

Thomas L. Norman, CPP/PSP/CSC

Risk Analysis and Security Countermeasure Selection



CRC Press
Taylor & Francis Group

Risk Analysis and Security Countermeasure Selection

Risk Analysis and Security Countermeasure Selection

**Thomas L. Norman
CPP/PSP/CSC**



CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2010 by Taylor and Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number: 978-1-4200-7870-1 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Norman, Thomas, CSC.

Risk analysis and security countermeasure selection / Tom Norman.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-4200-7870-1 (hbk. : alk. paper)

1. Security systems. 2. Business enterprises--Security measures. 3. Office buildings--Security measures. 4. Computer security. 5. Risk assessment. I. Title.

HV8290.N67 2010

658.4'7--dc22

2009040274

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Dedication

This book is dedicated to the more than 179 people who lost their lives and over 350 who were injured by 10 terrorists in Mumbai, India. The attack began on November 26, 2008, from land and sea and was finally put down on November 29, 2008. Included in the list of those killed was the Chief of Mumbai's Anti-Terror Squad, Hemant Karkare. The attacks were a series of coordinated terrorist attacks carried out across Mumbai, India's largest city. Attack sites included Chhatrapati Shivaji Terminus, the Oberoi Trident Hotel, the Taj Mahal Palace and Tower, the Leopold Café, Cama Hospital, the Orthodox Jewish-owned Nariman House, the Metro Cinema, and areas outside the Times of India Building at St. Xavier's College. There was also a taxi blast at Vile Parle and an explosion at the Mazagaon docks in Mumbai's port area.

The 10 attackers used simple methods, tactics, and weapons (a moving shooter attack) to kill and injure a large number of people. The attack had been predicted for days. The attack took place during the run-up to the Indian Parliamentary election cycle.

Although the attack exposed many shortcomings in the Mumbai public security apparatus, there were also great examples of heroism from these fine people.

This was particularly painful for the community, because it shook the Indian psyche and destroyed the feeling of safety and security that had been painstakingly built over several years since several previous major attacks in Mumbai in 2003.

The perpetrators of this horrible crime were spawned by Lashkar-e-Taiba (LeT), a foreign terrorist organization (FTO) operating from within Pakistan, with training and planning help from Al Qaeda, based upon statements by Ajmal Amir, the only terrorist who was captured alive. Some of the attackers came from Pakistan and hijacked an Indian fishing vessel to avoid waterway security.

The immediate goals of the attack were to destroy the Indian community's faith in their security apparatus; undermine the existing Indian regime; destabilize relations between India and Pakistan; encourage the election of more militant Indian Parliamentarians with an eye toward further destabilizing Indo/Pakistan relations; cause India to put pressure on the moderate Pakistani regime with a goal toward undermining their popularity within Pakistan, leading toward regime change in Pakistan; and to get Pakistan to move its troops from the western borders, where they had been fighting against the Taliban and Al Qaeda to strengthen its eastern border with India in anticipation of clashes there, thus relieving the pressure that both Pakistan and the United States had put on the Taliban and Al Qaeda. The long-term strategic goals appear to be creating chaos and possibly anarchy inside Pakistan in order to effect regime change and thus pave the way to create a Taliban-like regime that would gain access to nuclear weapons by the terrorist organizations for use against India and the West.

(Note: Subsequent to writing this Dedication, the Taliban has indeed commenced a strategic push against the Pakistani regime which, as I write now, is being opposed by

a major operation by the Pakistani military, displacing tens of thousands in the Federally Administered Tribal Areas [FATA], the Swat Valley, and in Waziristan.)

I had completed a risk assessment for a major Indian firm only 2 months earlier that predicted that exactly this kind of attack could take place, as my number one concern.

Effective countermeasures exist for this and numerous other types of terrorist attacks. In the case of moving shooter attacks, the countermeasures are focused on deterrence and active intervention using reactive electronic automated protection systems (REAPSs) to contain the attack and the attackers, thus reducing the possible number of victims and rendering the attackers immobile and thus easy targets for rapid action forces. These should also be coupled with off-site command and control capabilities for any tier 1 terrorist target, which render control of the security system away from the terrorists and give it instead to Special Operations Police Units. (REAPSs are described in detail in my second book *Integrated Security Systems Design* [Butterworth-Heinemann, 2007]. REAPS elements should be accompanied by a commissioning regime of the security system that denies the attackers access to it (which they used effectively to counter police and military responders) and provide that resource remotely to the responders and not the attackers.

There are lessons to be learned from every terrorist attack. The chief lesson from the November 2008 Mumbai attacks is that it is of paramount importance to leave physical, electronic, and operations security to knowledgeable antiterrorism professionals and not to technical firms that may understand electronics but which have no expertise in planning antiterrorism measures, especially when many lives depend on the quality of their ill-conceived and hopelessly inadequate recommendations made solely from the pinnacles of their modest knowledge. Having a risk analysis performed and countermeasures developed by unqualified firms is a risky affair with dreadful consequences.

We can do better than this.

Contents

Preface	xxi
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	32
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

Lesser Software Tools	58
Affordable Tool Examples	58
Summary	63
Tools	64
Chapter 4 Critical Thinking and the Risk Analysis Process	67
Introduction	67
Overview of Critical Thinking	67
The Importance of Critical Thinking	68
Analysis Requires Critical Thinking	70
The Eight Elements That Make Up the Thinking Process	71
The Concepts, Goals, Principles, and Elements of Critical Thinking	71
Critical Thinking Concepts and Goals	71
Principles	72
Elements of Critical Thinking	73
Purpose	73
The Question at Issue: Most Thinking Is about Problem Solving	74
Understand Our Own and Others' Points of View	74
Gather Assumptions	75
Gather Information	75
Examine the Implications and Possible Consequences Related to the Issue	76
Determine What Concepts, Theories, Definitions, Axioms, Laws, Principles, and Models Are Applicable to the Issue	77
Draw Interpretations and Inferences and Conclusions and Formulate Recommendations	77
Pseudo-Critical Thinking	78
Intellectual Traits	78
The Importance of Integrating Critical Thinking into Everyday Thinking	79
Applying Critical Thinking to Risk Analysis	80
More about Critical Thinking	80
The Root of Problems	81
Summary	81
Chapter 5 Asset Characterization and Identification	85
Introduction	85
Theory	85
Practice	85
Asset List	85
Asset Categorization	86

Interviews	87
Facility and Asset Lists	88
Research	90
Surveys	90
Tools	97
Summary	98
Theory	98
Practice	99
Facility and Asset Lists	99
Tools	99
Chapter 6 Criticality and Consequence Analysis	101
Introduction	101
Twofold Approach	101
Criticality	101
Consequence Analysis	103
Building Your Own Criticality / Consequences Matrix	104
Criticality / Consequence Matrix Instructions	104
Summary	108
Criticality	109
Consequence Analysis	109
Chapter 7 Threat Analysis	111
Introduction	111
Theory	111
Threats versus Hazards	111
All Hazards Risk Analysis	114
Design Basis Threat	124
Practice	124
Tools	128
Adversary / Means Matrix	129
Summary	138
Design Basis Threat	139
Practice	140
Tools	140
Chapter 8 Assessing Vulnerability	141
Introduction	141
Review of Vulnerability Assessment Model	141

Define Scenarios and Evaluate Specific Consequences	142
Asset / Attack Matrix	144
Threat / Target Nexus Matrix	146
Weapons / Target Nexus Matrix	147
Adversary Sequence Diagram Path Analysis	148
Surveillance Opportunities Matrix	150
Evaluate Vulnerability	152
Survey Points	152
Quantitative Analysis Matrices	153
Determine Accessibility	153
Identify Intrinsic Vulnerabilities	153
Natural Countermeasures	154
Evaluate Effectiveness of Existing Security Measures	154
The Vulnerability Calculation Spreadsheet	155
Qualitative Analysis Section	155
Vulnerability Detail Spreadsheet	157
Vulnerability Detail Matrix	157
Summary	157
Review of the Vulnerability Assessment Model	157
Define Scenarios and Evaluate Specific Consequences	159
Evaluate Vulnerability	159
The Vulnerability Calculation	160
Qualitative Analysis Section	160
Infiltration and Attack Vulnerabilities	160
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

Prioritization of Risk	194
Prioritizing by Probability	195
Prioritizing by Consequences	195
Prioritizing by Criticality	195
Prioritizing by Cost	195
Communicating Priorities Effectively	196
Making the Case	196
Best Practices Ranking Risk Results	197
Displaying the Ranked Results as a Visual Graphic	198
Summary	199
Prioritization Criteria	200
Natural Prioritization (Prioritizing by Formula)	200
Communicating Priorities Effectively	200
Making the Case	200
Best Practices — Ranking Risk Results	200
Displaying the Ranked Results as a Visual Graphic	201
Making the V ² Matrix	201

SECTION II: POLICY DEVELOPMENT BEFORE COUNTERMEASURES

Chapter 12 Security Policy Introduction	205
Introduction	205
The Hierarchy of Security Program Development	205
What Are Policies, Standards, Guidelines, and Procedures?	206
Other Key Documents	207
The Key Role in Policies in the Overall Security Program	208
Policies Define All Other Countermeasures	208
Legal Challenges	209
Challenges by Users	209
Benefits to Having Proper Policies	210
Control Factors	211
Summary	212
The Hierarchy of Security Program Development	212
Policies, Standards, Guidelines, and Procedures	212
The Key Role in Policies in the Overall Security Program	212
Control Factors	213

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

Process for Developing and Introducing Security Policies	244
Policy Requirements	244
Basic Security Policies	245
Security Policy Implementation Guidelines	245

SECTION III: COUNTERMEASURE SELECTION

Chapter 15 Countermeasure Goals and Strategies	249
Introduction	249
Countermeasure Objectives, Goals, and Strategies	250
Access Control	250
Deterrence	252
Goals	252
Strategies	252
Detection	253
Goals	253
Strategies	254
Surveillance Detection	254
Attack Detection	254
Assessment	255
Goals	255
Strategies	256
Response (Including Delay)	257
Goals	257
Strategies	257
Evidence Gathering	258
Goals	258
Strategies	258
Comply with the Business Culture of the Organization	259
Goal	259
Strategies	260
Minimize Impediments to Normal Business Operations	260
Goals	260
Strategies	260
Safe and Secure Environments	261
Goals	261
Strategies	261

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

Countermeasure Effectiveness	308
Functions of Countermeasures	308
Examples	308
Infiltration Scenarios	310
Attack Scenarios	310
Attack Objective Parameters	313
Criminal Violent Offender Types	313
Economic Criminal Types	314
Economic Criminal Objectives	314
Criminal Offender Countermeasures	315
Countermeasure Effectiveness Metrics	316
Functional Effectiveness	316
Helping Decision Makers Reach a Consensus on Countermeasure Alternatives	317
Summary	319
Chapter 18 Security Effectiveness Metrics	321
Introduction	321
Theory	321
Sandia Model	321
A Useful Commercial Model	323
What Kind of Information Do We Need to Evaluate to Determine Security Program Effectiveness?	328
What Kind of Metrics Can Help Us Analyze Security Program Effectiveness?	330
Adversary Sequence Diagrams	330
Vulnerability / Countermeasure Matrix	332
Security Event Logs	336
Patrol Logs (Vulnerabilities Spotting / Violations Spotting)	337
Annual Risk Analysis	337
Summary	337
A Useful Commercial Model	338
Useful Metrics	339
Security Event Logs	339
Patrol Logs	339
Annual Risk Analysis	339
Chapter 19 Cost-Effectiveness Metrics	341
Introduction	341
What Are the Limitations of Cost-Effectiveness Metrics?	342

What Metrics Can Be Used to Determine Cost-Effectiveness?	346
Communicating Priorities Effectively	349
Making the Case	349
Basis of Argument	351
Countering Arguments	352
Complete Cost-Effectiveness Matrix	353
Complete Cost-Effectiveness Matrix Elements	353
Security Program Recommendations Summary Board	355
Vertical and Horizontal Elements	355
Vertical Elements	355
Horizontal Elements	357
Risk Descriptions	357
Countermeasure Options and Cost Elements	357
Countermeasure Mitigation Values	357
Risk Rankings and Budgets	357
Phase Recommendations and Phasing Budgets	361
Budget Breakdowns by Phases and Risks	361
Summary	365
The Limitations of Cost-Effectiveness Metrics	365
Cost-Effectiveness Metrics	366
Communicating Priorities Effectively	366
Making the Case	366
Chapter 20 Writing Effective Reports	367
Introduction	367
Presentation	368
Graphics	368
Preparation for a Successful Presentation	369
The Comprehensive Risk Analysis Report	371
Executive Summary	371
Introduction	371
Assessment Process	372
Facility Characterization	372
Threat Assessment	373
Vulnerability Assessment	374
Asset / Attack Matrix	375
Threat / Target Nexus Matrix	375

Contents	xix
Weapon / Target Nexus Matrix	375
Surveillance Opportunities	375
Risk Calculation	376
Countermeasures	376
Baseline Security Program	377
Identifying Key Assets for Special Consideration	378
Develop Countermeasure Budgets	378
Countermeasure Implementation Recommendations	379
Report Supplements	379
Risk Register	379
Footnotes	380
Tables	380
Index and Glossary	380
Attachments	380
Countermeasure Budget Presentation	382
A Microsoft PowerPoint Presentation	382
Handouts for the Presentation	382
Summary	382
The Comprehensive Report	383
Countermeasures Budgets	383
PowerPoint® Presentation	383
Presentation	383
Graphics	383
Preparation for a Successful Presentation	384
Index	385

Preface

When people ask me how long I have been in security consulting, I usually tell them that I have been working in the security industry since before electricity. It has been over 35 years now. As an old guy, I have seen a lot of things. The security industry is simply fascinating. There are few human endeavors that bring together sociology, economics, psychology, technology, architecture, landscaping, project management, engineering, critical thinking game theory, and logic into one big bowl of soup. I love this industry.

I have watched the industry grow and mature from a general lack of awareness of security on the part of most of the public and corporate management to a current state where there is a heightened sense of security among many public and private sectors. Government has always been aware of security, as governments are prone to trying to protect themselves against all kinds of threats. Since September 11, 2001, I have seen a fundamental shift in security awareness that is at the same time refreshing, startling, and concerning.

I see a desire to look at security as more of a business unit, in a more professional and methodical way (that is good). There is also a tendency to treat every facility as a potential terrorist target, often wasting the organization resources on facilities that terrorists have no history of targeting and which do not fit the strategic objectives of any known terrorist organization (not so good). My kudos go to the New York City Police Department (NYPD) for their important work in this area.

Most organizations today want a risk analysis before committing resources to solutions (also good). However, the industry is now fraught with “consultants” who have little if any formal training or education and who often propose their company’s products or services as the obvious solution. Oddly, a single organization can go to several different security vendors (dogs, guards, systems, investigators) and get answers from each vendor — which is that it is the specific vendor’s products or services that the organization needs the most. This is not consulting. This is predatory behavior by self-interested vendors, which is above the interests of their clients. This is also not a display of any functioning concern for the lives of the people who dwell in the organization’s buildings. Uniquely, these firms who employ “consultants” with little or no real knowledge about risk almost always charge little or nothing for their consulting efforts, and it is easily worth the cost (little or nothing).

This is sad and unfortunate and I think almost criminal, as people’s lives and livelihoods are at great risk when poor risk analysis is employed. These organizations would not hire a physician, accountant, structural engineer, or architect without credentials, yet they will often hire anyone who has the word “consultant” on his or her business card, with no check of qualifications whatsoever.

Risk analysis is heady stuff. A good risk analysis is a marvelous thing. It enlightens, it informs, it educates, and it illuminates the vague into the clear. It helps management organize its thinking into clear and obvious action, properly prioritized, with precious

organizational resources spent on the least-cost, most-effective solutions. Poor risk analysis results in vague programs with no clear direction or purpose and no metrics for measurement. What other business unit could operate in such darkness?

I have read many books on risk analysis, but I have never read one “risk analysis” book that teaches the process of analysis.* All these books talk about security principles. Most discuss methodologies. Some teach how to conduct interviews and surveys, and write reports. I have not read one that teaches analytical skills. Perhaps there is one, but I have not seen it. I think a book on risk analysis should leave the reader understanding what analysis is and what it is not, and teach the ideas, principles, elements, and process.

There are many software tools to assist in risk analysis but only a few are analytical in nature. Most are checklists that leave a sense of protection while actually offering little insight into risk. Some of the software tools create vast lists that are impressive in weight but do not categorize, sort, or present the data in any meaningful way. Others are so scant that they can hardly be called tools at all. Still, they present themselves in the market as useful tools.

There are also a number of approved risk analysis methodologies. I have used many including the Central Intelligence Agency (CIA) model, models promoted by the U.S. Armed Forces, the U.S. Department of State (DOS), the Department of Justice (DOJ), the Federal Emergency Management Agency (FEMA), the Department of Homeland Security (DHS), and models created by Sandia National Labs, along with others. There are methodologies that are particular to specific industries — water departments, high-rise office buildings, oil/gas/chemical facilities, pipelines, railroads, bridges, government buildings, prisons, and so forth). The DHS has an evolving list of approved methodologies that apply to various types of facilities and industries, all of which are valuable.

It can be confusing for an aspiring security practitioner to try and learn all of these ideas, and to master even some of all the software tools and methodologies. So how is one to wade through all this and find the way? I have used both the great and small in my long career. I have read hundreds of security books, used software tools that cost thousands of dollars, and used tools that were free. I have found all somewhat useful and have learned much from each experience.

Years ago, when I first began consulting, I was confronted by various client accounting departments demanding that specific information be presented with my invoices. I found this time consuming, confounding, and downright unproductive to collect all this data and present it to each client according to their specific procedures. In many ways, the DHS-approved list of methodologies is much like that. All methodologies require much of the same information, presented in much the same way, but with slight variations in data collection, processing, and presentation.

I solved my accounting dilemma by looking at the worst case of what every client was asking for (including my most demanding client, an agency of the U.S. Government), and then I developed a time-keeping and accounting system that presented all the information they asked for, every time, for every invoice. I never received one complaint from any of my clients after that. As a result, my efficiency immediately increased because I no longer had to keep different time and expense records for each client. I spent less time doing more. It was an important lesson that has served me well in my career. Do the best for everyone, and one can do more for everyone with much less effort than creating a

* There is one book on “vulnerability” that does teach analysis: *Vulnerability Assessment of Physical Protection Systems* by Mary Lynn Garcia (Butterworth-Heinemann, Oxford, 2005). Mary Lynn Garcia is a light in the wilderness.

unique program for each. It is the commoditization of data services to the best advantage for stakeholders, clients, as well as the consultant.

Over the years, I have developed a process of risk analysis (not itself an actual methodology) that is scientific, methodical, extensively thorough, and one that I believe fits the requirements of every methodology approved by the Department of Homeland Security. Where most analysts consider perhaps a hundred points of analysis, this process considers many thousands. This process takes into account every requirement of every major risk analysis methodology and pretty much fulfills the requirements of them all. Thus, in one single approach, one can easily move from reviewing water facilities to liquefied natural gas (LNG) terminals, to retail malls, to airports, to hotels, to office towers, to entire cities. Over the years, I have developed a reputation as a consultant who produces astonishingly complete reports at highly competitive rates. I have been asked to teach this approach by other colleagues and have been pleased to do so. Even though most consultants diligently try to conceal their methods, I have always believed in teaching. After my second book *Integrated Security Systems Design* (Butterworth-Heinemann, 2007), which taught security-system design in a new, thorough, and comprehensible way, I received many requests by colleagues to write another book to present risk analysis in the same way.

This approach is both thorough and fast and can produce results that can usually fit the requirements of almost every major risk analysis methodology. In the same amount of time that others take to create mediocre work, you can easily produce a risk analysis that is unbelievably comprehensive. This methodology also produces the “Holy Grail” of budgeting. That is, it creates budgets that are prioritized by relative effectiveness and relative risk. It creates budgets that allow management to clearly see what and how to prioritize the organization’s assets in the most effective way. You can do this. By reading this book, you will learn what many security practitioners for many years thought was impossible—to produce a risk analysis that accurately estimates and presents risks of all threats and budgets that are supported by both effectiveness and cost-effectiveness calculations.

This book provides insight into threat actors of all types that is unavailable from any other single source. It is organized in a way that conveys meaning, not just information. You will learn more from this book than from any other book on the subject of risk analysis, including, and most importantly, how to actually perform risk analysis, a subject that one would think would be the keystone of every book on the subject but which for a number of reasons is simply missing from virtually every other risk analysis book.

This book will open your eyes not only to risk analysis but most likely to a whole new way of thinking.

Now, begin reading. Begin learning the amazing art of critical thinking and how to apply it to the very important task of risk analysis. Then, get ready to create the most comprehensive and easy-to-understand risk assessments you ever thought possible.

