidelines  239
Regulatory-Driven Policies  240
Nonregulatory-Driven Policies  242
Summary  244
**SECTION III: COUNTERMEASURE SELECTION**

**Chapter 15  Countermeasure Goals and Strategies**

<table>
<thead>
<tr>
<th>Countermeasure Goals and Strategies</th>
<th>249</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>249</td>
</tr>
<tr>
<td><strong>Countermeasure Objectives, Goals, and Strategies</strong></td>
<td>250</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>250</td>
</tr>
<tr>
<td><strong>Deterrence</strong></td>
<td>252</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>252</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>252</td>
</tr>
<tr>
<td><strong>Detection</strong></td>
<td>253</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>253</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>254</td>
</tr>
<tr>
<td><strong>Surveillance Detection</strong></td>
<td>254</td>
</tr>
<tr>
<td><strong>Attack Detection</strong></td>
<td>254</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>255</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>256</td>
</tr>
<tr>
<td><strong>Response (Including Delay)</strong></td>
<td>257</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>257</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>257</td>
</tr>
<tr>
<td><strong>Evidence Gathering</strong></td>
<td>258</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>258</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>258</td>
</tr>
<tr>
<td><strong>Comply with the Business Culture of the Organization</strong></td>
<td>259</td>
</tr>
<tr>
<td><strong>Goal</strong></td>
<td>259</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>260</td>
</tr>
<tr>
<td><strong>Minimize Impediments to Normal Business Operations</strong></td>
<td>260</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>260</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>260</td>
</tr>
<tr>
<td><strong>Safe and Secure Environments</strong></td>
<td>261</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>261</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>261</td>
</tr>
</tbody>
</table>
Design Programs to Mitigate Possible Harm from Hazards and Threat Actors 261
Summary 263

Chapter 16 Types of Countermeasures 265
Introduction 265
Baseline Security Program 265
  Typical Baseline Security Program Elements and Implementation 266
    Program Elements 266
  Designing Baseline Countermeasures 267
Specific Countermeasures 268
Countermeasure Selection Basics 269
  Hi-Tech Elements 269
    Access Control Systems 269
    Detection Systems 276
    Consoles and Management Offices 288
    Security System Archiving Technologies 288
    Security System Archiving Schemes 290
    Security System Infrastructures 291
  Lo-Tech Elements 294
    Locks 294
    Revolving Doors 295
    Mechanical and Electronic Turnstiles 295
    Vehicle Gates 296
    Deployable Barriers 296
    Lighting 297
    Signage 297
  No-Tech Elements 298
    Define the Deterrence Program 298
    Define the Response Program 302
    Define the Evidence-Gathering Program 304
Summary 304
  Baseline Security Program 305
  Specific Countermeasures 305
  Countermeasure Selection Basics 305

Chapter 17 Countermeasure Selection and Budgeting Tools 307
Introduction 307
  The Challenge 307
<table>
<thead>
<tr>
<th>What Metrics Can Be Used to Determine Cost-Effectiveness?</th>
<th>346</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicating Priorities Effectively</td>
<td>349</td>
</tr>
<tr>
<td>Making the Case</td>
<td>349</td>
</tr>
<tr>
<td>Basis of Argument</td>
<td>351</td>
</tr>
<tr>
<td>Countering Arguments</td>
<td>352</td>
</tr>
<tr>
<td>Complete Cost-Effectiveness Matrix</td>
<td>353</td>
</tr>
<tr>
<td>Complete Cost-Effectiveness Matrix Elements</td>
<td>353</td>
</tr>
<tr>
<td>Security Program Recommendations Summary Board</td>
<td>355</td>
</tr>
<tr>
<td>Vertical and Horizontal Elements</td>
<td>355</td>
</tr>
<tr>
<td>Vertical Elements</td>
<td>355</td>
</tr>
<tr>
<td>Horizontal Elements</td>
<td>357</td>
</tr>
<tr>
<td>Risk Descriptions</td>
<td>357</td>
</tr>
<tr>
<td>Countermeasure Options and Cost Elements</td>
<td>357</td>
</tr>
<tr>
<td>Countermeasure Mitigation Values</td>
<td>357</td>
</tr>
<tr>
<td>Risk Rankings and Budgets</td>
<td>357</td>
</tr>
<tr>
<td>Phase Recommendations and Phasing Budgets</td>
<td>361</td>
</tr>
<tr>
<td>Budget Breakdowns by Phases and Risks</td>
<td>361</td>
</tr>
<tr>
<td>Summary</td>
<td>365</td>
</tr>
<tr>
<td>The Limitations of Cost-Effectiveness Metrics</td>
<td>365</td>
</tr>
<tr>
<td>Cost-Effectiveness Metrics</td>
<td>366</td>
</tr>
<tr>
<td>Communicating Priorities Effectively</td>
<td>366</td>
</tr>
<tr>
<td>Making the Case</td>
<td>366</td>
</tr>
</tbody>
</table>

**Chapter 20  Writing Effective Reports**  
 367

<table>
<thead>
<tr>
<th>Introduction</th>
<th>367</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation</td>
<td>368</td>
</tr>
<tr>
<td>Graphics</td>
<td>368</td>
</tr>
<tr>
<td>Preparation for a Successful Presentation</td>
<td>369</td>
</tr>
<tr>
<td>The Comprehensive Risk Analysis Report</td>
<td>371</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>371</td>
</tr>
<tr>
<td>Introduction</td>
<td>371</td>
</tr>
<tr>
<td>Assessment Process</td>
<td>372</td>
</tr>
<tr>
<td>Facility Characterization</td>
<td>372</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>373</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>374</td>
</tr>
<tr>
<td>Asset / Attack Matrix</td>
<td>375</td>
</tr>
<tr>
<td>Threat / Target Nexus Matrix</td>
<td>375</td>
</tr>
</tbody>
</table>