Acknowledgments

I am most thankful to my adopted home of Beirut, Lebanon, and my kindest business partners, Cheikh Nabil el Khazen and Adel Mardelli for 10 years of constant encouragement and support, especially for their support for my efforts toward perfection in the craft of risk analysis and security systems designs.

I am also grateful for my Houston, Texas, associate Michael Crocker, CPP/CSC, for the many opportunities he has created both in wonderful project experiences and career development. Crocker is Senior Vice President of two ASIS regions and handles it all with total aplomb. His insistence on excellence is always rewarding and inspiring.

I am also grateful to my Abu Dhabi colleague and friend, Ranjan Maini, whose focus on quality and encouragement is persistent and unending.

I am grateful for the review and guiding comments on the manuscript by John R. Dew, CPP, one of the Federal Bureau of Investigation's (FBI's) most interesting former Counterterrorism Task Force members; Harvey M. Stevens, PhD, CPP, CHSIII, President of Stevens Associates, Inc., a most extraordinary and versatile security consultant; Malcolm Nance, counterterrorism genius; Michael Crocker, CPP/CSC, Michael Crocker, CPP and Associates, Inc., what every security professional should aspire to be; and Ranjan Maini, APEX Security Consultants, Abu Dhabi, United Arab Emirates (UAE), one of the most technically competent security professionals in the Gulf.

I am enormously grateful to my publisher and friends, Mark Listewnik (pronounced "Listevnik"), who helped convince me to write this book and whose patience and encouragement kept me going through many difficult months of writing when I had no energy left from the volume of work I was otherwise under; to Linda Leggio and Stephanie Morkert at Taylor & Francis/CRC Press for their constant support and guidance; and to Cynthia Kamalo for her constant support.

I am grateful to the many consultants who have picked my brain and encouraged me to write this book about risk analysis.

I am endlessly grateful to ASIS International and to the ASIS Oil, Gas, and Chemical Industry Security Council for their important support of the entire security industry and whose encouragement to aspiring industry professionals helps them to grow and culture their skills.

I am also thankful for the many readers of my articles and books who send e-mails and letters encouraging me to write more and asking for expansions on what I have written. It is for you that I write.

I am grateful to the security industry for tempting a poor wayward young audio designer to forsake his career in commercial audio systems and move over to a far more rewarding career in security.

For each of those above, I am humbled by their encouragement and kindness, without whom this book would never have been written.

SECTION I

Risk Analysis

Risk Analysis — The Basis for Appropriate and Economical Countermeasures

INTRODUCTION

With the exception of militaries and nongovernmental organizations (NGOs) such as peacekeeping organizations, most organizations seek to fulfill their organization's mission by positioning themselves in an area of need for which they have expertise to offer, and otherwise seek to avoid risk and benefit from positive political, business, social, and economic trends. The most successful organizations do this not intuitively, but analytically, annually reviewing their situation with respect to industry and market trends, to economic trends, and to business and security risks.

As the world becomes increasingly volatile in all of these areas, the skillful analysis and reporting of these issues becomes increasingly critical to the success of organizations of all types.

But sadly, my experience indicates that many organizations employ vaguely defined security programs that often attempt to protect unknown vulnerabilities from unknown threats. Still today, many organizations do not employ reliable risk assessment methods to establish their security programs. We often see countermeasure programs employed with no security policies whatsoever to support the programs. This results in uncoordinated, often purposeless countermeasures that are a waste of money. This is the result of tactical rather than strategic thinking, solving a problem while often creating others, similar to constructing a building with only a cursory understanding of its purpose.

Often, countermeasures are poorly conceived to protect the organization against risks that are only assumed and for which no empirical data exist. This blundering approach would not be tolerated in any other business unit of the organization. But because management may often base their decisions on hastily and poorly prepared risk assessments, such decisions are based on assumptions, rather than facts and clearly drawn conclusions.

Many organizations believe that they cannot afford any risk assessment and base their security programs entirely upon the ill-advised judgments of a single (often totally unqualified) individual. I often hear that management does not wish to spend funds to study risk. But the same management is willing to spend far larger amounts to protect the organization against some unknown risk. This would not happen in any other business unit. Just as bad are organizations that utilize a risk assessment offered by a contractor

or vendor, which (quite not surprisingly) usually finds a compelling need for large expenditures on its own products or services.

The reasons for this are many, but most derive from the fact that security risk assessment is to some still a black art, less science than voodoo. Many methodologies are applied using a series of assumptions instead of analysis, and many security managers are not truly well founded in the science of risk assessment. Like any discipline, one can only be effective in one's job if one is very well founded in the basic principles of the discipline.

Let me make the case here that any security professional who is not extremely well founded in risk analysis is handicapped in every other portion of the security profession. Risk assessment is the foundational skill of all other security skills. It is like basic math to accounting, finance, or science. It is like grammar and vocabulary to a historian, author, or journalist. It is like critical thinking and debate to policy makers. Any security professional who is not extremely well founded in risk assessment can simply not succeed well for his or her own career or to well serve the organization he or she works for in any security role.

This is because everything else in a security program derives from the risk analysis process. The countermeasure selection process, operational decisions, staff deployment, how to utilize electronic solutions, the development of policies and procedures, training, liaison with local authorities, emergency preparedness, indeed everything else, is founded on security risk analysis. So, the quality of every down-line decision is affected by the quality of that person's skills in risk analysis.

Without the insight into risk that that skill gives, every other decision is based upon assumptions based in ignorance instead of qualitative insight. A decision that may appear to be tactically correct to a security supervisor may in fact be strategically inept. The supervisor may not possess the risk analysis skills to understand the threat environment or to see vulnerabilities that would be immediately apparent to a skilled risk analyst. So, he orders a guard to ignore his patrol in order to make an appearance when the chairman will be passing by in order to give an appearance of better security. Skilled threat actors will see this habit and plan their operation to exploit this vulnerability.

Any risk assessment done by anyone who is not well founded in the fundamentals of risk assessment will by definition be an incompetent risk assessment and may instead actually insert additional risk into the countermeasures program through ill-advised recommendations.

Any risk assessment done by a contractor or vendor whose recommendations include needs for their services or products is, by nature, inherently full of conflicts of interest and cannot be trusted. This is especially true where the cost of the risk assessment is nil or substantially less than one performed by a competent risk analyst. In almost every case where I have seen a risk assessment performed by a contractor or vendor, the "analyst" had little or no qualifications whatsoever. Many are done by individuals who have attended many seminars on sales techniques but few if any seminars on risk analysis. These contractors and vendors do a terrible disservice to their clients and may be exposing themselves to very high legal liability.

Now the good news. When you finish reading this book, you *will* be well founded in the foundations of the process of risk analysis conforming to U.S. Department of Homeland Security (DHS) requirements. You will be able to provide a quality report with convincing arguments and findings and with countermeasure selections that are reasonable and cost-effective, and with the evidence to back up your claims.

This is the book for organizations that need a world-class risk assessment but cannot budget the \$100,000-plus that some consultants charge or even the \$10,000-plus that

some better risk assessment software costs. This is the book that teaches how to equal or better those results with only your time and basic spreadsheet and word-processing software. You will do that because you will learn the analysis skills necessary to accomplish the task, develop the tools to analyze and develop a report at a level of depth that few others can equal at any price, and then learn how to present those data in a form that anyone can understand.

This book discusses the various risk analysis methodologies currently under use by the DHS and will help the reader to understand which of these is best to use for a particular type of facility.

CRITICAL THINKING

No other risk assessment book that I have ever read teaches the process of critical thinking, which is a *required skill* for correct analysis of any kind. Critical thinking is not taught in most high schools, colleges, and universities, except at the most cursory level. A California study on the role of critical thinking in the curricula of 38 public and 28 private universities concluded that the skill is “clearly an honorific phrase in the minds of most educators.”* The study concluded that university faculty members “feel obliged to claim both familiarity with it and commitment to it in their teaching, despite the fact that … most have only a vague understanding of what it is and what is involved in bringing it successfully into instruction.” The authors of the study found that 89% of the faculty interviewed “claimed critical thinking was the primary objective of their instruction,” but only 19% could define the term, and only 9% were evidently using it on a daily basis in their instruction.[†] Critical thinking is a required skill for risk analysis, notwithstanding that most security industry books do not teach the skill and very few security consultants understand or use the practice in development of their risk assessments. You will learn the fundamentals of critical thinking in this book.

QUALITATIVE VERSUS QUANTITATIVE ANALYSIS

There are two main schools of Risk Analysis Report writing — *quantitative* and *qualitative*. Qualitative analysis involves interpreting interviews, words, and images; Quantitative analysis involves interpreting numbers from data and estimates. In simple terms, qualitative analysis is intuitive; quantitative analysis is mathematical. Qualitative reports tend to be wordy and require extensive reading; quantitative reports tend to be full of charts, graphs, and tables and can be equally laborious to digest. In the hands of highly skilled analysts, qualitative reports can be a thing of beauty, and it is very obvious as to whether a qualitative report was written by an experienced analyst because the skill of the analyst emerges obviously through his or her reports as does equally the lack of skill emerge from unskilled and inexperienced analysts. It is often more difficult to see the experience level in quantitative reports and can be difficult to judge the quality of

* Richard W. Paul, Linda Elder, and Ted Bartell, “Executive Summary, of 38 Public Universities and 28 Private Universities to Determine Faculty Emphasis on Critical Thinking in Instruction,” *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations*, California Commission on Teacher Credentialing, Sacramento CA, 1997 (Dillon, CA: Foundation for Critical Thinking, 1997).

[†] *Critical Thinking and Intelligence Analysis*, David T. Moore, p. 62.

the analysis in quantitative reports. It is entirely possible to generate a quantitative report that is of poor quality if simple data crunching takes place in the absence of good analytical skills. Which method is better? I say, both. By that, I do not mean that they are equally valuable; I mean that a thorough analysis should use both qualitative and quantitative analysis. This book teaches a process that combines both into a very thorough analysis process that guides the analyst to the correct results. This process complies with all of the DHS-approved methodologies to the best of my knowledge.

This book will provide you with the skills and the tools to perform risk analysis and to create reports using a super-set of one of the most powerful risk assessment methodologies available. Your analysis will be more complete, with many more points of analysis than the large majority of professional security consultants, and your reports will also be more organized, be easy to read, and have much more depth than many security consulting firms that charge over \$100,000 for their reports. You will not only learn all the fundamentals of the science of risk analysis, but you will also have learned the skills for analysis including research and reference, analysis, and presentation. You will also learn how to build and use your own skills and tools.

Required Skills

- Skill #1: Gathering Data
 - Get the organization's mission statement
 - Understand the organization's programs
 - Assets by classifications
 - Existing countermeasures
- Skill #2: Research and Evidence Gathering
 - Interviews (see Figure 1.1)
 - Internet research
 - Telephone research
 - Records research



FIGURE 1.1 Interviews Form the Basis for Risk Analysis

- Surveys
- Asset classifications
- Historical data relating to security events
- Criticalities and consequences assessments
- Bibliography building
- Countermeasure research
- Skill #3: Critical Thinking in the Risk Analysis Process
 - Maintaining focus on purpose — Why examine this? What is the issue at hand?
 - Identifying key questions to be answered in the analysis
 - Observing and understanding the implications of different points of view
 - Examining evidence and its implications on the analysis
 - Drawing inferences from the evidence
 - Concepts affecting the evidence
 - What theories, definitions, axioms, laws, and principles or models underlie the issue?
 - What is the reliability of the evidence?
 - What are the effects of personal prejudices on the reliability of inferences?
 - What are the assumptions and what is their effect on risk conclusions?
 - Drawing implications on the consequences of the risk — What might happen and what does happen?
- Skill #4: Quantitative Analysis (see Figure 1.2)
 - Data classification
 - Data input
 - Data crunching
 - Risk analysis result calculations
- Skill #5: Qualitative Analysis
 - Converting quantitative data into qualitative data



FIGURE 1.2 Quantitative Analysis Examples

- Skill #6: Countermeasure Selection
 - Countermeasure selection
 - Cost-benefit analysis
- Skill #7: Report Writing
 - Report organization
 - Expanding and explaining quantitative data
 - Writing qualitative sections
 - Writing the recommendations
 - Writing the executive summary
 - Addendums

Tools

This book also presents the essential tools to produce world-class risk analysis reports. These include the following:

- Tool #1 — The book presents the elements of a high-quality Risk Analysis Report
- Tool #2 — The Risk Analysis Tool
- Tool #3 — The Countermeasure Options Analysis Tool
- Tool #4 — The Countermeasure Decision Matrix (see Figure 1.3)

Further, the book provides the reader with these technical tools that are available at virtually no cost (assuming the reader already owns a word processor and spreadsheet program) which rival or exceed the effectiveness of some of the most expensive risk analysis programs available in the marketplace today. Some of those software programs cost up to \$6,000 (including training). For the price of this book, you may be able to exceed the results of those programs.

THEORY, PRACTICE, AND TOOLS

This book will explain each element of risk analysis and countermeasure selection in terms of its theory, practice, and tools. The book will explain in adequate detail how to assemble MS Excel® spreadsheets for each element. Those readers who prefer to use a commercial software tool may skip the sections explaining how to build the Excel spreadsheets. For those who are interested in building and using their own world-class risk analysis software tool, the first two tabs on the Excel workbooks are explained in cell-by-cell detail and after that in adequate detail to build the remaining sheets.

The process fully complies with every accepted risk assessment methodology in use today and generally exceeds all of them in pure depth of analysis.

The processes discussed herein will demystify risk and move the reader from the tactical to the strategic, from being reactive to being proactive.

- Who Should Read This Book?
 - You should. If you are reading this book, it is almost certainly because you have been asked to perform a risk analysis and are trying to make certain that the Risk Analysis Report will be thorough and accurate, which will result in effective and affordable recommendations. You no doubt have a

Our Lady of Perpetual Funding — Medical Center Security Landscaping and Fencing Decision Matrix													
Goals Description	Goals Achieved					Risks Mitigated					Rank	Cost	Effectiveness
	1	2	3	4	5	A	B	C	D	E			
Fence Entire Property with Gates at Major Road Entrances only *	1	1	1	1	1	1	1	1	1	1	7	2	High
Fence Parking Lots and Garage Only **		1	1	1		1					4	3	Low
Use Landscaping Only to Create a Barrier to Unwanted Visitors			1	1	1						3	4	Low
Use Landscaping and Fencing to Enclose Property and Deny Access Except at Major Road Entrances Only *	1	1	1	1	1	1	1	1	1	1	10	1	High

Notes:
Score is based on highest number of goals achieved and threats mitigated or eliminated.
Rank is based on highest score.
Final Estimated Cost numbers may be lower than estimates on revolving doors

* Assumes guard house at major road entrances.
** Assumes no guard houses at any entrance.
*** Workplace violence threat actors cannot be easily identified at the perimeter. None of these options is an effective deterrent.

(Decision Matrix is a PRP Best Practices™ Tool)

FIGURE 1.3 Decision Matrix

background in security manpower management or some aspect of security technology. In some cases, the reader may be an architectural professional who has been asked to take security measures into consideration. In every case, you will be a person who wants to ensure the success of your project. This book will help you do that.

- Why Should You Read This Book?
 - Part of what is confusing about risk analysis to most security professionals is that there is no unique way to analyze risk. Dozens of methodologies exist from simple checklists to highly structured and detailed methodologies that can cost millions to fully implement for a mega-organization. The DHS alone references over a dozen different methodologies at the time of this writing. Which methodology is the correct one to use? How do we select it? How do we defend the choice?
 - Once a risk analysis methodology is selected and implemented, how are appropriate countermeasures selected? These questions often confound even veteran security professionals, who often end up advancing a tried and true method they have used for years in lieu of one that is possibly more appropriate. Chapter 2 will discuss various risk analysis methodologies and how to select which one to use for any particular project.
- How Can I Be Sure That I Will Really Learn the Principles of Risk Analysis from This Book?
 - This book uses a convention that absolutely works, which is the repetition of important principles. You will find that the book introduces a subject early in the book and then, as the book progresses, that same principle will be illustrated again in many different ways as other principles are explained. All of the principles of risk analysis relate together, like the parts of an engine. One cannot understand the role of pistons without understanding the roles of the cylinders and crankshaft. The same applies to risk analysis. Probability, vulnerability, and consequences are highly interrelated as are their constituent components. As the role of vulnerability is explored, the role of assets and threats will be revisited. As we explore assets, we will see a prelude to the discussion on criticality and consequences. You will understand these principles because they are not just discussed once but are explored in many different ways as they relate to each other.

From a general standpoint, all good *risk analysis methodologies* have two main sections:

1. Analyze Risks
2. Recommend Countermeasures to Mitigate the Risks

The risk analysis portion of all good risk analysis methodologies has certain things in common:

- They begin the process of risk analysis by *reviewing the organization's assets*.
- Then they review *threats* (probabilities).
- Then they review *vulnerabilities*.
- Then they calculate *risks*.

Certain risk analysis methodologies, notably ASME RAMCAP* and DHS CFATS,[†] rely on threat assessment results from government sources.

Subsequently, all better risk analysis methodologies also delve into countermeasures selection. It is also customary to develop budgets for the countermeasures.

This is where *risk mitigation* programs often fall apart, however. Most budgeting programs are pretty basic. The more advanced methodologies still only offer “good, better, best” options for mitigating specific risks without much detail behind why one is good, another is better, and one is best. This causes two main problems:

1. The vagaries of this approach do not provide useful data on why one approach is better than another.
2. This approach does not provide the organization’s security program advocate with much useful data to help support his or her case to management or budgeting authorities from whom monies to implement the security programs will be sourced.

Any analysis should result in countermeasure recommendations that can convincingly make the case that actual risk mitigation can occur at a cost that is affordable to the operation of the organization. If not, how can an organization’s budgeting committee be expected to part with funds for unknown results?

How do “good, better, best” relate to cost effectiveness? Does “best” reduce the possibility of risks occurring by a multiple of the cost of the mitigation? Are there any metrics whatsoever? Often the answer is “No,” or “I don’t know,” and the result from management is not surprisingly often “Hell no!” Thus, the entire risk assessment exercise gets laid aside, with only a few uncoordinated, scattered programs or applications being implemented, and those are often the least cost effective, most commonly being the implementation of incomplete and poorly planned electronic security systems. As a life-long designer of electronic security systems, I am nonetheless convinced that electronics is the “High Priest of False Security” and that electronic measures should supplement, not supplant, operational security measures.

This book is all about risk assessment and mitigation metrics — how to develop them, how to proof them, and how to present them in a fashion that is virtually irrefutable. This book presents the penultimate approach to risk assessment and shows you how to scale that up or down to meet the organization’s budget and schedule. *This book also shows you how to present to the organization’s management the fact that any risk not mitigated is accepted.* (This is one of the most important facts to end any risk analysis presentation.)

I have tried to make this book one of the most thorough ever written on the subject of risk analysis and mitigation so that it can be used as the single industry reference guide for professional risk assessment. This book is usable across a broad range of risk analysis case studies. It is specifically designed to be useful at the highest level (global and regional security risk analysis in terrorism environments — the area where I do most of my work). The book is also useful down to the level of assessing and mitigating risk for the smallest assets, such as a single electrical substation or executive suite.

* ASME Innovative Technologies Institute, LLC, Risk Analysis and Management for Critical Asset Protection (RAMCAP).

† DHS Chemical Facility Anti-Terrorism Standards (CFATS).

The book begins by studying risk analysis, later moving into countermeasure selection and budgeting. The book will also teach you how to prepare a high-quality Risk Analysis Report that will be the envy of very high-priced security consulting firms. Any report prepared using the tools and methods taught in this book will compete head to head with the most expensive and thorough risk assessment reports in the marketplace today. In fact, arguably, using the practice and tools taught in this book, your reports will make many security consulting firms' reports look unprepared and amateur by comparison. This is not meant as a criticism of most security consulting firms, just a statement that this important work can be done much better; after completing this book, the reader will know how to do much better.

Although the principles discussed focus on security risks, many if not most of the principles can also be applied with minor modifications to political, economic, social, and business risks as well. This is the one book you will need on risk analysis and countermeasure selection.

Theory

The difference between success and failure in risk analysis lies in the difference between knowledge and assumptions.

Let us begin with some simple questions that are often never asked. These questions are foundational — that is, understand them and their answers, and you understand what is behind risk. Most people performing security assessments that I have met cannot answer many of these questions correctly. Most people operate at a more intuitive level, from their assumptions. *However, trying to analyze risk from a standpoint of assumptions is in its own way the very definition of risk.*

Without understanding the questions and their answers, it is not possible to mitigate risks correctly. So although these questions seem very basic, they are essential.

- What is risk?
 - Risk is the likelihood of occurrence of an unwanted event that can adversely affect the mission of the organization. It includes four elements:
 - An asset (facility, structure, etc.)
 - The likelihood of a threat actor with intent
 - Vulnerabilities in the protective systems of the asset
 - Consequences of the threat action
- What types of risk do organizations face?
 - Risks exist in two forms: natural and man-made.
- What are the five types of *threat actors*?
 - Terrorists
 - Economic criminals
 - Violent criminals (other than terrorists who use violence as a means to their goals)
 - Subversives (protest organizations, etc.)
 - Petty criminals (vandals, prostitution, invasion of privacy, etc.)
- Why do organizations face risks?
 - Most risks are those that organizations face because they do not plan for them
 - Most risks can be mitigated to a greater or lesser extent
- Why do organizations care about risk?

- Every organization begins with a mission
- The organization acquires assets in order to support the carrying out of its mission
- Those assets range from miscellaneous (paper clips) to critical (the organization's information technology department)
- The loss of one or more critical assets could prevent the organization from carrying out its mission
- How does one analyze risk?
 - Risk is the combination of a possibility of an unwanted event times the severity of that event on the most critical assets of the organization, times the probability of such an event actually occurring
 - For terrorism, probability is replaced by gauging the value of the organization's asset in question as a potential target to the aggressor (asset target value)
 - For natural risks, tables of probability exist
 - Man-made events fall into five categories: terrorism, economic crimes, violent crimes, subversive crimes, and petty crimes
 - Risks can only occur where there are assets and vulnerabilities
- What can one do to mitigate risk? Risks can be mitigated by the following:
 - Shedding assets
 - Duplicating assets
 - Protecting assets (reducing vulnerabilities — reducing the probability of success of a threat action)
 - Transfer the risk to others (e.g., by insuring the assets)
- Can one eliminate all risk?
 - No
 - Every organization must accept some risk because the cost of mitigating against all risk would be more than the probable damage caused by letting the risk occur (for economic risks and unforeseen violent crimes)
 - For terrorism, the cost to mitigate some risks could prevent the organization from carrying out its mission
 - Subversive risk often requires high levels of cooperation with sometimes reticent law enforcement
 - Some levels of petty crimes will always exist

Practice

All better risk assessment methodologies include the following elements. (Different risk assessment methodologies express these attributes in different ways and may use different terminologies to describe them.)

- *Asset Characterization:* Understand and describe the organization's assets.
- *Threat Identification:* Understand and describe what threats there are against the organization's assets.
- *Consequence Analysis:* Understand and describe the criticalities of the listed assets to the organization's mission and the consequences to the organization of a successful threat action.
- *Vulnerability Analysis:* Understand and express the vulnerabilities of the organization's assets.

- *Threat Assessment:* Understand how threat actors view the organization's assets and which assets the threat actors would find most interesting.
- *Risk Assessment:* Express risk in the form of a calculation. (This should be scalable, so that risk can be calculated for any single asset, or for the entire organization.)
- *Risk Prioritization:* Prioritize the risks, so that the most important risks can be mitigated first and the least important risks will be mitigated last.
- *Risk Management:* Provide recommendations for countermeasures to mitigate the risks.

Additionally, any Risk Analysis Report ideally should include the following:

- A statement of the *organization's mission*.
- A statement describing the *organization's business programs* and the business processes that are critical to the success of carrying out those programs.
- A statement of how the organization's assets support the business programs (including ranking of asset criticalities).
- A list of the users of those assets, and notes detailing from which categories the threat actors may arise.
- Prioritized budgets for the proposed countermeasures.
- Space planning information.
- Blast calculation resource information.
- Qualifications of the risk analyst (including the analyst and his or her organization).
- A bibliography of references.
- A table of contents.
- A table of figures.
- An index.
- Optionally, a *risk register* may be required by the client. This is discussed in Chapter 20.

Of the dozens of popular risk analysis methodologies, there are great and small. Many are specifically designed to address risk at a specific type of organization (pipelines, water supply facilities, chemical facilities, marine facilities, etc.). These will be covered in some detail in later chapters. But it is important to be well founded in the fundamentals of risk analysis in order to be able to traverse the broad terrain of many different types of facilities to which your skills will be applied.

There are also dozens of popular risk analysis methodologies that do a poor job of serving the client's needs. Look carefully at the list of basic risk analysis elements above. I will say definitively that any methodology that does not include all of these elements is inadequate to the task and cannot result in a successful mitigation of risk. This is especially true of risk analysis checklists, of which dozens exist in the commercial sector. Most of these focus on vulnerabilities rather than on a total risk equation. And most of these do not use any systematic approach even to evaluating vulnerability. These all do a terrible disservice to their clients by giving a feeling that risk has been studied while it has not been. Worse, those checklists are often used by people who have little understanding of who the potential threat actors are and what tactics they use to carry out their terrorism and criminal attacks. In short, such inadequate checklists in the hands of incompetent "security providers" can actually increase a facility's risks by ending the process of risk analysis with one effort, which resulted in totally inadequate security planning.

Any methodology that does not address a list of the organization's assets is assuming facts not in evidence. Any methodology that does not analyze threat actors assumes facts not in evidence. Any methodology that checklists vulnerabilities is almost certain to miss others not on the checklist.

Many security professionals assume that it is acceptable to insert gross assumptions into the risk analysis equation. For example, most risk assessment methodologies ask the vulnerability level of listed assets. But they do not identify what vulnerability means or evaluate the component variables of the vulnerabilities. Let me say again: *The difference between success and failure in risk analysis lies in the difference between knowledge and assumptions.*

This is not to say that there are times when expediency or budget demands a quick, intuitive risk estimate, but let us not call it an analysis. Call it what it is — it is a *risk estimate*.

Tools

This book is about the process of understanding, analyzing, and mitigating security risks and then developing workable, cost-effective solutions to mitigate the risk.

It is also about empowering any professional security manager, analyst, or consultant to do the very best work in the industry without expending thousands of dollars for conventional risk analysis software.

The first and most important point of success for a quality risk analysis is the analysis skill. So, the first set of skills taught in this book is research, analysis, and critical thinking and how to select and use the proper tools of analysis.

The following is being repeated for emphasis, as this is the core of the book which must be fully and intuitively understood. This book also presents four software word-processing and spreadsheet tools that make convincing and nearly irrefutable arguments to support the risk conclusions and countermeasure recommendations and which helps drive consensus when there are multiple options on the table to choose from. These last points are most important and are widely disregarded by most risk analysis methodologies.

- Tool #1 — The book presents the elements of a high-quality *Risk Analysis Report* so that the reader can generate very complete and convincing reports.
- Tool #2 — *Risk Analysis Tool*: One of the most frustrating things for veteran security analysts is the virtual requirement to purchase (and continue investing in annual updates of) very expensive risk analysis programs. Some of the best of these programs cost thousands of dollars each year to buy and keep current. This book presents a spreadsheet-based risk analysis tool that will result in deep and convincing risk analysis results, comparable to (and quite arguably superior to) the programs that cost thousands of dollars a year to buy and maintain. The tool results are color coded to help assure that organization leadership, who may be unfamiliar with risk analysis methodologies, can digest massive amounts of data in seconds.
- Tool #3 — *Countermeasure Options Analysis Tool*: This tool does something amazing that to my knowledge has never been done before and most security professional think cannot be done at all. It allows the security analyst to determine the best countermeasure based upon effectiveness and cost-effectiveness. The latter is a function of cost versus the countermeasure's effectiveness elements, including the countermeasure's ability to do the following:

- Control access
- Deter attacks
- Detect attacks
- Assess the event
- Respond to the event
- Collect evidence
- Mitigate multiple vulnerabilities
- Sort the countermeasures into a three-dimensional color-coded spreadsheet:
 - From:
 - Most critical vulnerabilities
 - Most cost-effective solutions
 - To:
 - Least critical vulnerabilities and
 - Least cost-effective solutions
- Tool #4 — *Countermeasure Decision Matrix*: The book presents a decision matrix tool that helps achieve consensus as to the correct countermeasure solution when there are several popular options, or when options are contentious, or when ideas are few. This tool (the Countermeasure Decision Matrix) has on many occasions achieved total unanimous consensus among a large group of managers who were each highly committed to widely differing options.

ORGANIZATION

This book is presented in three sections:

- Section I — Risk Analysis
 - Chapters
 - 1 — Risk Analysis — The Basis for Appropriate and Economical Countermeasures
 - 2 — Risk Analysis Basics and the Department of Homeland Security—Approved Risk Analysis Methods
 - 3 — Risk Analysis Skills and Tools
 - 4 — Critical Thinking and the Risk Analysis Process
 - 5 — Asset Characterization and Identification
 - 6 — Criticality and Consequence Analysis
 - 7 — Threat Analysis
 - 8 — Assessing Vulnerability
 - 9 — Estimating Probability
 - 10 — The Risk Analysis Process
 - 11 — Prioritizing Risk
- Section II — Policy Development before Countermeasures
 - Chapters
 - 12 — Security Policy Introduction
 - 13 — Security Policy and Countermeasure Goals
 - 14 — Developing Effective Security Policies

- Section III — Countermeasure Selection and Budgeting
 - Chapters
 - 15 — Countermeasure Goals and Strategies
 - 16 — Types of Countermeasures
 - 17 — Countermeasure Selection and Budgeting Tools
 - 18 — Security Effectiveness Metrics
 - 19 — Cost-Effectiveness Metrics
 - 20 — Writing Effective Reports

SUMMARY

A security risk analysis should be performed before any countermeasures are selected or implemented.

- Qualitative reports mainly focus on interviews, words, and images while quantitative reports mainly focus on the analysis of numbers. The use of both is better than the use of either one alone.
- All better risk analysis methodologies include the following elements:
 - *Asset Characterization:* Understand and describe the organization's assets.
 - *Threat Identification:* Understand and describe what threats there are against the organization's assets.
 - *Consequence Analysis:* Understand and describe the criticalities of the listed assets to the organization's mission.
 - *Vulnerability Analysis:* Understand and express the vulnerabilities of the organization's assets.
 - *Threat Assessment:* Understand how threat actors view the organization's assets and which assets the threat actors would find most interesting.
 - *Risk Assessment:* Express risk in the form of a calculation. (This should be scalable, so that risk can be calculated for any single asset, or for the entire organization.)
 - *Risk Prioritization:* Prioritize the risks, so that the most important risks can be mitigated first, and the least important risks will be mitigated last.
 - *Risk Management:* Provide recommendations for countermeasures to mitigate the risks.
- Additionally, any Risk Analysis Report ideally should include the following:
 - A statement of the organization's mission.
 - A statement describing the organization's business programs and the business processes that are critical to the success of carrying out those programs.
 - A statement of how the organization's assets support the business programs (including ranking of asset criticalities).
 - A list of the users of those assets, defining from which categories the threat actors may arise.
 - Prioritized budgets for the proposed countermeasures.
 - Space planning information.
 - Blast calculation resource information.

- Qualifications of the risk analyst (including the analyst and his or her organization).
- A bibliography of references.
- A table of contents.
- A table of figures.
- An index.
- Skills taught in this book include the following:
 - Skill #1 — Gathering Data
 - Skill #2 — Research and Evidence Gathering
 - Skill #3 — Critical Thinking in the Risk Analysis Process
 - Skill #4 — Quantitative Analysis
 - Skill #5 — Qualitative Analysis
 - Skill #6 — Countermeasure Selection
 - Skill #7 — Report Writing
- Tools presented in this book include the following:
 - Tool #1 — The book presents the elements of a high-quality Risk Analysis Report format so that the reader can generate very complete and convincing reports.
 - Tool #2 — The Risk Analysis Tool
 - Tool #3 — The Countermeasure Options Analysis Tool
 - Tool #4 — The Countermeasure Decision Matrix

CHAPTER 2

Risk Analysis Basics and the Department of Homeland Security—Approved Risk Analysis Methods

INTRODUCTION

At the end of this chapter, you will understand the approaches that the U.S. Department of Homeland Security (DHS) has embraced over time to study risk, the elements of risk analysis, typical interested stakeholders and agendas for a risk analysis study, commercially available risk analysis software tools, risk analysis basics, risk assessment steps, some information on how to select the right methodology for a particular kind of project, and why DHS is unconcerned for most facilities about the specific risk assessment methodology used to study risk.

“Over the years, there have been numerous criticisms from various groups over how risk is assessed and, as a result, DHS grants are allocated.”* DHS has evolved in its understanding of risk and its application of formulas to measure it. From a “macro-risk” standpoint (risk to communities versus risk to facilities or structures), the DHS risk approach evolved as follows:

Stage I: R = P. From Fiscal Year (FY) 2001, when the Department of Justice (DOJ) had primary responsibility for assessing risk, to FY2002 to FY2003, when this responsibility was transferred to DHS. This first stage of risk assessment could be characterized as early stage developmental. During this period, risk was generally assessed and measured according to population numbers. In short, risk (R) was equated to population (P).

Stage II: R = T + CI + PD. This period covers from FY2004 to FY2005. During this period, the importance of critical infrastructure, population density and a number of other variables was included in the assessment of risk. However, the formula for risk remained additive and “risk-like,” as probabilities were not an

* CRS Report for Congress — *The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, February 2, 2007, Congressional Research Service. Prepared for Members and Committees of Congress, Order Code RL33858, p. CRS-4.

essential element of the risk assessment process. Risk was assessed as the sum or threat (T), critical infrastructure (CI), and population density (PD).

*Stage III: R = T * V * C = T * (V&C).* This period covers from FY2006 to today, {2009, author's note} a time when probability of particular events was systematically introduced into the formula.

The DHS has overtly or tacitly approved a number of different risk assessment methodologies for use on critical infrastructure facilities. This new approach to allocating the remaining funds required an assessment of risk using a formula that considers the threat to a target/area, multiplied by vulnerability (V) of the target/area, multiplied by consequence (C) of an attack on that target/area. As a result, the risk assessment formula became $R = T * V * C$. Variables were no longer additive but were multiplied, implying weighting of variables and some assessment of the likelihood that certain events would occur.

The Current Process

FY2007. Risk will be evaluated at the Federal level using a risk analysis model developed by DHS in conjunction with other Federal entities. Risk is defined as the product of three principal variables:

- Threat (T) — the likelihood of an attack occurring
- Vulnerability and Consequence (V&C) — the relative exposure and expected impact of an attack

Although DHS continues to discuss its risk methodology in terms of the $R = T * V * C$ formula, it appears as if the department is treating vulnerability (V) and consequence (C) as an amalgamated, single variable.*

In the discussion above, it can be seen that the DHS view is to communities more than to individual facilities and structures. And this explains much about why DHS has taken the relaxed attitude that it has toward establishing definitions for risk assessment methodologies for individual facilities and structures. Those have been left up to interpretation of DHS departments (for example, the U.S. Coast Guard for maritime facilities, waterways, and terminals), and DHS has been open to industry input vis-à-vis individual industries and special interest groups.

RISK ANALYSIS FOR FACILITIES AND STRUCTURES

The object of risk analysis is to understand the *risks, vulnerabilities, criticalities, and consequences* (see Figure 2.1) well enough to develop or improve security countermeasures that can effectively deter, detect, assess, delay, respond, and gather evidence of serious threat actions against the facility in question.

Through the years, various risk analysis formulas have been developed with greater or lesser compliance to this goal. All good risk assessment methodologies include four things:

1. Consideration of Threat
2. Consideration of Probability
3. Consideration of Vulnerability
4. Consideration of Consequences

* Ibid., pp. CRS-6–8.

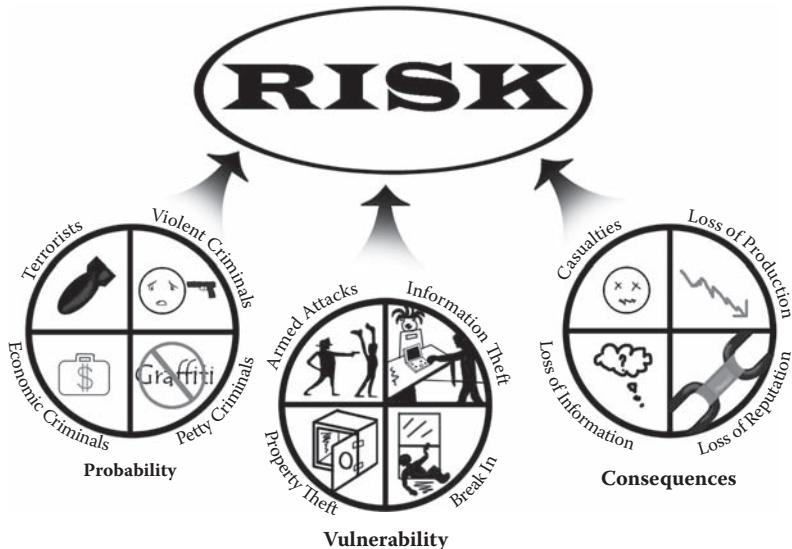


FIGURE 2.1 Risk Factors

Better risk assessment methodologies also include methods to guide the analyst toward appropriate countermeasures.

The best risk assessment methodologies also include metrics for assessing the best choice of countermeasures as measured by their effectiveness in countering potential threats.

The very best methodologies also include metrics for assessing the best choice of countermeasures, not only from an effectiveness point of view, but also from a cost-effectiveness point of view.

Critical infrastructure and key resources (CIKR) sectors include the following*:

- Agriculture and Food
- Commercial Facilities
- Dams
- Energy
- Information Technology
- Postal and Shipping
- Banking and Finance
- Communications
- Defense Industrial Base
- National Monuments and Icons
- Transportation Systems
- Chemical
- Critical Manufacturing
- Emergency Services
- Health Care and Public Health
- Nuclear Reactors, Materials, and Waste
- Water

* Source: U.S. Department of Homeland Security.

- Military Sites Are under the Purview of the U.S. Department of Defense, Not the DHS
- Critical Manufacturing
- Government Facilities Including the Educational Facilities Subsector

Guidelines for the protection of such facilities include the Homeland Security Act of 2002 and the National Infrastructure Protection Plan (NIPP). These guidelines are useful for determining the criticality and protection measures appropriate for similar facilities in any country in the world and thus serve as a benchmark for protection of such facilities. The balance of this book is about risk analysis for critical infrastructure and key resources facilities worldwide. However, the methods may also be used on facilities that do not fit these criteria.

The NIPP is comprehensive and can be reviewed in detail at: www.dhs.gov. In the search field, enter NIPP.

MANY INTERESTED STAKEHOLDERS AND AGENDAS

As with any important issue, many individuals and organizations can be expected to express input on how to achieve the objectives of the program. In the case of the NIPP, this includes interests from various branches of the government, such as the U.S. Coast Guard who are responsible for enforcement or standards and guidelines, and also industry and special interest groups. Resulting from this, as one might expect, there is no single standard for risk assessment for critical infrastructure facilities. So, for any particular type of facility, there may be competing risk assessment methodologies that are forwarded by government agencies, national laboratories, branches of the military, industries, and industry interest groups. All of these have put forward risk assessment methodologies for use on CIKR facilities, and DHS has either directly or tacitly approved a wide variety of risk assessment methodologies for use.

Some of these methodologies are industry specific, and a few are intentionally widely applicable. Some of these methodologies are highly detailed and scientific, and others are generic and vague. Some of the methodologies place a high degree of control in the hands of the analyst, and others remove important segments such as threat and asset target analysis and place it in the hands of the reviewing agency.*†

This is most confusing for management of these facilities and risk analysts to know which methodology to use for a specific facility. Should the analyst use a methodology that was developed for that specific industry or a more generic model that is suitable to all? Would the generic model work on every type of facility? Would it be accepted by everyone, including DHS? Can the analyst use an industry-specific model on a facility that is not part of that industry? Would that be accepted by DHS or by stakeholders? How many risk assessment methodologies should an analyst be competent in? How many types of risk assessment software should he or she buy and maintain?

Obviously, the direct and indirect costs of buying and training in a variety of methodologies are a consideration. Lost time, lost productivity, sorting through the vagaries

* For example, RAMCAP.

† Chemical Facility Anti-Terrorism Standards (CFATS) also place threat and asset target value definitions in the hands of the reviewing agency.

of many different programs can all become confusing to the analyst and can actually reduce his or her effectiveness.

The cost of some of the risk assessment programs runs into the tens of thousands, and training costs can add many more thousands to the cost of the programs. As many of these methodologies and programs utilize different formulas and interpretations of the same basic data, one can easily become lost in the sheer size of the forest of methodologies. It would be useful if there was one methodology that could be relied upon to do the job in every type of facility and which would be unquestioned as to completeness and authenticity. The good news is that there are two that easily fit this bill.

Sandia National Laboratories has developed a set of methodologies called RAM (Risk Assessment Methodology), for which many subsectors have been developed. All of the subsector methodologies rely on the same basic risk analysis formula. The main differences involve vulnerability assessment aspects that are unique to the facility types.

Another methodology, shown in Figure 2.2, is one developed for the oil/gas/chemical sector called the API/NPRA SVA method (American Petroleum Institute/National Petrochemical and Refiners Association Security Vulnerability Assessment method). Both of these methods are so thorough and complete that they are widely accepted as being at the pinnacle of the risk assessment methodologies.

Both the Sandia Risk Assessment Methodology and the API/NPRA models are scalable. That is, they can both be applied to relatively simple sites with minimal analytical requirements or to complex organizations with many campuses, many facility types, and many departments and services.



FIGURE 2.2 American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA) Cover

The Sandia models are scalable to the point of being virtually certain with respect to the efficacy of existing countermeasures, as details such as the mixture of concrete and spacing of rebar in defensive walls can be considered in the delay formula.

Such levels of detail, although completely appropriate for facilities such as nuclear power plants, nuclear stockpiles, and weapons facilities, can be far too much for most commercial facilities such as airports, hotels, and the like, where serious threats of terrorism exist and the cost to analyze to Sandia's level of detail, while laudable, can make not only the cost of countermeasures but also the cost of the analysis completely unaffordable. In Sandia's model, for example, the analysis team for the Vulnerability portion alone may include the following*:

- A Vulnerability Assessment Project Leader
- A Systems Engineer
- A Security Systems Engineer
- An Intrusion Sensing Subsystem Subject Matter Expert (SME)
- An Alarm Assessment Subsystem SME
- An Alarm Communication and Display (AC&D) Subsystem SME
- An Entry Control Subsystem SME
- A Delay Subsystem SME
- A Response System SME
- A Communications Subsystem SME
- An SME Analyst

Such a team, when evaluating a hotel that caters Western guests in Pakistan, will result in a risk analysis that is cost prohibitive and findings and recommendations that do not support the function of hoteling. So, despite Mae West's assertion that "Too much of a good thing — is wonderful," in risk analysis, one must strike a balance between affordability and results. Despite my very high regard for Sandia's reaching the practical pinnacle of risk analysis methodologies (and that is my opinion), in some cases, too much of a good thing is too much to use in practicality. The Sandia model can be scaled back to the minimum, and the methods taught in this book can be applied to the minimum to medium application of Sandia's model. It is also notable that the Sandia model focuses primarily on terrorist threats rather than on economic crimes or petty criminal threats. The Sandia model offers little focus on internal economic threats, for example. As such, the Sandia model is extraordinarily well suited to such facilities as nuclear storage facilities and nuclear power plants, and in the opinion of some, it is not as well suited to conventional commercial facilities, such as hotels, shopping malls, or stock exchanges.

COMMERCIALLY AVAILABLE SOFTWARE TOOLS

Commercial software programs have been developed to support these and other DHS-approved methodologies. Many of these programs cost thousands of dollars and require thousands further in costs for training courses in the methodologies and software tools. Thus, a cottage business has grown around the complexities of implementation of the various methods. This is a common response to regulation — that is, that regulation

* *Vulnerability Assessment of Physical Protection Systems*, p. 55, Mary Lynn Garcia, Sandia National Laboratories (Butterworth-Heinemann, Oxford, 2005).

spawns implementation tools and training, on which businesses are built to service these perceived needs, and those businesses have a vested interest in building and maintaining a perception of complexity, thus driving the need for the training and software programs. Some of these programs produce volumes of information with little, if any, useful summary.

At this point, it should be noted that DHS does not require the use of any specific software program to perform the analysis.

The risk analysis methods discussed in this book can be used to support all DHS-approved methodologies equally well. Variations between the methodologies are in four main areas:

- Scaling of estimates (0 to 1, 1 to 5, or 1 to 10)
- Order of evaluation (some view asset target value as part of vulnerability, and others view it as part of threat analysis, for example)
- Formulas (although there are marked differences in formulas, and some like Sandia are more scientific than others, most reach conclusions that are in the same order of magnitude)
- Qualitative versus quantitative analysis (most adapt well to qualitative analysis, but some like API/NPRA and Sandia rely more on quantitative approaches, though qualitative analysis summaries can be added)

The methods taught in this book are extremely thorough and can be applied to all DHS-approved methodologies in all of their interpretations.

RISK ANALYSIS BASICS

Risk formulas are usually quite simple. Most typically they involve:

- Risk = A Threat Actor with Intent (Probability) * An Exploitable Vulnerability, prioritized by criticality and consequences.

Numerous variations exist, but all formulas result in a ranking of risk by some combination of probability, vulnerabilities, and consequences.

A variation on the risk formula is:

- Risk = (A Threat Actor with Intent + Probability + An Exploitable Vulnerability)/3, prioritized by criticality and consequences.

Threat — An active *threat actor* with the capabilities and intent to do harm to the organization.

Probability — The *likelihood* that a target has been or will be selected by a threat actor (any asset of the organization that can be attacked in fulfillment of the mission of the threat actor).

Vulnerability — Any condition or factor associated with the selected target that can be exploited to carry out an attack — vulnerabilities may be individual or systemic (e.g., a door left unlocked or poor training of guards).

Different methodologies sort these elements in different ways, sometimes renaming them, but the elements are really always the same.

The degree of risk varies in accordance with the following:

- Likelihood Variables
 - Threat Variables
 - The existence and degree of motivation of a threat actor
 - The capabilities of the threat actor, including the threat actor's training
 - The availability of resources to the threat actor
 - Types of threat actors
 - Terrorists
 - Economic criminals
 - Violent criminals
 - Subversives
 - Petty criminals
 - Target Selection Variables (Target selection variables depend on the type of threat actor)
- Vulnerability Variables
 - Vulnerability variables include the following:
 - Accessibility
 - Surveillance opportunities
 - Intrinsic vulnerabilities
 - Natural and existing countermeasures including the following:
 - Physical countermeasures
 - Electronic countermeasures
 - Operational countermeasures
- Consequence Variables
 - Criticality of assets to the mission of the organization
 - Difficulty in replacing assets back into operation (recuperation)
 - Consequences of loss
 - Loss of life
 - Loss of property
 - Loss of proprietary information
 - Loss of business reputation
 - Loss of business productivity

All of the many and varied risk analysis methodologies utilize these three basic elements:

1. Probability (Threat Actors and Target Selection)
2. Vulnerability
3. Consequences

Probability is simply the likelihood that a threat actor will select and then act upon a target. For certain criminal acts in certain geographic regions where accurate criminal records are kept and are available to the risk analyst, probability can be derived by historical data. That is never so for terrorism, where too few instances and evolving tactics prevent historical data from being developed. Therefore, for terrorism, target selection factors are an appropriate surrogate for probability factors.

RISK ASSESSMENT STEPS

The steps involved in risk assessment include the following:

- *Asset Characterization:* Understand and describe the organization's assets (business function, environment, building and perimeter types, population, access/egress, etc.).
- *Threat Identification:* Understand and describe what *threats* there are against the organization's assets and select a threat level that the security program will be designed to counter or effectively or otherwise mitigate effectively.
- *Criticality Analysis:* Understand, describe, and rank the criticalities of each of the listed assets to the organization's mission.
- *Consequence Analysis:* Understand, describe, and rank the consequences of loss of the listed assets to the organization's mission in terms of the severity of the loss of the following:
 - Casualties
 - Production or business function
 - Proprietary information
 - Business reputation
- *Vulnerability Analysis:* Understand and express the vulnerabilities of the organization's assets.
- *Likelihood (Probability) Assessment:* Understand how threat actors view the organization's assets and which assets the threat actors would find most attractive to exploit. This can be accomplished using statistical values or asset target value estimates.
- *Risk Assessment:* Express risk in the form of a calculation. (This should be scalable so that risk can be calculated for any single asset, or for the entire organization.)
- *Risk Prioritization:* Prioritize the risks, so that the most important risks can be mitigated first, and the least important risks will be mitigated last.
- *Risk Management:* Provide recommendations for countermeasures to mitigate the risks.

In order to protect the organization's assets, the analyst must determine what those assets are. All organizations have four types of assets:

1. People (including Management, Employees, Customers, Visitors, Contractors, and Vendors)
2. Property (including Real Property, Fixtures, Furnishings and Equipment [FF&E])
3. Proprietary Information (including Proprietary Business Processes, Strategic Plans, Customer Lists, Vital Records, Accounting Records, etc.)
4. Business Reputation (ask any ex-Arthur Anderson, LLP employee)*

* Arthur Anderson, LLP, was once one of the “Big Five” accounting firms along with PriceWasserhouse Coopers, Deloitte & Touche, Ernst & Young, and Tomatsu. Now there are four. Arthur Anderson, LLP, failed resulting from a business reputation scandal.

In order to protect the organization's assets, the risk analyst must determine what those assets are and how critical those assets are to the organization's mission and what consequences could occur if the vulnerabilities are exploited. It is important to understand that what we are really protecting is the mission of the organization. Let me repeat that. *It is important to understand that what we are really protecting is the mission of the organization.*

- *Threat Identification:* Understand and describe what threats there are against the organization's assets.
- *Criticality Analysis:* Understand what assets are critical to carrying out the mission of the organization.
- *Consequence Analysis:* Understand and describe what unwanted consequences could occur if a threat actor exploits a vulnerability in the critical assets of the organization's mission.

The root of the problem will be discussed now. All risk derives from threat actors who are interested in the organization's assets. No threat actor equals no risk. No assets equals no risk. Now, this may seem obvious; however, it is illuminating to remember that security organizations do not attempt to protect all of the organization's assets equally. Therefore, all assets are not equal. That is, all assets are not of equal value to the client. Some assets are more critical than others. And due to the varying degrees of criticality and consequences, not all vulnerabilities are equal in the eyes of threat actors.

- *Vulnerability Analysis:* Understand and express the vulnerabilities of the organization's assets.
- *Threat Assessment:* Understand how threat actors view the organization's assets and which assets the threat actors would find most interesting.
- *Risk Assessment:* Express risk in the form of a calculation. (This should be scalable so that risk can be calculated for any single asset, or for the entire organization.)
- *Risk Prioritization:* Prioritize the risks, so that the most important risks can be mitigated first and the least important risks will be mitigated last.
- *Risk Management:* Provide recommendations for countermeasures to mitigate the risks.

Formulas that include consequence as part of the basic analysis include all of the Sandia National Laboratories formulas. Sandia uses a model called RAM (Risk Assessment Methodology).

In the Sandia formula:

$$\text{Risk} = P_A * (1 - P_E) * C$$

P_A is the likelihood of adversary attack, P_E is the security system effectiveness, $1 - P_E$ is adversary success, and C is the consequence of loss of the asset.

For simplicity, in the Sandia model, Risk = Likelihood * Vulnerability * Consequence.

Note that the elements are the same and that the net result is virtually identical. All three formulas result in virtually the same result. Sandia has versions of RAM for Biological Facilities (Bio-RAM), Communities (RAM-C), Chemical Facilities (RAM-CF),

Dams (RAM-D), Energy Infrastructures (RAM-E), Prisons (RAM-P), Power Transmission System (RAM-T), and Water Utilities (RAM-W).

Although Sandia National Laboratories is highly respected, and it created all of these numerous and effective tools, some industries have widely adopted the Sandia Risk Assessment Methodologies, but others have not.

DHS-Approved Risk Assessment Methodologies

Following are relevant codes, standards, and risk analysis methodologies that are accepted for use by DHS:

- ASME-ITI Tools
 - *RAMCAP™* — ASME Innovative Technologies Institute, LLC, is used by the DHS to assess critical infrastructure facilities. RAMCAP is a relatively complete methodology that is designed for a facility's own staff to use.
- Sandia Tools
 - Bio-RAM
 - RAM-C
 - RAM-CF
 - RAF-D
 - RAM-E
 - RAM-P
 - RAM-P
 - RAM-W
- DHS Tools
 - CARVER+Shock
 - ISPS
 - NVIC-05-05 — Liquefied Natural Gas (LNG) Risk Assessment
- Federal Emergency Management Agency (FEMA) Tools
 - FEMA-452
- Relevant Codes and Standards
 - *FEMA 386-7* — Integrating Human-Caused Hazards into Mitigation Planning
 - *FEMA-426* — Plan of Instruction for Building Design for Homeland Security
 - *FEMA-452* — Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings
 - *DHS—OIG-07-33* — Department of Homeland Security, Office of Inspector General: The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection, February 2007, CARVER+Shock Method
 - *DOD — Unified Facilities Criteria (UFC)* — UFC 4-010-01 DoD Minimum Anti-Terrorism Standards for Buildings
 - *DOD-5200.08-R and Army Regulation 190-13* — Physical Security Program
 - *Department of Justice* — Minimum Security Standards for Federal Buildings
 - *General Services Administration* — The Facilities Standards for the Public Buildings Service
 - *Occupational Safety and Health Act (OSHA) Section 1910* — General Industry Standards

- Military Standards
 - (MIL-HDBK) 1013/1, The Design Guidelines for Physical Security of Facilities
 - FM 3-19.30 — Physical Security
- Federal Specifications
 - RR-F-191 Chain Link Fence Specifications
 - RR-F-191K_Gen: Fencing General Specification
- DHS-Approved Methodologies for Specific Industries
 - Chemical — RAMCAP — ASME
 - Critical Infrastructure — RAMCAP — ASME
 - Gas/Oil/Chemical — API/NPRA
 - Nuclear — ASME RA-S Probabilistic Risk Assessment for Nuclear Power Plants
 - Food — CARVER+Shock
 - Sandia Methodologies
 - Bio-RAM — Biological Facilities
 - RAM-C — Communities
 - RAM-CF — Chemical Facilities
 - RAM-CI — Critical Infrastructures
 - RAM-D — Dams
 - RAM-E — Energy Infrastructures
 - RAM-P — Prisons
 - RAM-T — Electrical Transmission Systems
 - RAM-W — Water Facilities
- Commercially Available Software Tools Supporting These Methodologies
 - Chemical — RAMCAP Plus — ASME Software Tool for evaluating RAMCAP Projects
 - Critical Infrastructure — RAMCAP Plus — ASME Tool (as above)
 - Gas/Oil/Chemical — API/NPRA — SVA-Pro (Dyadem)
 - Nuclear — ASME RA-S Probabilistic Risk Assessment for Nuclear Power Plants
 - Food and Agriculture — CARVER+Shock
 - Sandia Software Tools
 - *Adversary Sequence Diagram (ASD)* — Graphical representation of physical protection system elements along paths that adversaries can follow to accomplish their objective.
 - *Systematic Analysis of Vulnerability to Intrusion (SAVI)* — Determines the most vulnerable path to a specific asset.
 - *Analytic System and Software for Evaluating Safeguards and Security (ASSESS)* — Determines the most vulnerable path to a specific asset.
 - *Joint Combat and Tactical Simulation (JCATS)* — Estimates response force effectiveness.

Many of these software tools can be applied to methodologies for which they were not originally written. (See the list of methodologies that each software tool can support on the Web site for that software tool. As this list changes often, it is not listed.)

WHICH METHODOLOGY TO USE?

Community versus Facility Methodologies

The DHS community methodology $R = T * (VC)$ is not usable for individual facilities due to the fact that DHS is using that formula for allocation of funds to communities, and it is not granular enough to apply to individual facilities.

For individual facilities, DHS continues to allow latitude in methodologies as long as the methodology submitted considers threat likelihood, vulnerability, and consequences. Arguments rage over whether threat and probability should be calculated by DHS or by the submitting risk analyst. There are compelling arguments in both camps. DHS, in fact, requires that the Threat component be supplied only by DHS for certain specific fields (RAMCAP, CFATS, etc.). And for facilities that are clearly outside the purview of DHS, such as hotels and sports arenas, the argument absolute in favor of the individual analyst as DHS will not do so.

Further, for any facility for which the risk analysis is not being submitted to DHS or one of its departments for review, the risk analyst must conduct the threat/probability analysis.

Strengths and Weaknesses of Major Methodologies

- *Full-Scale Sandia Process* — Extremely robust analysis method; very scalable; completely scientifically supportable; may be used qualitatively, quantitatively, or a combination of both; ideal for facilities where a very robust analysis is required requiring very deep analysis of vulnerabilities, though can be used in a less robust fashion. Full-Scale Sandia Process utilizes deeply researched calculations for every quantitative date entry point, which makes it both highly precise and simultaneously very costly to perform. The Full-Scale Sandia Process is usually performed only by Sandia National Laboratories, due to the expertise required to accommodate its stringent requirements successfully. It is outside the abilities of all but the most capable and well-equipped risk laboratory teams. This approach is highly recommended for high-consequence critical infrastructure facilities.

In my opinion, it is unwise to use any other risk analysis process than the Full-Scale Sandia Process for any facility where the consequences of loss could affect the health or lives of an entire community (such as for certain high-consequence chemical facilities, i.e., Phosgene, Ammonium Nitrate, Methyl Isocyanate, etc.). (On December 3, 1984, a release of methyl isocyanate from a Union Carbide plant in the city of Bhopal, India, exposed more than 500,000 people and immediately killed 2,259 people. Estimates are that more than 8,000 died within 2 weeks and an additional 8,000 have since died from gas-related diseases.*)

- *ASME RA-S* — Limited to heavy nuclear facilities only.
- *API/NPRA* — A very good analysis methodology; extremely thorough; originally developed for oil/gas/chemical facilities but works equally well on any facility; fully scalable; ideal for any type of facility for government, industry, or commercial sectors; and may be used as qualitative or quantitative analysis tool

* Wikipedia.

or a combination of both. Can be used on almost any facility, except where DHS stipulates RAMCAP or CFATS.

API/NPRA is the next best thing to the Full-Scale Sandia Process in my opinion. It uses essentially the same elements but relies on the expertise and experience of the risk analyst for *estimating* the factors rather than precise scientific tests to *scientifically determine* the factors. In the hands of a well-skilled risk analyst, API/NPRA can result in similar results to the Full-Scale Sandia Process. (RAMCAP Plus would be third in my opinion — see below.)

- **CARVER+Shock** — A very weak analysis tool, originally intended for target selection for Special Forces; makes only the vaguest definition of criticality, consequence, and vulnerability; almost useless for most facilities as a complete analysis tool, but may be used as part of API/NPRA for a portion only of asset target value analysis. Not recommended as a stand-alone risk analysis methodology.
- **RAMCAP Framework** — Good analysis tool, but in certain uses it relies on a top-screen process so that DHS can provide a threat assessment for use in the RAMCAP framework.* While having DHS provide the threat assessment helps to assure that such data is up to date, it arguably is less transparent to the client and the analyst. RAMCAP Plus (the ASME RAMCAP software tool) provides the ability to analyze threats independently to some extent.
- **CFATS (Chemical Facility Anti-Terrorism Standards)** — This is a DHS process that is specific to Chemical Facilities. Like RAMCAP, threat analysis is in the hands of DHS.

Now there are two important things to note:

1. Neither the DHS nor any of the methodologies actually require the use of any specific software tool. That is, any software tool, whether commercially available, manually assembled, or simply paper-and-pencil calculations are acceptable to the methodologies and to DHS, as long as the calculations are submitted and supported. That means that if a risk analyst settles on a particular software tool that can support any methodology, DHS will accept use of that tool for analysis.
2. In most cases, DHS does not actually require any particular methodology to be applied to any particular type of facility. (Notable exceptions are CFATS for the chemical industry and the Sandia or ASME RA-S methods which are required for nuclear facilities.) That is, the Sandia model or API/NPRA models that are extremely thorough can be and have been applied to many facility types for which they were not originally intended. As both Sandia and API/NPRA are both recognized as being at the pinnacle of analysis in terms of being thorough, both are ideal candidates for use on all types of facilities. Both are scalable and can be applied simply or to the extreme. RAMCAP is also worthy of consideration.

SUMMARY

It can be seen that the view of the DHS is on communities more than that of individual facilities and structures. DHS has left the definitions for risk assessment methodologies

* RAMCAP Framework Version 2.0, p. 25.

for individual facilities and structures to the interpretation of specific DHS departments (for example, the U.S. Coast Guard for maritime facilities, waterways, and terminals), and DHS has been open to industry input vis-à-vis individual industries and special interest groups.

Risk Analysis for Facilities and Structures

The object of risk analysis is to understand the risks well enough to develop or improve security countermeasures that can effectively deter, detect, assess, delay, respond, and gather evidence of threat actions against the facility in question. The level of deterrence is the sum of these individual countermeasure results combined with the determination of the individual threat actor.

Through the years, various risk analysis formulas have been developed with greater or lesser compliance to this goal. All good risk assessment methodologies include four things:

1. Consideration of Threat
2. Consideration of Probability
3. Consideration of Vulnerability
4. Consideration of Consequences

Better risk assessment methodologies also include methods to guide the analyst toward appropriate countermeasures.

The best risk assessment methodologies also include metrics for assessing the best choice of countermeasures as measured by their effectiveness in countering potential threats.

The very best methodologies also include metrics for assessing the best choice of countermeasures not only from an effectiveness point of view, but also from a cost-effectiveness point of view.

Guidelines for the protection of such facilities include the Homeland Security Act of 2002 and the National Infrastructure Protection Plan (NIPP). These guidelines are useful for determining the criticality and protection measures appropriate for similar facilities in any country in the world and thus serve as a benchmark for protection of such facilities.

Many Interested Stakeholders and Agendas

Many interested individuals and organizations (stakeholders) will express input on how to achieve the objectives of the program. In the case of the NIPP, this includes interests from various branches of the government, such as the U.S. Coast Guard who are responsible for enforcement or standards and guidelines, and also industry and special interest groups. As DHS allows the appropriate branches of the government to dictate the actual risk analysis methodology for the facilities under their purview there is no single standard for risk assessment for critical infrastructure facilities. So, for any particular type of facility, there may be competing risk assessment methodologies that are forwarded by government agencies, national laboratories, branches of the military, industries, and industry interest groups. All of these have put forward risk assessment methodologies for use on CIKR facilities, and DHS has either directly or tacitly approved a wide variety of risk assessment methodologies for use.

Commercially Available Software Tools

Commercial software programs have been developed to support a number of DHS-approved methodologies. It should be noted that DHS does not require the use of any specific software program to perform the analysis.

Risk Analysis Basics

Risk formulas are usually quite simple. Most typically involve: Risk = A Threat Actor with Intent (Probability) * An Exploitable Vulnerability, prioritized by criticality and consequences. In the author's opinion, prioritization should only be on consequences as criticality is only one factor of consequences.

Numerous variations exist, but all formulas result in a ranking of risk by some combination of probability, vulnerabilities, and consequences.

A variation on the Risk Formula is:

- Risk = (A Threat Actor with Intent * Probability * An Exploitable Vulnerability) * consequences; and
- Risk = (A Threat Actor with Intent + Probability + An Exploitable Vulnerability)/3, prioritized by criticality and consequences.

Threat — An active threat actor with the capabilities and intent to do harm to the organization.

Probability — The likelihood that a target has been or will be selected by a threat actor (any asset of the organization that can be attacked in fulfillment of the mission of the threat actor).

Vulnerability — Any condition or factor associated with the selected target that can be exploited to carry out an attack — vulnerabilities may be individual or systemic (e.g., a door left unlocked or poor training of guards).

Different methodologies sort these elements in different ways, sometimes renaming them, but the elements are really always the same.

Risk Assessment Steps

The steps involved in risk assessment include the following:

- Asset Characterization
- Threat Identification
- Criticality Analysis
- Consequence Analysis
- Understanding and Expression of the Vulnerabilities of the Organization's Assets
- Likelihood (Probability) Assessment
- Risk Assessment
- Risk Prioritization
- Risk Management Recommendations

Which Methodology to Use?

The following are some strengths and weaknesses of major methodologies:

- *RAMCAP* — Good analysis tool, but relies on DHS to add threat and asset target value to the client analyst's RAMCAP calculations. Although this ensures that such data is up to date, it is not transparent to the client or the analyst.
- *API/NPRA* — Very good analysis method; extremely thorough; intended for oil/gas/chemical facilities, but works equally well on any facility; fully scalable; ideal for any type of facility for government, industry, or commercial sectors; and may be used as qualitative or quantitative analysis tool or a combination of both. Can be used on almost any facility, except where DHS stipulates RAMCAP.
- *ASME RA-S* — Limited to nuclear facilities only.
- *CARVER+Shock* — Very weak analysis tool; originally intended for target selection for Special Forces; makes only the vaguest definition of criticality, consequence, and vulnerability; almost useless for most facilities as a complete analysis tool, but may be used as part of API/NPRA for a portion only of asset target value analysis. Not recommended as a stand-alone risk analysis methodology.
- *Sandia Methodologies* — Extremely robust analysis method; very scalable; completely scientifically supportable; may be used qualitatively, quantitatively, or a combination of both; ideal for facilities where a very robust analysis is required, requiring very deep analysis of vulnerabilities, though can be used in a less robust fashion. Recommended for high-consequence critical infrastructure facilities.

Neither the DHS nor any of the methodologies actually require the use of any specific software tool. In most cases, DHS does not actually require that any particular methodology be applied to any particular type of facility.

CHAPTER 3

Risk Analysis Skills and Tools

INTRODUCTION

At the completion of this chapter, you will understand all of the skills necessary to perform a comprehensive world-class risk analysis as well as the tools available to help you do that.

You will be introduced to both commercial and self-developed tools, either of which can result in risk assessments that are well beyond the quality of what is average in the commercial security consulting marketplace. But they are not beyond your reach.

For readers interested in developing their own risk analysis templates rather than in using a commercially available program,

- One of the objectives of this book is to help cash-strapped security managers develop a world-class risk assessment tool that is the equal of or superior to multi-thousand-dollar programs. To that end, this book presents a variety of Microsoft Excel templates that I believe generally conform to all of the U.S. Department of Homeland Security (DHS)-approved methodologies listed in Chapter 2. However, any good spreadsheet program can be used to develop the templates. Taken together, they comprise a complete *quantitative risk analysis approach* to fulfill the requirements of any better risk assessment methodology. Each of these templates breaks down the components of threat, vulnerability, probability, and risk into detail, allowing for a very complete assessment. Coupled with *qualitative text* developed from the *quantitative data* of these templates, a very comprehensive Risk Analysis Report can be developed at virtually no software cost (assuming the analyst already has access to Microsoft Excel or similar spreadsheet software). Once the templates are originally developed, they can be used again and again, on project after project with equally excellent results.
- These templates help the analyst through the various steps to analyze risk quantitatively, culminating in a set of charts displaying risk by facility and area which anyone can easily understand. The ultimate charts display the organization's assets arrayed in a prioritized fashion so that anyone can easily see what assets are most at risk and which of those are most critical to the organization. Some tools are useful to help the analyst understand several areas of analysis. For example, the Sandia Adversary Sequence Diagram concept is useful to help the analyst understand vulnerabilities and probabilities and to help select appropriate countermeasures.
- These templates will each be explained throughout this book in enough detail so that any person who has basic competence using a spreadsheet program from

any major software vendor can build his or her own set of templates that can be adapted for all future risk analysis projects throughout his or her long career. The matrices relating to a risk analysis topic are explained within the chapter describing that topic.

- Those readers who are not interested in developing a set of templates as described herein can skip the sections that explain how to build the templates. These are usually contained at the end of each chapter relating to a specific matrix. The balance of the chapter will teach the principles that are useful with any software tool and provide a deeper understanding of the process than is usually available.
- Those readers who are interested in developing a set of templates should read these sections carefully and then develop the matrices one at a time until the entire set is developed. These can be developed all in a single workbook with a separate tab at the bottom for each individual matrix so that a given project includes only a single spreadsheet file with all matrices contained within that one file.
- This book will explain each element of risk analysis and countermeasure selection in terms of its theory, practice, and tools. The book will explain in adequate detail how to assemble MS Excel spreadsheets for each element. Those readers who prefer to use a commercial software tool may skip the sections explaining how to build the Excel spreadsheets. For those interested in building and using their own world-class risk analysis software tool, the first two Tabs on the Excel Workbooks are explained in cell-by-cell detail and after that in adequate detail to build the remaining sheets.

It is typical for security practitioners to present a proposal to conduct a risk assessment in several phases of work. These often correspond to the skills needed to perform the work and also to deliverables (reports) that are presented to the client at the end of each phase of work.

Risk assessment phases often include the following:

- Survey and Research Phase
- Analysis Phase
- Countermeasure Selection and Budgeting Phase
- Report Phase

Deliverables corresponding to these phases often include the following:

- Survey Phase
 - Report — Survey Findings and Immediate Action Items
- Analysis Phase
 - Report or Notice of Completion (including general findings)
- Countermeasure Selections and Budgeting Phase
 - Notice of Completion (and Sometimes a Rough-Order Magnitude Budget)
- Report Phase)
 - Comprehensive Report Usually in Two Phases
 - 75% Report — For Presentation and Review by the Client
 - 100% Report — Including Responses to Client Comments from the 75% Report

SKILLS

Risk analysis requires seven basic skills:

- Skill #1: Gathering Data
 - Get the Organization's Mission Statement
 - Understand the Organization's Programs (Business Units)
 - Assets by Classifications
 - Existing Countermeasures
- Skill #2: Research and Evidence Gathering
 - Interviews
 - Internet Research
 - Records Research
 - Surveys
 - Asset Classifications
 - Historical Data Relating to Security Events
 - Criticalities and Consequences Assessments
 - Telephone Research
 - Bibliography Building
 - Countermeasure Research
- Skill #3: Critical Thinking in the Risk Analysis Process
 - Maintaining Focus on Purpose — Why Examine This? What Is the Issue at Hand?
 - Identifying Key Questions to Be Answered in the Analysis
 - Observing and Understanding the Implications of Different Points of View
 - Examining Evidence and Its Implications on the Analysis
 - Drawing Inferences from the Evidence
 - Concepts Affecting the Evidence
 - What theories, definitions, axioms, laws, and principles or models underlie the issue?
 - What is the reliability of the evidence?
 - What are the effects of personal prejudices on the reliability of inferences?
 - What are the assumptions, and what is their effect on risk conclusions?
 - Drawing Implications on the Consequences of the Risk — What might happen and what does happen?
- Skill #4: Quantitative Analysis
 - Data Classifications
 - Data Input
 - Data Crunching
 - Risk Analysis Result Calculations
- Skill #5: Qualitative Analysis
 - Converting Quantitative Data into Qualitative Data
- Skill #6: Countermeasure Selection
 - Countermeasure Selection
 - Cost-Benefit Analysis
- Skill #7: Report Writing
 - Report Organization
 - Expanding and Explaining Quantitative Data

- Writing Qualitative Sections
- Writing the Recommendations
- Writing the Executive Summary
- Addendums

The tools used in aiding these skills are as follows:

- Tool Set A: Asset Identification Tools (including Consequences Analysis)
- Tool Set B: Probability Assessment Tools (Threats and Asset Target Value)
- Tool Set C: Vulnerability Assessment Tools
- Tool Set D: Risk Analysis Tools

Each one of these skills will now be examined in order.

Skill #1: Gathering Data

All risk analysis is based on the data gathered at the beginning of the risk analysis process. Typically, the analyst includes a survey phase for the purpose of containing the data-gathering tasks together.

All the data to be gathered are related together, so it is often an iterative process. That is, we may interview key stakeholders, conduct surveys of properties, and during the survey find items or issues that we want to go back to the stakeholders with in order to get clarification.

The primary data needed for a risk assessment should include the organization's mission statement, a list of programs they have developed in support of that mission, a list of assets by classification that support the programs, the organization's functional organization chart, the relationship between the business functions and the physical property, existing countermeasures used to protect those assets, and any historical data relating to past security events.

The importance of getting data gathering complete and right cannot be stressed enough. Any failure in data gathering will result in incomplete, insufficient, or incorrect data sources for analysis. Therefore, the analysis could be missing vital information that could point to major risk. Two examples are presented below.

On one project, we noticed that the truck tunnel to the loading dock of a project on an island also contained a chase housing all of the utility services to the entire island. Thus, any major truck bomb would not only result in a massive crater but would also destroy all the utilities to the island, rendering the island and all buildings on it uninhabitable and with no vehicular access to the island.

On another project, we were considering options for controlling access to a property that had a very leaky perimeter with many entrances for vehicles and pedestrians of all types. We finally developed what we thought was a workable scheme to screen visitors and employees when we were informed that there was an off-site employee parking lot that would create a traffic flow of hundreds of employees every day into and out of one of the screening points that we had not accounted for. This threw off our entire throughput calculations and made our scheme unworkable. The truth is in the details.

- *Interviews:* Most basic data can be gathered in initial interviews. Follow-up interviews may also be required as new information comes to light in the survey and research process.

- *Types of Data Required:* We will now examine the types of data we need and review the skills and work processes needed to accumulate all the data. Remember, it will be from this data alone that all of our analyses, risk conclusions, and recommendations will derive, so completeness is essential.

Get the Organization's Mission Statement

Few security consultants bother with the *organization's mission statement*, but it is foundational to understanding everything else about the organization. The organization grows entirely out of its mission statement. That is, every program, every asset, every business process, every customer served, and every action taken by the organization are in support of its mission statement. Every function of every asset and employee, contractor, and vendor is in support of the mission statement. The organization's mission statement relates to asset target value calculations. That is, how attractive is this organization to various types of attackers? Different threat actors select their targets primarily based on the organization's mission statement. For example, nongovernmental organizations (NGOs) working in high-threat zones may all be subject to attack by insurgents, but those who have a mission statement that includes the goal of proselytizing for a religion different than that of the insurgents may be most at risk (and in my opinion should not be there, as they arrogantly disrespect the sensitivities of the local culture and in so doing put many other lives than their own at risk, including those who are working to help the local populace in a much more respectful manner). So, get the mission statement.

Understand the implications of the mission statement. Mission statements can be either lofty or humble, or convoluted or direct. One organization I knew joked that their mission statement was “piles and piles of cash!” Another had a heartfelt goal of bettering the community through its services. So, each mission statement contains clues about management attitudes and goals. By examining these attitudes and goals against the reality of the workplace, one can also judge the sincerity of the mission statement. The organization that joked about *piles and piles of cash* ended up abandoning their initial business plan of security consulting and became a security integrator when the first multimillion-dollar opportunity presented itself. By abandoning their original mission statement, they became unfocused and transitioned to a business model they did not understand, ultimately not well serving their customers and (arguably) their reputation in the local marketplace. As in the marketplace, organizations that do not act in concert with their mission statement often develop competing programs that make the job of security much harder.

Competing programs and business agendas also often result in unfocused applications of other supporting programs, including security programs. Those organizations may pay lip service to security while actually doing little that actually supports a secure environment.

The consultant who does not fully understand and appreciate the organization's mission statement and compares it to the reality on the ground will surely miss the point when analyzing risk.

Understand the Organization's Programs (Business Units)

Deriving from the organization's mission statement, the first agenda of any organization is to develop programs in support of that mission. From the programs, derive all assets of all types, and all of the *organization's business processes*.

The role of security in an organization is to assist in protecting these assets and business processes from potential threat actors and hazards. The key to understanding

the programs and business processes is in the organization's *functional organization chart*.

It is important that the reader is aware that functional organization charts do not always tell a true story. It is strongly recommended that the security risk analyst ask first what programs the organization has established to support its mission statement. If one relies solely on the functional organization chart, or if one asks and receives the functional organization chart before asking what programs the organization has put in place in support of its mission, it is very likely that the client's respondent will simply point you to the functional organization chart, which may have errors, flaws, missing elements, and deviations from the real set of programs. For example, it is often surprising to discover that the security organization is not listed on the organization chart. This is because it is not a program in direct support of the mission but is one of the several programs in "dotted-line" support of the mission. That is, it is a program that supports programs that directly support the mission.

This is also a critical example of how the organization's management thinks and approaches organization, program development, and problem solving in general. The degree to which the functional organization chart accurately reflects all of the actual programs is telling into how the organization approaches its program development and problem solving in general. You will likely see this reflected in how the organization approaches the recommendations of the Risk Assessment Report later.

Assets by Classification

There are four major classes of assets (see also Figure 3.1):

1. People
2. Property
3. Proprietary Information
4. Business Reputation

People Itemize each type of user in the building. Users will typically include the following:

- Key Senior Management
- Management and Employees
- Contractors
- Vendors
- Visitors
- Customers

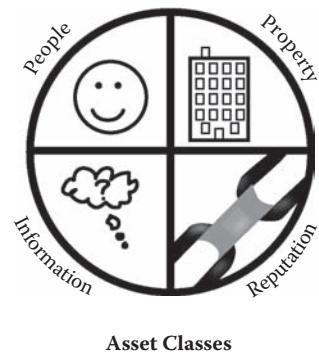


FIGURE 3.1 Asset Classes

You will need to note the occupancies (where they work and interact), the hours of occupancy, tasks, uses of hazardous materials or equipment, their needs for access, and their frequency of access. It is also important to note any classic or specific threats against these people.

Property Classify the organization's property in the following ways:

- *Real Property*: Real property (land and buildings) should be classified by its location and purpose (what business units does it serve), and what type of property it is (office building, office suite, bridge, airport hangar or terminal, warehouse,

maintenance yard, vehicle storage yard, etc.). Larger organizations will have many locations and types of buildings. These should be categorized by type and size of facility in a spreadsheet and mapped.

- *Vehicles:* Company-owned, leased, and privately owned vehicles on company or company leasehold property (office building parking lot).
- *Equipment:* Equipment can include information technology systems (file servers, etc.), other office equipment (such as copiers, printers, and so forth; furniture, cash registers, etc.). For most projects, a detailed list is not necessary, just a set of categories and their general locations.

Proprietary Information Proprietary information is unique to this organization and facilitates the conduct of business and should not be available freely to the public or competitors. Classify the organization's proprietary information as follows:

- Information Technology System
- Security System
- Voice Communications System
- Paper Files (also including Vital Records)

The location, quantity, and type of information should be noted, as well as its sensitivity and criticality.

Business Reputation The organization's *business reputation* should be characterized from several points of view, including the following:

- Senior management's characterization
- Management and employees' characterizations
- Contractor/vendors' characterization
- Several customers' characterizations

Gather the good and the bad and categorize them according to the sources and characterizations onto a small spreadsheet.

Existing Countermeasures

In interviews, try to determine the organization's security program. This will include the following:

- Mission statement and goals of the program
- Security management (including their qualifications, skills, and training)
- *Hi-tech elements:* Electronic security program (alarm/access control system, photo-ID system, security video system, security communications systems including radios and intercoms, etc.)
- *Lo-tech elements:* Access-controlled and nonaccess-controlled gates, doors, and barriers; lighting; signage; property-marking system; key-control system; etc.)
- *No-tech elements:* Policies and procedures, guard patrols and posts, trained dogs, investigation programs, law enforcement liaison program, security awareness program, emergency preparedness program, disaster recovery program
- Future plans
- Historic security events

Skill #2: Research and Evidence Gathering

All analysis is based upon information and evidence. Information and evidence can be gathered in numerous ways, including the following:

- Interviews
- Internet research
- Telephone research
- Surveys
- Asset classifications
- Historical data relating to security events
- Criticalities and consequences assessment
- Bibliography building
- Countermeasure research

Interviews

Conducting interviews is more than just making a list and checking it twice. Interviews are a skill, science, and art. The following are key elements*:

- Preparation for the Interview
 - Choose a setting with few distractions. Avoid settings with loud noises. (I once had to conduct interviews next door to a construction site that was driving piles into the earth. It was nearly impossible for anyone in the room to stay on point.) Additionally, try to avoid interviewing people in their offices, as it is a sure bet they will be distracted by phone calls and people walking in.
 - Explain the purpose of the interview.
 - Cover any terms of confidentiality.
 - Explain the format for the interview.
 - Indicate how long you expect the interview to take.
 - Invite them to contact you later if they remember anything relevant that was missed in the interview.
 - Ask them for any questions they may have.
 - Record the interview by taking notes or tape recording. It is best to dedicate a specific person to take notes.
- Types of Interviews
 - *Informal, conversational interview:* Some interviews are best held as informal discussions. This is generally true of any top management, as they usually do not have time for extended, structured interviews. These will be held with other management and staff.
 - *Closed, structured response interview:* Some practitioners prefer to use a series of structured questions. These are useful as they can be on handouts that the interviewee can easily follow. Looking ahead, he or she can also have time to formulate more meaningful responses to upcoming questions.
 - *Guided interview:* Most of my interviews are guided interviews. These are notable by a series of topics rather than specific questions. This allows

* Interviewing techniques here are adapted from www.managementhelp.org/evaluatn/intrview.htm, General Guidelines for Conducting Interviews, by Carter McNamara, MBA, Ph.D., Authenticity Consulting, LLC, and adapted from the *Field Guide to Consulting and Organizational Development* (Robbinsdale, MN: Authenticity Consulting, LLC, 2006).

straying from a topic in order to amplify a point or go to something noteworthy but not exactly on topic.

- *Open-ended interview:* Open-ended interviews can be held with management and incidental employees. For example, I often stop during a survey and ask questions to employees who seem willing to facilitate. While asking questions about the facility and its use, I may also interject questions about the company's mission, security habits, and so forth. These can be most illuminating as one can often get "the unvarnished truth" from such interviewees.
- Types of Questions
 - *Background:* It is good to begin an interview with a few background questions. I usually focus on how that person came to be in their position (early training, education, choice of career, choice of company, progress within the firm, challenges, working conditions, etc.).
 - *Knowledge:* This is the heart of the interview. What does the person know to be true about the topics or questions? Knowledge is provable and confirmable. No opinions should be entered here.
 - *Opinions/Values:* Any opinions should be noted as such, differentiating them from provable knowledge. Opinions have value. Opinions focus on what should change, not just what is.
 - *Feelings:* Ask how the person feels about a condition, a topic, and so forth.
- Sequence of Questions
 - Get the interviewee involved and focused on the topics as soon as possible.
 - Gather facts before asking about any opinions or conclusions.
 - Ask questions about the present before asking questions about the past or future. This gives context, and it is usually easier for someone to talk about the present.
 - Get the person's point of view about the topics.
 - Allow and encourage the interviewee to provide additional information of his or her own preference and expand on the interviewee's opinions about what are the problems to address and what should be done.
- Wording of Questions
 - Generally, questions should be open-ended.
 - Questions should be as neutral as possible, avoiding any questions that might influence their answers. For example, never ask something like "I don't think these people should be allowed to ..., do you?"
 - Ask questions one at a time, not compounded together.
 - Word questions clearly, using simple sentences. Define any special terms involved in the question.
 - Watch out for "why" questions. These imply a cause and effect that may not actually exist. Such questions may also cause the interviewee to become defensive, in that he or she may feel it necessary to justify his or her response. This can inhibit the interviewee's response to future questions.
- Conducting the Interview
 - Be professional but engaging. Everyone likes to open up to a person he or she feels welcome with; conversely, few open up to interviewers who are "stuffed shirts."
 - Occasionally verify that notes are up to date or that the tape recorder is working.
 - Ask one question at a time.

- Remain as neutral as possible. It should not be possible for the interviewee to sense any agenda on your part. Act as if “you’ve heard it all before.”
- Encourage responses with occasional nods, and confirmations.
- Recorders or note-takers are better than notes taken by you. Whenever you take a note, the interviewee also notes that that answer is of interest to you. This can affect the interviewee’s future responses.
- Provide a transition between major topics. “Let’s move on to...”
- Keep the interview on topic. Do not lose control of the interview. For example, do not let the interviewee stray off topic, take so long to answer questions that time runs out, or begin asking leading questions of you. This can come at the end of the interview if you are willing.
- Follow-Up
 - Verify that the tape recording or notes are complete.
 - Clarify any vague notes.
 - Write down any observations made during the interview, such as were there any surprises in the interview, where did the interview take place and at what time, and did you notice any deception or unwillingness to cover any topics.

Internet Research

Research is the key to credibility in reports. Every source of data, especially controversial data, and every inference, implication, or conclusion should have solid reference to concepts, theories, definitions, axioms, laws, principles, models, and credible sources. Research is also the key to good conclusions. Research ferrets out valid and invalid points of view, relevant and irrelevant issues. Research helps the analyst understand the data at a level of depth and breadth not possible with only interviews and surveys.

When you are creating a risk analysis, research should be conducted into the organization’s mission, history, key stakeholders, and industry and criminal history vis-à-vis attacks against its assets.

- Research on the assets can be conducted on the Internet using online tools, such as: Lexis/Nexis (www.lexis-nexis.com)
- HighBeam Research® (www.highbeam.com)
- Bedford/St. Martin’s (www.dianahacker.com/resdoc/)
- Questia (www.questia.com/Index.jsp)
- Purdue University’s CORE (Comprehensive Online Research Education) (<http://gemini.lib.psu.edu/core/login/login.cfm>)
- Rand Research (www.rand.org)
- University of California, Irvine — Criminology, Law, and Society (<http://www.lib.uci.edu/online/subject/subpage.php?subject=crim>)
- McAfee® (http://www.mcafee.com/us/research/criminology_report/default.html), www.Google.com, and www.amazon.com (see also Figure 3.2)

Anyone who uses Google® has a pretty good sense of how to conduct online research. The methods are usually simple and straightforward. Most online research tools search periodicals, books, and professional and academic papers. Google also searches for Web pages, images, news, and shopping. Google is also a good source of information for road and satellite maps relating to organizations worldwide.



FIGURE 3.2 Internet Research

Most of these tools permit searches one of two ways: basic or advanced. To perform a basic search, one simply enters the search criteria in the search field. Simple searches can be conducted by entering all of the search criteria. In response, most search engines produce a results page, which is a list of references related to the search terms, generally with the most relevant searches nested near the top of the search.

More advanced searches can be conducted in several other ways:

- *Choosing Search Terms:* Choosing the correct search terms is a primary key to finding the information you need. Start with the obvious, the industry, for example *Oil*. Then add a more specific term, for example, *pipeline attacks*.
- *Framing:* You can also look for exact finds by “framing” the search to assure that the exact phrase contained within quotes “oil pipeline attacks” will be searched for, which will exclude everything except those results that contain that exact phrase.
- *Exclude Words:* You can exclude certain terms by adding a minus sign in front of a word you do not want the search engine to find results for. For example, *oil pipeline attack — gas*.
- *Site-Specific Search:* Even if a Web site does not support searches for content that matches a certain phrase, Google can search the entire site for you. Enter “site:something.com” after the search string. For example, “*oil pipeline attack*” *site: www.something.com*.
- *Similar Words and Synonyms:* Enter the tilde sign “~” before the word you want to find similar words or synonyms for. For example, “*oil pipeline*” ~attack.
- *Specific Document Types:* If you want to find a particular document type, such as *pdf* or *ppt* files, enter “*oil pipeline*” ~attack filetype:*ppt*.
- *This OR That:* By default, Google searches for Web sites that contain all words. If you want to find just this or that, enter “*oil pipeline disaster*” OR “*oil pipeline attack*.” The word OR should be uppercase.
- *Phone Listing:* You can find a person or organization’s phone number or find who owns a phone number. To find an organization’s phone number, enter *contact “organization name” OR phone “organization name.”* To find who owns

HighBeam RESEARCH More than Search ... it's Research

Hello, Thomas. You are a Full Member. [Log out](#)
[My account](#) | [Preferences](#) | [Help](#)

Library Web Reference < 3 ways to research Text size: T T T T

Advanced Search

Search: oil pipeline attack

and these words: terrorist

or these words: theft

exclude these words: qas

Publication types:

- Almanacs
- Books
- Dictionary
- Encyclopedias
- Magazines
- Maps
- News Wires
- Newspapers
- Pictures/Images
- Press Releases
- Thesauruses
- Transcripts
- White Papers

Dates: All Dates through (mm/dd/yyyy format)

Author:

Article title:

Search within:

- All publications or only the publications selected below
- Exclude the publications selected below

Search

FIGURE 3.3 Advanced Search Example

a phone number, enter phonebook: 617-555-1212 (note this number does not work, use a real phone number).

- *Area Code Look-Up:* To find the area from which a telephone's area code is located, enter the area code (e.g., "617").
- *Answer to Life, the Universe, and Everything:* You can also look this up on Google, but I will just give you this answer: 42.
- *Advanced Searches:*
 - Google also has an Advanced Search function that is to the right of the Google search field under www.Google.com and www.google.com/ig (which is a wonderful Web site that consolidates Google Calendar®, Gmail®, date/time/news/weather, and other useful tools). The advanced search fields include many variations and exclusions that are useful.
 - Certain research Web sites facilitate highly detailed searches. One of the best of these, as mentioned earlier is Highbeam Research (Figure 3.3). Each research Web site has its own protocols but generally includes most of the categories below:
 - General search terms
 - Exclusions
 - And/OR functions
 - Synonyms
 - Sources from which to search
 - Specific sources (individual magazines, for example)

Telephone Research

Much research can also be conducted by telephone. You can find additional sources for information by asking key stakeholders who they think might know this information. Many times, they will have the contact and phone number handy and may be willing to make introductions for you. Telephone research is particularly valuable when you have to confirm or expand on knowledge about a contractor's contribution to the organization. For example, to get information from a shipping company, information technology consultant, or support vendor.

Records Research

Certain information can only be obtained through records research. Examples may include police records, crime statistics for a given facility, and questions of ownership or lease terms. For some sites, the applications of certain countermeasures are constrained by lease terms. For example, if a fourth-floor tenant of a twelve-story building wants to place electronic turnstiles in the main lobby, this affects other tenants, and so clarification of leasing terms and management willingness are necessary to confirm.

Surveys

Like interviews, surveys are the backbone of information gathering. Unlike interviews, surveys rely mostly on your own observations and expertise. Surveys can also be combined with interviews where a risk assessment of many facilities is involved, thus saving numerous repeat trips. Surveys deserve a checklist, but do not feel constrained to stay on point, just be certain to cover all the points. During surveys, you will likely find many unexpected things.

- **Notes:** Notes not only help us remember what we saw, but also help us to add context, thus helping us remember things that were not noted. This is an important principle. The very act of taking down a note helps us to remember things that we saw, heard, or concluded which occurred in the general time frame of the note. Thus, a single note can help us remember a dozen things or more that are not related to the note. Notes should be taken for the following:
 - Key concepts
 - Architectural, landscaping observances
 - System observances (condition, age, technology, brands, models, etc.)
 - Operational observances (the operations of both the security group and the overall organization)
 - Cultural observances (the business or regional culture has a profound effect on what sorts of countermeasures will be accepted)
 - Points of view expressed by stakeholders, including users (these should be sought out)
 - Detailed notes on existing console rooms, including all security system equipment and the nature and equipment in the room, including noise level, activity, other equipment available, and so forth
- **Photos:** Take many photos or videos. Invariably, the one thing I need a picture of most is the thing I thought was too unimportant to shoot during the survey. Shoot



FIGURE 3.4 Pocket Digital Light Meter

everything whether it seems relevant or not. Video can be most helpful as you may capture a fleeting image of that thing you did not think you would need as you pan across from one thing to another. I use a 12-megapixel camera with a 150-degree field-of-view lens for all indoor and much outdoor work. This allows me to zoom in digitally to see details that I thought were irrelevant at the time of shooting.

- *Files:* Save photos and notes in a file. Digital files are better as they can be edited and inserted into reports more easily.
- *Day/Night:* Conduct the survey during the day and the night. Everything changes at night, including the lighting, character of the workforce, quantity and quality of employees, the way they work and interact with each other, the public and access points, and so forth. Take lighting levels using a quality light meter. My personal favorite is the Pocket Digital Light Meter type, which typically ranges down to 0.1 Fc (foot-candles) up to 2,000 Fc (Figure 3.4). Accuracy is acceptable, and cost is low. Additionally, these light meters have a separate sensor and display, separated by a 1 meter or so cable, so readings can be taken accurately and seen readily without affecting the sensor. Any good meter will do.

Asset Classifications

The risk analysis is measured as the risk of an unwanted event happening to any of the organization's assets. See Chapter 5 on assets for a detailed description.

Historical Data Relating to Security Events

For criminal threats history, it is useful to research the history of crimes at the location, for the client's industry or for the client's other similar facilities. Location criminal history can be obtained from the local police database or from a commercial source such as CAP Index®. History of crimes against the client's industry or against the client's other properties may be obtainable from Internet research, or from the client's own security department.

Criticalities and Consequences Assessments

Each asset has two criticality factors. The first factor is the asset's criticality to the mission of the organization, and the second is the lost time and productivity, and cost of recuperating the asset if damaged or lost. Actually, the first element is criticality and the second is the consequence. Only the client can determine criticality, although the security analyst may estimate criticality in the absence of client input on the subject.

An asset's criticality to the mission of the organization is gauged by how severe the organization's operations would be damaged if the asset is lost or severely damaged. Certain assets are critical to the mission of an organization. For example, in small organizations, the key management may be critical. The loss of their expertise, strategic insight, and so forth, could spell disaster for a small organization. For larger organizations the critical asset could be a key facility, business process, or formula. For example, a software manufacturer's business would be severely disrupted if the source code to their operating system or software suite were openly available. Likewise, military or marketing strategy could be a critical asset, and its compromise could spell military or market defeat at the hands of enemies or competitors. In 2008, during the credit crisis, automakers found it nearly impossible to finance cars and trucks as their credit sources dried up. As few customers can pay cash for a new vehicle, this had an immediate and severe impact on auto and truck sales. To determine critical assets, one must be open-minded and look at the whole business process, including all kinds of suppliers. This is an example of where critical thinking (see Chapter 4) is important, because it places a focus on assumptions. Few automakers were prepared for the credit crunch because they had assumed that credit availability was a given. Nothing in the business process is a given.

Certain assets may not be critical to the mission of the organization in its initial loss (that is, the organization could continue to operate for a while by working around the asset's loss by depending more on other assets), but the loss of the asset could compel the organization to replace the asset at a cost so great, or a time cycle so long as to make continued normal operations impractical. For example, during the October 17, 1989, San Francisco earthquake, many businesses were disrupted when transportation bridges and elevated motorways collapsed. This had a knock-on effect in the transit time for workers living across the water or who had always depended on those motorways. As employees failed to be able to get to work in a timely manner and the long time durations necessary to repair the motorways became more apparent, the critical employees looked for other employment nearer to home rather than looking for new homes nearer their work. Many businesses that depended on employees with special skills were severely disrupted as it was often those employees who commuted the farthest across those bridge and motorways. Those businesses and employees had always assumed that the transportation corridors were a given. Nothing in the business process is a given.

Bibliography Building

As research accumulates, it is helpful to build a bibliography of books and articles. When conducting Internet research, it is helpful to print the reference Web page or article to a PDF* file and save it under the project directory in a subdirectory named *Bibliography*. A

* PDF stands for Portable Document Format, invented by Adobe Systems® in 1993 for universal document exchanges in a manner that is completely independent of any hardware, software, or operating system and not requiring any costly application software to view. PDF is an open standard and conforms to ISO 32000-1:2008.

good practice is to code-name the file for a keyword lookup. This is particularly helpful for references to Web sites, articles, and papers that can vanish from the Internet over time. This ensures that if a reference is challenged, it is easy to access and prove.

Countermeasure Research

Research on appropriate countermeasures is a science and an art, requiring significant skills to find correct products for unique applications. This is by no means comprehensive, but the key elements are as follows:

- Determine an available range of possible countermeasures, including *hi-tech*, *lo-tech*, and *no-tech* options.
- One way to do this is to use Google and enter the specific vulnerability and the word *countermeasures* — for example, if one enters the phrase “B&E* door vulnerability countermeasures,” many references are given. One is www.spymall.com/catalog/library-lock.htm, which is a library of locksmithing, including a reference to many books on techniques of *breaking and entering* and a range of effective countermeasures to those methods and tactics.
- If research is needed on a specific type or manufacturer of a specific countermeasure, this can be found by searching Google for variants on the name of the countermeasure or its possible product name, on the vulnerability the countermeasure is designed to address, or by searching *ASIS International’s Seminar and Exhibits Final Program and Exhibits Guide* (for a comprehensive list of security industry manufacturers and service providers) and *ASIS International’s Security Industry Buyers Guide*®, both of which are briefs of offerings of the entire security industry. The *Security Industry Buyer’s Guide* can also be found at the following Web site, which is worth bookmarking: www.sibgonline.com/public/subcatl2.asp.
- Regarding bookmarking, it is important to organize browser bookmarks into categories using the *Organize Bookmarks* function of Firefox® or the *Organize Favorites* function of Microsoft Internet Explorer®. The *Firefox Foxmarks* function also synchronizes home, work, and laptop computer browsers so that the same bookmarks are available on all and are continuously updated.
- It is most helpful to build a library of useful manufacturer Web sites, and routinely copy all of the product data sheets you find on the Internet into a directory of reference products, services, and security solutions. To do this, one needs a PDF printer or writer (many are available online, including some that are free downloads — search for *PDF printer* or *writer* on Google). The extra time it takes to print the data sheet and file it away is time well spent the next time you are looking for that unique wall-mounted duress button, automatic security electronic turnstile, or DHS-rated vehicle crash barrier, and you just cannot remember the name of the product or manufacturer.
- It is very important to have a copy of and subscribe to *ASIS International’s Protection of Assets Manual*®, (*POA Manual*), which is itself a basic library of security strategies and solutions. The hard copy is valuable as a quick reference, and the online copy is searchable. One cannot get the whole story of the POA manual in the online version. The hard copy is good to have.
- Additionally, a good library is critical to a security practitioner’s professional development and acts as a powerful research tool. One should buy books

* B&E stands for Breaking and Entering.

voraciously. It is money well spent and will save countless hours of searching for that one thing you remember seeing on the news or Internet but cannot find. Usually, it was written about in a book. There are many excellent books in the footnote sections of each chapter of this book that together form the foundation of an excellent security library.

Skill #3: Critical Thinking in the Risk Analysis Process

See Chapter 4 for a detailed discussion on critical thinking and its application to the risk analysis process. The essentials of critical thinking as it applies to risk analysis are covered in detail, including the following:

- Maintaining Focus on Purpose — Why examine this? What is the issue at hand?
- Identifying Key Questions to Be Answered in the Analysis
- Observing and Understanding the Implications of Different Points of View
- Examining Evidence and Their Implications on the Analysis
- Drawing Inferences from the Evidence
- Concepts Affecting the Evidence
 - What theories, definitions, axioms, laws, and principles or models underlie the issue?
 - What is the reliability of the evidence?
 - What are the effects of personal prejudices on the reliability of inferences?
 - What are the assumptions, and what is their effect on the risk conclusions?
- Drawing Implications on the Consequences of the Risk — What might happen and what does happen?

Skill #4: Quantitative Analysis

There are two forms of risk analysis — *quantitative* and *qualitative*. In the simplest form, Quantitative analysis has to do with the measurement or estimation of a thing, and qualitative analysis has to do with the description of its characteristics, attributes, features, or value.

A debate has raged for decades over the merits of one versus the other. The debate originated in the science of sociology and has expanded into many other sciences, including risk analysis. The debate rose to prominence in the 1970s through a backlash against the priority attached to scientific or positivist methodology in sociological textbooks. Attempts to reconcile the two points of view date back to Michael Mann (in the journal *Sociology*, 1981).*

Quantitative analysis is based upon quantitative (numeric) data. The terms *data crunching*[†] and *data mining*[‡] both relate to quantitative analysis. The idea of quantitative analysis is that if one can examine a problem from enough points of view and measure or estimate each of those elements, one can understand enough about it to make

* John Scott and Gordon Marshall, eds., *A Dictionary of Sociology* (Oxford: Oxford University Press, 1998).

[†] Jean J. Schensul and Margaret Diane LeCompte, eds., *Ethnographer's Toolkit* (Lanham, MD: AltaMira Press, 1999), 195.

[‡] Associated Content, Don Rainwater, "The Benefits of Data Mining in Qualitative & Quantitative Research," November 28, 2007, "Data mining is the process of sorting through large amounts of information to find patterns or symbolic clusters of information"

valid conclusions. For example, nearly every university that teaches geology begins by teaching students how to classify rocks into their shapes, textures, colors, density, mass, and hardness. All other aspects of geology are built on this fundamental understanding. Quantitative analysis is built on classification and measurement or estimation.

- *Data Classification:* Data must be classified into their constituent components. In risk analysis, one classifies assets, threats, vulnerabilities, and probabilities; and then risk can be estimated.
- *Data Input:* Once classified, data about the assets, threats, vulnerabilities, and probabilities must be gathered or estimated and input. Data estimates are in the form of numbers or estimates, usually along a range of least to worst. Each data entry cell is a point of analysis, as it represents consideration of a factor of an asset, threat, vulnerability, or probability.
- *Data Crunching:* Raw data (the input) must be crunched (calculated) in some meaningful way to reach conclusions. This is often a two-step process with step 1 being sums, multiples, averages, and so forth, of the data inputted, and step 2 being the setting up and running of structured query language (SQL) algorithms that bring meaning to the data.
- *Risk Analysis Result Calculations:* Meaningful calculations can be concluded from this by ranking the results of the data crunching.
- DHS-approved risk analysis methods all use some measure of quantitative analysis.

Quantitative analysis is always a component of qualitative analysis, even when the quantitative analysis is not forthright (not calculated). The analysis must perform some quantitative analysis in order to reach any meaningful conclusions about the assets, threats, vulnerabilities, and probabilities.

Skill #5: Qualitative Analysis

Qualitative analysis has to do with the description of its characteristics, attributes, features, or value and the estimating of those values in general terms (low, medium, high, etc.). In the end, data only have meaning qualitatively. Most commonly, qualitative analysis is based on observer impressions of relatively small (presumably representative) samples. Thus, qualitative data are often subjective, as the data are the analyst's interpretation of the research and analysis. But that, in fact is the point of analysis, to reach a conclusion about what to do about the issue. Every risk assessment uses qualitative analysis as the act of writing the report and its conclusions and recommendations.

Presumably, the analyst should know enough about the subject to reach valid conclusions. Unfortunately, most analysts are not trained or skilled in critical thinking, and without that training, any analysis will almost certainly be based upon assumptions, biases, and preconceptions. The data are too often used to support an original conclusion, which was reached before gathering the data. Qualitative analysis can be prone to significant flaws unless the analysis is based on critical thinking processes. In such cases, qualitative analysis is often conducted from a basis of quantitative data. I believe that the best reports are the result of both quantitative and qualitative approaches. Quantitative data can sample very large quantities of data, a qualitative analysis usually focuses on a small (hopefully representative) data field. The use of quantitative data helps ensure that

the small data sampled for the qualitative analysis is truly representative, relevant to the issues and less biased by personal prejudices.

Converting Quantitative Data into Qualitative Data

Data versus Information For analysts who use the dual analysis approach, one must collect and process quantitative data and then process it into meaningful information. Data are only plain facts, but information is actionable. Data are abstract; information has focus. Information is a collection of data that are interpreted and processed to determine meaning; then the data are useful and become information.

Quantitative analysis should be conducted in a way that computes averages, sums, or multiples of the raw input points and then ranks that data into highest to lowest. This provides the analyst with a comparison of the data that is useful to determine which data are most relevant and important.

Skill #6: Countermeasure Selection

Chapters 15, 16, and 19 all deal with countermeasure selection from three distinct points of view. Chapter 15 focuses on the goals of countermeasures. Chapter 16 explains the three types of countermeasures and gives examples of many, including their applications, capabilities, and exploits. Chapter 19 introduces a Countermeasure Selection Tool that helps focus the analyst and client on the best type of countermeasure for a particular vulnerability.

Countermeasure Selection

The whole idea of security is to understand risks that could be exploited by potential threat actors and to create measures to counter the potential threats (i.e., countermeasures). There are three broad types of countermeasures: *Hi-tech*, *lo-tech*, and *no-tech*. Hi-tech (electronic) countermeasures employ electronic systems to deter, detect, assess, and assist in the response and to collect evidence. Lo-tech solutions include locks, barriers, lighting, architectural, and CPTED* solutions. No-tech solutions include policies and procedures, security staffing, training, awareness programs, investigations, and security dogs.

These three types of solutions should be used in combination to address vulnerabilities to achieve multiple layers of protection. The most valuable assets should be protected by multiple layers, from the outer perimeter inward.

The key elements of protection include the following:

- *Access Control*: Limiting access to vulnerable assets only to those who have a legitimate need to access them.
- *Deterrence*: Creating a psychological impression that the risk of acting as a threat actor could be greater than the reward, either through creating the possibility that the threat action may not succeed, or that the threat actor may be caught and penalized.

* CPTED stands for Crime Prevention Through Environmental Design. “CPTED is the proper design and effective use of the built environment which may lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life.” (Dr. C. Ray Jeffrey, National Institute of Crime Prevention — <http://www.cptedtraining.net/>)

- *Detection:* Creating detection technologies that can alert a security staff of any unwanted or inappropriate activity within their purview.
- *Assessment:* Technologies that can help the security staff assess what has been detected to determine if it is a real threat or just a false alarm.
- *Response Including Delaying Technologies:* A variety of responses can be mounted to legitimate threat actions, including the response of security staff, voice communications from a console to a threat actor to warn them away, delaying technologies such as deployable barriers, and aggressive responses to aggressive threats (automated weapons, etc.).
- *Gathering Evidence:* Closed-circuit television (CCTV) systems and audio systems can gather evidence for prosecution and training.

Cost-Benefit Analysis

It is not enough just to determine a range of possible countermeasures, but one must also select the ones that are most appropriate. Appropriateness can be measured in two dimensions: *effectiveness* and *cost*.

- *Effectiveness* can be assessed by the potential countermeasure's ability to perform the six roles above. (I break the assessment down into seven roles, including the countermeasure's ability to delay an intruder.) Each countermeasure can be estimated to be able to perform one of these six functions less or more effectively.
- *Cost* is the second factor. The two factors together create the function of cost-effectiveness. Thus, in the comparison of any two countermeasures that are equally effective, the one with the lower cost is more cost effective.

Skill #7: Report Writing

Report writing is one of the most critical skills of a good risk analyst. Analysts who cannot write well cannot communicate their analyses effectively and, thus, are less effective analysts.

Chapter 20 focuses entirely on effective report writing. The keys to effective report writing include the following:

- Report Organization
- Expanding and Explaining Quantitative Data
- Writing Qualitative Sections
- Writing the Recommendations
- Writing the Executive Summary
- Addendums

Tools

In order to perform analysis, a risk analyst must have tools to collect and analyze the pertinent data. This can be done by simply using a notepad and pencil or by using a software tool. Many commercially available software tools have been developed, both great and small, ranging from the economical to the very expensive. Additionally, many analysts who perform analysis frequently have developed individual software tools to perform the analysis that are as effective as commercially available tools. I do not wish to say that either commercial software or custom software templates are better or worse than

the other, you can judge for yourself. However, so many other analysts have asked me to explain my approach that I am presenting it for open copy by anyone. It is based upon a Microsoft Excel template that I developed and is among the most thorough quantitative analysis tools that I have ever seen, exceeded only by a deep Sandia team analysis, costing many times more. Arguably, a couple of commercially available tools are as effective, but they cost thousands of dollars. The Excel template tools that are illustrated in this book are not meant to be the only solution, but they should be used as an exemplar of what a good tool should do. Any software tool that embodies the characteristics of these template tools will do the job, including sophisticated formally written risk assessment software costing many thousands of dollars.

Analysts who select more economical software options should assure that they perform all of the analysis illustrated in the tools that follow in this book. Most economical software tools do not and thus fall short of the objective of actual analysis, but should rather be considered risk-estimating tools. There is nothing wrong with using risk estimating tools for simple projects on low-risk facilities, but one should not expect the results of actual analysis. That is, one should expect that undiscovered risks may exist against which no countermeasure has been programmed and that certain of those risks could be severe and could result in a catastrophic lapse of security programming, possibly costing careers and even lives.

Analysis is a process and is not inherently dependent upon any specific tool. Thus, these tools have been developed to illustrate the risk analysis process and provide a cost-efficient and very effective means of accomplishing that task. The use of far more expensive software may be appropriate, depending upon the budget and circumstances of your particular organization, and it is not my intent to dissuade any reader from obtaining and using more sophisticated software tools.

Commercially Available Software Tools

- **SVA-Pro®:** One of the best of the commercially available tools is SVA-Pro. SVA-Pro was developed by Dyadem International Ltd. (a Canadian firm), largely in response to the requirements of AcuTech Consulting Services®, one of the finest risk-consulting firms in the world. AcuTech was founded by David A. Moore, PE, CSP. SVA-Pro is one of a suite of software products which were developed to address a wide range of industry risks. I have used SVA-Pro, and it is a highly competent tool, once formatted for the specific needs of the project. The software requires significant customization (which is possible through paid training from Dyadem, or by Dyadem in response to submitted criteria with one of their paid support packages). The software is highly difficult to customize without the direct and costly support of Dyadem, which seems to wish to compel its users to receive both support and training in order to receive adequate support to customize the program to specific project needs. (Personal opinion of author, also supported by other SVA-Pro users I have spoken with.)

Once configured SVA-Pro creates voluminous quantitative data. SVA-Pro has industry standard templates for Center for Chemical Process Safety's (CCPS) Security Vulnerability Analysis (SVA), American Petroleum Institute/National Petrochemical and Refiners Association's (API/NPRA) SVA for petroleum and petrochemical industries, and Risk Analysis and Management for Critical Asset Protection (RAMCAP). SVA-Pro is arguably one of the finest commercially available risk analysis tools.

- **RAMCAP Plus®:** RAMCAP Plus was developed as a software tool to support RAMCAP projects. It is generally quite thorough and presents usable reports.

Opinions differ on whether SVA-Pro or RAMCAP Plus is better. RAMCAP Plus seems to require less custom configuration.

- *RiskWatch®*: RiskWatch software (by RiskWatch in Annapolis, Maryland) allows the user to evaluate risks and produces reports and graphs that specifically detail compliance within these regulations, showing where controls are needed. RiskWatch conducts automated risk analysis, physical security reviews, audits, and vulnerability assessments of facilities and personnel. Security threats include crimes against property, crimes against people, equipment or systems failure, terrorism, natural disasters, fire, and bomb threats. Question sets include entry control, perimeters, fire, facilities management, and guards. RiskWatch software appears to comply with the requirements of most DHS risk analysis methodologies.*

These three tools can be used as a benchmark comparison for others.

Lesser Software Tools

Numerous software templates are available, such as the National Fire Protection Association (NFPA) Risk Assessment Checklist. Many of these types of tools provide a simple checklist with the idea of helping the security practitioner evaluate risk. In the case of the checklist mentioned above, the document is a two-page checklist divided into two parts. Part 1 identifies assets or operations at risk, and Part 2 determines facility hazards. Such checklists do little to help security practitioners assess risks (notwithstanding the document's name "Risk Assessment Checklist"). This particular checklist (which is typical of many) completely ignores vulnerabilities and is otherwise only binary in nature (hazard is possible/hazard is not possible, terrorism is possible/or it is not possible, etc.). There is no risk calculation. Anyone using this template would be utterly unprepared to develop a security program of any kind. Such tools are to be avoided.

Affordable Tool Examples

The next few paragraphs reiterate information presented at the beginning of this chapter for clarity:

One of the objectives of this book is to help cash-strapped security managers develop a world-class risk assessment tool that is the equal of multithousand dollar programs. To that end, this book presents a variety of Microsoft Excel templates that I believe conform to all of the DHS-approved methodologies listed in Chapter 2. Taken together, they compose a complete quantitative risk analysis approach to fulfill the requirements of any better risk assessment methodology. Each of these templates breaks down the components of threat, vulnerability, probability, and risk into detail, allowing for a very complete assessment. Coupled with qualitative text developed from the quantitative data of these templates, a comprehensive Risk Analysis Report can be developed at virtually no software cost (assuming the analyst already has access to Microsoft Excel or similar spreadsheet software). Once the templates are originally developed, they can be used again and again, on project after project with equally excellent results.

These templates help the analyst through the various steps to analyze risk quantitatively, culminating in a set of charts displaying risk by facility and area which

* Excerpted from RiskWatch® Web site.

anyone can easily understand. The ultimate charts display the organization's assets arrayed in a prioritized fashion so that anyone can easily see what assets are most at risk and which of those are most critical to the organization. Some tools are useful to help the analyst understand several areas of analysis. For example, the Sandia Adversary Sequence Diagram concept is useful to help the analyst understand vulnerabilities and probabilities and to help select appropriate countermeasures.

These templates will each be explained throughout this book in enough detail so that any person who has basic competence using a spreadsheet program from any major software vendor can build his or her own set of templates that can be adapted for all future risk analysis projects throughout his or her long career. The matrices relating to a risk analysis topic are explained within the chapter describing that topic.

Those readers who are not interested in developing a set of templates as described herein can skip the sections that explain how to build the templates. These are usually contained at the end of each chapter relating to a specific matrix.

Those readers who are interested in developing a set of templates should read these sections carefully and then develop the matrices one at a time until the entire set is developed. These can be developed all in a single workbook with a separate tab at the bottom for each individual matrix so that a given project completes only a single spreadsheet file with all matrices contained within that one file.

This approach is arguably equal to or superior to any of the commercially available software tools and without the need to spend thousands of dollars.

- *Tool Set A: Assets and Consequences Tools*
 - *Asset List:* The first step uses a spreadsheet to create a list of the organizations' assets in an organized fashion, broken out by the four major categories of assets: People, property, proprietary information, and business reputation. These are the categories that most tools will use. This tool is described in Chapter 5, "Asset Characterization and Identification." This will form the basis (Asset Target List) for most of the other matrices.
 - *Criticalities and Consequence Matrix:* This matrix defines the criticalities of each listed asset to the mission of the organization and the resulting consequences of its loss in terms of the following:
 - Loss of Life
 - Loss of Property
 - Loss of Productivity
 - Loss of Proprietary Information
 - Loss of Business Reputation
- *Tool Set B: Probability (Likelihood) Assessment Tools*
 - *Adversary/Means Matrix:* This matrix defines potential threat actors and an estimate of their motivation, capabilities, history, weapons used, and attack scenarios. This information helps the analyst to understand which threat actors to be most concerned about and is essential to establishing a *design basis threat*.*

* The Design Basis Threat (DBT) is that threat against which protective measures are designed to be effective. Threats that exceed the DBT are beyond the capabilities of the countermeasures.

- *Adversary Sequence Diagram:* This diagram is a tool developed by Sandia Laboratories that includes a drawing (or drawings) of the facility and identifies the entry locations and pathways that a threat actor could take to reach target objectives. This helps the risk analyst understand where detection, assessment, and delay countermeasures should be placed.
- *Asset Target Value Matrices:*
 - Historical statistics are of no use in likelihood predictions for terrorism events, because they are too rare, and there are not enough historical data. In the absence of historical data, one can use Asset Target Value Matrix estimates. Asset Target Value Matrices use a set of metrics that help the analyst determine what kind of targets are most likely to be subject to a terrorist event, and for any given facility, where such attacks might take place. Asset Target Value Matrices examine the factors that terrorists might use to select a facility to target and where in the target a successful attack would be most preferable. Asset Target Value matrices can also be of value in estimating likely locations for various types of criminal behavior.
 - *Terrorism Asset Target Value Matrices:* I use two different types of matrices for terrorism. There is no single matrix that is widely accepted by the entire security industry. However, early after the September 11, 2001, attacks in New York City and Washington, D.C., a model appeared from the U.S. Department of Defense that gained wide acceptance, called the CARVER + Shock model. The second model is the KSM Matrix. Each of these evaluates a facility or area of a facility for factors that designated terrorist organizations would use for targeteering (target selection):
 - *CARVER+Shock Matrix:* CARVER is an abbreviation for
 - Criticality
 - Accessibility
 - Recuperability
 - Vulnerability
 - Effect
 - RecognizabilityThe CARVER has long been used by special forces around the globe as a basis for targeting for military purposes. The additional attribute “Shock” was added to adapt the familiar CARVER model to terrorism. CARVER is still widely accepted, though critically flawed. I use it as one of two models because it is widely accepted. It is flawed because there is no evidence that any terrorist organization uses all these factors (or these factors alone) for targeteering and because the categories are too broad to be of use.
 - *KSM Matrix:* This is the second matrix that I use. KSM stands for Khalid Shaikh Mohammed, the presumed mastermind behind the 9/11 attacks and reportedly many others. When one examines the elements of the targets selected by KSM, a pattern emerges which is useful for analyzing potential targets of attacks by major terrorist organizations. The factors include the following:
 - The target fits the strategic objectives of the organization.
 - Mass casualties are possible.
 - The target will attract the media and is on “media-friendly” ground (visually accessible).

- The target is of economic importance by itself, or represents an economically important sector of the economy.
- The target is of cultural importance to the constituent community of the victims and where possible is also culturally important to the terrorist organization's constituent community.
- The target is vulnerable.
- There is a high probability of success of the planned attack scenario.
- A successful attack against this target could result in increased recruiting and fund-raising for the terrorist organization

These factors make it a useful matrix for many major terrorist organizations, not only Al Qaeda, but especially for organizations that have close ties with Al Qaeda. However, the actual matrix factors should be analyzed in the context of the elements of targeting history of each terrorist organization under consideration.

- *Economic Crimes Asset Target Value Matrix:* Economic crimes probabilities can be derived from historical records (crime statistics, CAP Index reports, and so forth; or, if such are not available such as for a new facility, an estimate can be constructed from an Economic Crimes Asset Target Value Matrix). Factors that are useful for the latter include the following:
 - An attack against this target could result in economic gain.
 - There is a high probability of success.
 - There is a high probability of escape.
 - There is a low probability of subsequent capture.
- *Violent Crimes Asset Target Value Matrix:* Similarly, violent crimes probabilities can be derived from historical records or estimated from the following factors:
 - There are available surveillance positions.
 - Access identification is not required.
 - Forcible access is possible.
 - A sneak-path is possible.
 - The target is vulnerable to physical attack.
 - The target is vulnerable to social engineering* access methods.
 - There is a high probability of success.
 - There is a high probability of escape.
- *Subversives Matrix:* Subversives, as it applies to NGOs, include any person or organization that acts in a disruptive manner, contrary to the organization's operating interests. Subversives can be acting with intent against the organization's interests, or without intent, disregarding the organization's interests and in a manner that is counter to those interests. Examples include the first category of subversives which may include activist organizations and individuals; and the second category could include persistently disruptive employees or person who intrudes on the privacy of VIP patrons. Factors for subversives could include the following:

* Wikipedia: "Social engineering is the act of manipulating people into performing actions or divulging confidential information." For security purposes, social engineering can also be used to assist a perpetrator in gaining access to a secure or semisecure facility.

- The target conforms to the strategic objectives of the activist organization or individual.
 - The target is accessible.
 - The target operations are easily disrupted.
 - Time on premises is possible.
 - If apprehended, penalties are bearable.
 - *Petty Crimes Matrix:* Petty crimes include any misdemeanor (less than 1 year in jail, no prison time). Petty crimes may include any chronic or persistent minor criminal activity that could affect the operations or reputation of the organization if left unchecked. Some petty crimes are economic in nature, and some are social expressions. Examples may include the following:
 - Pickpockets and purse snatchers
 - Prostitution-related activities
 - Trespassers
 - Vandals
 - Stalkers
 - Matrix factors could include the following:
 - Discrete criminal activity is possible in the public space
 - Trespassing is possible or the activity will not likely be viewed as trespassing
 - There is an acceptable security risk to the threat actor
 - The activity may not be discovered until later
- *Tool Set C: Vulnerability Assessment Tools*
 - *Asset/Attack Matrix:* This matrix is used to determine what kinds of weapons and threat scenarios could be most effective against which assets. This information is valuable to the risk analyst to help determine which threat scenarios are most appropriate to design against, and where they should be applied.
 - *Surveillance Matrix:* Surveillance is an element of vulnerability and is also essential for conducting any type of criminal or terrorist attack. The Surveillance Matrix identifies which types of surveillance can be effectively conducted regarding which assets.
 - *Circulation Path/Threat Nexus:* The Circulation Path/Threat Nexus identifies where along building circulation paths there are natural crossing points for high-value personnel and potential threat actors. This matrix can be used on larger projects and those with high-value personnel assets.
 - *Circulation Path/Weapons Nexus:* The Circulation Path/Weapons Nexus identifies where along building circulation paths there are natural crossing points for high-value personnel and where various types of weapons could be used. This is valuable to determine not only special areas of risk, but also what types of weapons are likely to be used in these locations. This matrix can be used on larger projects and those with high-value personnel assets.
 - *Adversary Sequence Diagram:* Graphically addresses the entry locations and pathways that an aggressor could take to reach possible targets.
 - *Vulnerability Matrix:* Vulnerability includes accessibility, surveillance, and intrinsic vulnerability. These are mitigated by existing factors that could include natural countermeasures, physical measures, electronic measures, and operational measures.

- **Tool Set D: Risk Analysis Tools**
 - *Unsorted Risk Matrix:* This matrix views the consequence, vulnerability, and the various asset target value results from the various matrices above in worst case for each asset under consideration. The results are ranked by severity but are left unsorted (still sorted by the list of assets). I often create two Unsorted Risk Matrices, one for Terrorism Risks and a separate one for Criminal Risks.
 - *Sorted Risk Matrix:* This matrix is the same matrix as above but is sorted by consequences.
 - *V² Matrices:* These matrices present the risk factors in two dimensions (vulnerability and asset target value [equating to probability]) “V²”; and also overlays the criticality/consequence ranking of the asset, thus providing a three-dimensional picture of the risk for each asset and category of assets. The V² Matrix provides a way to present the final data which is easy for anyone to interpret, regardless of their knowledge or skill regarding risk.

Some of these tools are also useful in developing security program countermeasures. These include the V² Matrices, the Surveillance Matrix, the Vulnerability Matrix, the Adversary Sequence Diagrams, and the Circulation Path/Threat Nexus and Circulation Path/Weapons Nexus. These will be covered in later chapters in more detail.

Additionally, a proper Risk Analysis Report usually also includes *security program recommendations* (including countermeasure selections) and rough-order magnitude budgeting. These will also be covered in later chapters.

SUMMARY

Risk analysis requires seven basic skills:

- Skill #1: Gathering Data
 - Get the Organization’s Mission Statement
 - Understand the Organization’s Programs (Business Units)
 - Assets by Classifications
 - Existing Countermeasures
- Skill #2: Research and Evidence Gathering
 - Interviews
 - Internet Research
 - Records Research
 - Surveys
 - Asset Classifications
 - Historical Data Relating to Security Events
 - Criticalities and Consequences Assessments
 - Telephone Research
 - Bibliography Building
 - Countermeasure Research
- Skill #3: Critical Thinking in the Risk Analysis Process
 - Maintaining Focus on Purpose
 - Identifying Key Questions to Be Answered in the Analysis

- Observing and Understanding the Implications of Different Points of View
- Examining Evidence and Its Implications on the Analysis
- Drawing Inferences from the Evidence
- Concepts Affecting the Evidence
 - What theories, definitions, axioms, laws, and principles or models underlie the issue?
 - What is the reliability of the evidence?
 - What are the effects of personal prejudices on the reliability of inferences?
 - What are the assumptions and what is their effect on risk conclusions?
- Drawing Implications on the Consequences of the Risk
- Skill #4: Quantitative Analysis
- Skill #5: Qualitative Analysis
- Skill #6: Countermeasure Selection
 - Countermeasure Selection
 - Cost-Benefit Analysis
- Skill #7: Report Writing
 - Report Organization
 - Expanding and Explaining Quantitative Data
 - Writing Qualitative Sections
 - Writing the Recommendations
 - Writing the Executive Summary
 - Addendums

Tools

The common tools to perform a qualified Risk Analysis include:

- *Tool Set A:* Asset Identification Tools
 - List of Interviewees and Contacts
 - List of Assets (the resource for all that follows)
 - Criticalities and Consequences Matrix
- *Tool Set B:* Probability Assessment Tools
 - Adversary/Means Matrix (to develop the Design Basis Threat)
 - Adversary Sequence Diagrams
 - Crime Statistics
 - Asset Target Value Matrices for the following:
 - Terrorism
 - Ordinary Crime Tools
 - Economic Crimes and Violent Crimes
 - CAP Index or crime statistics
 - Or asset target value estimates for economic and violent crimes
 - Subversive Acts
 - Petty Crimes
- *Tool Set C:* Vulnerability Assessment Tools
 - Surveillance Matrix
 - Adversary Sequence Diagrams
 - Circulation Path/Threat Nexus Points Matrix

- Circulation Path/Weapons Nexus Points Matrix
- Vulnerability Matrix
- *Tool Set D:* Risk Analysis Tools
 - Unsorted Risk Matrix
 - Sorted Risk Matrix
 - V² Matrices (Top Level and by Areas)

CHAPTER 4

Critical Thinking and the Risk Analysis Process

INTRODUCTION

At the completion of this chapter, you will have a good basic understanding of critical thinking as it applies to risk analysis. This will include why analysis requires critical thinking, the eight elements that make up the thinking process, the goals, principles, and elements of critical thinking, the difference between pseudo-critical thinking and actual critical thinking, why critical thinking should become part of your everyday thinking process, applying critical thinking to risk analysis, and the roots of most problems.

OVERVIEW OF CRITICAL THINKING

Critical thinking is to thinking, like economics is to money management. Critical thinking applies a scientific process to the act of thinking that helps result in far superior conclusions and helps the thinker to support his or her conclusions with rational and defendable arguments. Critical thinking concepts and practice apply a structure of control to the thinking process that helps assure that all relevant data, evidence, points of view, assumptions, biases, and prejudices are considered (particularly those that are “out of the box”) and that the conclusions are well considered and thorough. Critical thinking helps assure that those conclusions are not false or based upon incomplete or inappropriate data, and that possible unintended consequences are considered.

Critical thinking is not based on a fixed set of procedures but is based on concepts and principles.* Its flexibility helps assure that it can be adapted to many different types of situations and will always help achieve the best possible outcome.

Critical thinking helps assure that personal weaknesses, prejudices, or personal agendas are not forwarded as part of the conclusions. Critical thinking can be used in any field where the quality of conclusions is important, particularly where the application of those conclusions may affect how organizations and people work, live, and interact. Critical thinking helps to achieve complex objectives and handle problems with multiple dimensions. Critical thinking also helps people achieve intellectual humility and strategically important results.

* Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools* (Dillon Beach, CA: Foundation for Critical Thinking Press, 2008).

THE IMPORTANCE OF CRITICAL THINKING

Critical thinking is important because it enables one to think about a problem more completely and to consider many factors that may not be intuitively apparent. Furthermore, the conclusion-reaching process is more likely to involve the consideration of factors that would likely be missed otherwise, thus helping to assure that conclusions reached are thoroughly considered.

Critical thinking helps the thinker reach conclusions that:

- Ensure that conclusions are all relevant to the issue under consideration.
- Are true to the purpose of consideration of the issue.
- Help assure that relevant theories, definitions, axioms, laws, principles, or models underlying the issue are considered in their proper context.
- Reduce the likelihood of personal biases, prejudices, self-deception, distortion, misinformation, and so forth, being injected into the conclusion process.
- Assure that all relevant stakeholders' points of views are considered, including their concerns, their goals and objectives, and their intended outcomes. This is true not only for positive stakeholders but also for stakeholders of opposing points of view.
- Consider all relevant evidence and exclude irrelevant evidence, including relevant and irrelevant data and experiences.
- Clarify for the thinker what assumptions are being taken for granted and consider the relevance of those assumptions to the issue at hand.
- Consider the implications and possible consequences of various possible recommended courses of action.
- Help the thinker infer conclusions from the evidence in light of all other considerations listed above.

Normal intuitive human thinking, left to itself, can often lead to self-deception, both for individuals and for societies.* Experience shows that many people (including such critical professions such as intelligence analysts) often reach decisions intuitively before thinking about a problem and then look for evidence to support the conclusions, often discarding any contradictory evidence along the way.†

* Roderick Hindery, *Indoctrination and Self-Deception or Free and Critical Thought?* (Lewiston, NY: Edwin Mellen Press, 2001).

† BNEN, June 8, 2003, by Raymond Whitaker and Paul Lashmar: “The WMD Fiasco: The Intelligence — Wheels fall off the ‘mobile labs.’” “The claims of Tony Blair, George Bush and other senior British and American figures, powerfully made in numerous speeches and several dossiers, including the February presentation to the UN Security Council by Colin Powell, the U.S. Secretary of State, were undermined by a stream of contradictory evidence. This included the leak of a classified document in the United States, the public comments of former intelligence officials, endorsed in private by their still-serving colleagues — and the testimony of Hans Blix, outgoing head of the UN weapons inspectors.”

This natural process of intuition-driven conclusions can be disastrous for individuals and organizations and can wreck budgets and careers. Entire programs have been based upon faulty thinking that in retrospect was obvious to everyone concerned.*

Critical thinking is important wherever the quality of thinking and the programs and expenditures for those programs affect the quality of people's lives. This is certainly true in matters of security, where inconveniences and costs can be high, and mitigation values can be debatable.

Unfortunately, everyone has biases. There is no simple way to overcome people's biases, as most people assume incorrectly that they have no biases or else minimize the consequences of what biases they agree that they may have.[†] Biases have a way of finding themselves injected subtly into our findings and recommendations.[‡]

Critical thinking is also important if:

- You want to assure that you are addressing the real issue and are not being misdirected to a red herring.
- You want to assure that you are examining the issue for the correct purposes and are not addressing an aspect of the issue that is itself a misdirection.[§]

* LawyerBizCoach.com: "Why New Coke Failed: Knowing your Customers is Key." Posted on June 8, 2006, by Krista "New Coke. New Coke came out because in blind taste tests, people preferred Pepsi to Coke. The revelation was startling and Coca-Cola decided that it was time to change their formula to make it sweeter like Pepsi. After months of tweaking the formula, doing blind taste tests, and changing their packaging, New Coke was launched.

It failed miserably. Why? Mainly because Coca Cola did not understand their customers. In blind taste tests, people usually only take a small sip of cola, whereas in real life, they drink full glasses of cola. People prefer sweetness in moderation, so when it came to drinking a can of cola, Coke drinkers preferred Coke's less sweet formula to Pepsi's sweetness.

But, it was not just the new formula that Coke drinkers opposed. The new packaging and marketing alienated them. They did not want something new. They wanted the same old Coca-Cola they knew and loved. New Coke failed because Coca-Cola did not know its customers. When the company returned to its old formula and re-launched Coca-Cola Classic, they did much better."

[†] FreeRepublic.com: March 17, 2004, "Think you're not biased? Prof says you are." Northwestern University Psychologist Professor Galen Bodenhausen tested the responses of 24 white university students who classified themselves sincerely as having no racial prejudice. In the first experiment, students watched a movie of a computer-generated face changing expression from hostility to happiness and back again. Researchers asked the participants to press a button when the facial expression changed. The participants also took tests to determine their explicit and implicit racial attitudes. In the second experiment, 15 computer-generated faces were morphed to contain racially ambiguous facial structures, skin tone, and hair styles. Each face was then manipulated to show either a happy or a hostile expression. This time, as in the first study, "When faces were seen to display relatively hostile expressions, individuals high in implicit prejudice tended to categorize them as African-American," Bodenhausen said.

[‡] Columbia Law Review, Vol. 48, No. 6 (September 1948), pp. 970-972: "Trial Examiner's Bias Evidenced by Findings as Ground for Reversing Administrative Order." "... The examiner's one-sided findings on credibility clearly evidenced bias and vitiated the Board's short form order adopting his report. *Pittsburgh Steamship Co. v. National Labor Relations Board* 167 F.2d 126 (C.C.A. 6th 1948)."

[§] Some Liquified Natural Gas (LNG) community activists have implied that LNG is dangerously explosive. <http://timrileylaw.com/LNG-LiquefiedNaturalGas.htm>: Citing an erroneous CNN report: "According to the CNN report on November 15, 2002, 'The company said the vessel, which had just unloaded a cargo of explosive natural gas in Barcelona, Spain, struck a submerged object.'"

In truth, LNG is not explosive when released into the atmosphere. www.weaverscove.com/knowthefacts.html: "7 — LNG vapors in an open environment cannot explode. To create an explosion, LNG vapors would need to be mixed with air and be in a confined space (i.e., inside a room in a building). [Exactly like normal piped gas — author's insertion.] In the remote event of an LNG spill from the facility or a tanker, there would be no explosion."

- You want to be certain that you are addressing all of the points of view and arguments that will be raised by any opposition.
- You want to acquire and address as much evidence as possible and as objectively as possible, regardless of which direction it may point.
- You want to eliminate any false assumptions and take into consideration any other presuppositions and assumptions.
- You want to deduce correctly what might happen and know what does happen.
- You want to draw correct inferences from the evidence.

ANALYSIS REQUIRES CRITICAL THINKING

One simply cannot analyze any problem without thinking about it carefully. Yet the analysis of some ill-prepared security industry workers who position themselves as security consultants is sadly often lacking in evidence of thought. There is evidence of opinion, of scant observation, of references to past experiences, and conclusions reached that often mostly provide evidence of an agenda that is not fully in the best interests of the client.

Observing, offering opinions, and focusing on only part of the problem are not analysis. Yet this is too often what passes for analysis. I am often asked to review the analysis work of other consultants, contractors, and vendors, in the context of preparing for a project. I am frequently shocked at what passes for risk analysis. In one analysis that reportedly cost the client over \$100,000, there was not a single reference given to support either the data or the conclusions. The report was filled entirely with references to “experience” and “we were told by (anonymous*) persons of authority,” with no validating reference. Upon reading the report, I counted only 22 points of analysis, while that particular case called for thousands.

The report, typical of so many, lacked the following elements of critical thinking:

- Threat assessment was apparently “off the shelf” and did not appear to have been refreshed for this project.
- Focus was primarily on basic vulnerabilities, and those were limited to the obvious, without any evidence of searching for environmentally unique vulnerabilities.
- Risk conclusions were drawn directly from the vulnerabilities, without reference to the type of threat actor.
- The report was written entirely from an authoritarian single point of view.
- There was little reference to research, no reference to interviews, no reference to source of facts (therefore making “facts” suspect), no reference to concepts, and one reference only to an applicable law.
- There was no context for interpretations.
- No options were offered.
- No mitigation effect was offered for countermeasures recommended.
- No budget was provided.
- No evidence was provided of architectural or aesthetic considerations for countermeasures, nor for their effect on the efficiency of daily operations.
- No consideration was made of the effect of recommended countermeasures on the quality of life effects for the customer and employee base.
- The qualifications of the consultant were not identified.

* The author’s insertion.

This was a classic Risk Assessment Report, the type of which I have seen many times. It was a straight line from assumptions to conclusions with no stops in between, supporting a preconceived point of view. Any data cited supported only the point of view offered. There was no evidence of analysis whatsoever, just a statement of “findings” and then straight off to recommendations. This is not analysis. This barely passes for thinking at all. We can do better.

THE EIGHT ELEMENTS THAT MAKE UP THE THINKING PROCESS

There are eight basic elements that make up all thinking processes, whether structured or unstructured, by anyone, anywhere, at any time:

1. We think for a purpose (we are thinking about some idea, thing, or person).
2. We bring to the thought a point of view.
3. We bring certain assumptions to the thought process.
4. We use information at hand to think about it.
5. The information may include facts, experiences, data, and so forth, to give our interpretations context.
6. We use concepts, ideas, and theories to interpret the information and give it meaning in the context of what we are thinking about.
7. We interpret the information and draw inferences, implications, and conclusions.
8. We extend our conclusions to think about what would happen if we were to act on our conclusions.

The process becomes iterative so that we compare our thoughts about our conclusions to the original data and determine if the outcome of our conclusions is beneficial to our point of view and fits our assumptions.

This sounds straightforward enough. But, much thinking is unstructured and undisciplined, often leading to erroneous conclusions, because we are all innately biased by our experiences, distorted by our minimal perspective, partial to our own point of view, uninformed about anything other than what we have been exposed to, and sometimes prejudiced, knowingly or unknowingly.

If we want to think better, we must take thinking apart and understand each of its elements and recognize them as we use them (Figure 4.1). This is the foundation of insight into our own thinking processes and the seed of better thinking.

THE CONCEPTS, GOALS, PRINCIPLES, AND ELEMENTS OF CRITICAL THINKING

Critical Thinking Concepts and Goals

Critical thinking applies intellectual standards to the elements of reasoning in order to develop intellectual traits.

The goals of critical thinking are to:

- Overcome biases in thinking.
- Be thorough and accurate.
- Consider all relevant data.

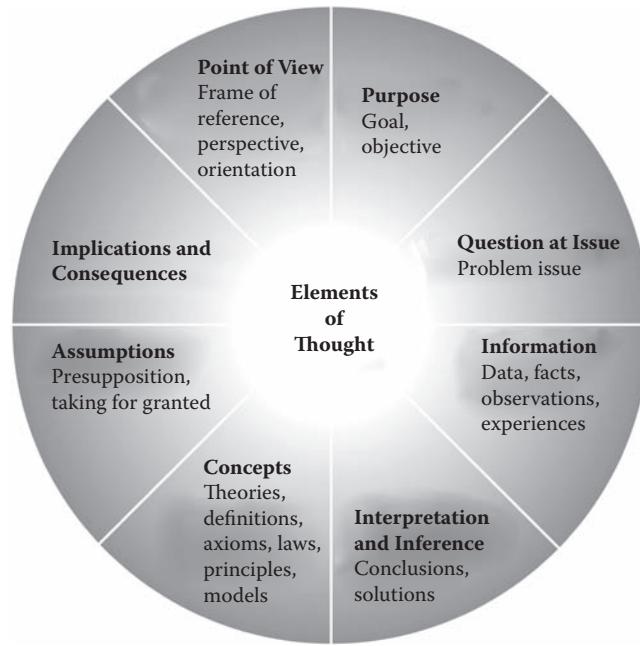


FIGURE 4.1 The Elements of Thought

- Apply a methodology to the thinking process to ensure quality results.
- Develop results that are true to the purpose of the issue.
- Develop conclusions and recommendations that take every relevant issue and point of view into consideration.
- Develop conclusions that are optimal outcomes for the participants.

Principles

Critical thinking principles* include the following:

- **Clarity**: Our thinking and our recommendations should be clear and understandable and easily grasped by the stakeholders. Elaborate as required to explain. Give examples, and illustrate the ideas.
- **Veracity**: Our thinking and recommendations should be free from errors and distortions, factual and true. Our information should be complete enough that stakeholders do not ask: How could we check on that? How could we find out if that is true? And how could we verify or test that?
- **Precision**: Our thinking and recommendations should be precise and provide adequate detail.
- **Relevance**: Our thinking and recommendations should be completely relevant to the issue. We should encourage stakeholder questions, such as: How does that relate to the problem? How does that bear on the question? And how does that help us with this issue?

* Drawn from www.criticalthinking.org/CTModel/CTModel1.cfm#.

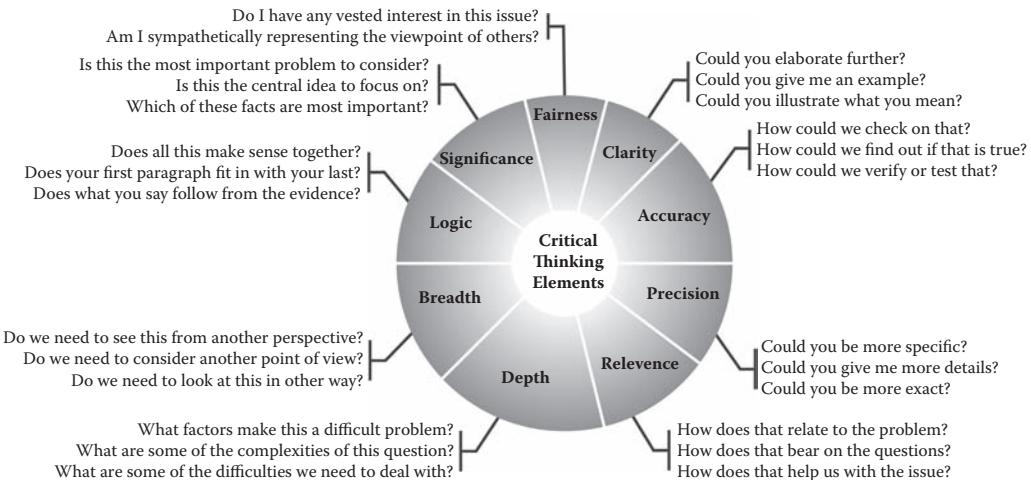


FIGURE 4.2 Critical Thinking Elements

- **Depth:** Our thinking should deal with all of the complexities and multiple inter-relationships. This defines what make up the difficulties of the problem.
- **Breadth:** Our thinking should encompass multiple viewpoints and perspectives.
- **Logic:** Ultimately, our recommendations should bring together the multiple elements of the problem and solution into a logical network that addresses all of the dimensions of the problem and satisfies or deals with the concerned stakeholders. Our conclusions and recommendations should follow from the evidence.
- **Significance:** Our thinking and recommendations should be focused on the important, not on the trivial.
- **Fairness:** Our thinking and recommendations should be justified by fairness, not be self-serving or one-sided. There should be no vested interests served over others, and our recommendations should be sympathetic to the viewpoints of others.

Elements of Critical Thinking

Figure 4.2 presents the elements of critical thinking.*

Purpose

We begin with a purpose for thinking. It is our goal, our objective — it may be what we are trying to accomplish. The term also may include functions, motives, and intentions.

One examines purpose by questioning why, for example:

- What is our purpose for doing...?
- What is the objective of this assignment, task, job, experiment, policy, strategy, and so forth?
- What is our central aim in this line of thought?
- What do we hope to achieve by approaching this line of thought?

* Drawn from www.criticalthinking.org/CTModel/CTModel1.cfm#.

All thinking has a purpose. We should take time to understand and state our purpose clearly and in a way that anyone can understand. Distinguish our primary purpose from any related purposes. Check periodically to see that we are still on target. Choose significant and realistic purposes.

The Question at Issue: Most Thinking Is about Problem Solving

All reasoning is an attempt to figure something out, perhaps to settle an argument or question about something or to solve a problem. We begin by stating the question clearly and precisely.

It is best to express the question in several ways in order to fully understand and clarify its meaning. It is ideal to break the question into its constituent components. By breaking things down, we tend to understand them better. Distinguish questions that have definitive answers from those that are merely opinion or that might have multiple viewpoints. This helps us to focus on the issue more clearly.

The question lays out the problem or issue and guides our thinking. When the question is vague or ambiguous, our thinking will naturally follow with a lack of clarity and distinctness. Questions should be clear and precise enough to guide our thinking.

Questions that can target the issue and help us to focus us on it include the following:

- What are the important questions imbedded in the issue?
- Is there a better way to put the question?
- Is the question clear or complex? And if complex, how can it be stated more clearly, by breaking it down or rephrasing?
- What do we have to know to settle this question?

Understand Our Own and Others' Points of View

Surprisingly to many, their own point of view may not be the only one worth considering. In fact, their own may only be worth considering in the context of others' points of view. That is, if everyone held our point of view, likely everyone's thinking about problems would be quite similar or identical. Thus, there might not even be a problem to consider.

Why look at others' points of view? We do not exist in a vacuum, as individuals alone. We exist in an environment in which virtually everything we want to do requires the participation or cooperation of others. Thus, in order to gain the help and support of others, we must present something of value for them to exchange for that help and support. And, when we are facing opponents, understanding their point of view is critical to being able to either sway their opinion to our point of view or to overcome their position.

Value those points of view as relevant. Others' points of view are relevant to the challenges we face. Our work and personal lives are made up primarily of the interchanges we have with others. Thus, fully understanding and appreciating the value of their points of view are critical to our ability to interact effectively.

In David T. Moore's work on critical thinking for the intelligence community,* he illustrates how President John Fitzgerald Kennedy utilized the critical thinking skill of comparing points of view to deal with the Cuban Missile Crisis of 1962 that brought the world to the brink of nuclear war and how Kennedy effectively avoided nuclear war by utilizing this important principle. Kennedy compared the points of view of Fidel Castro, Nikita Khrushchev, and his own (Kennedy's) points of view on the elements of the conflict.

* National Defense Intelligence College, Occasional paper number 14, "Critical Thinking and Intelligence Analysis," March 2007, p. 20.

By successfully analyzing the elements of points of view and knowing what Khrushchev's capabilities and position were, Kennedy was able to skillfully accommodate the critical political needs of the Russian, Cuban, and American leaders to reach a negotiated and face-saving agreement.

It is possible to conclude that problem solving that does not take into consideration the points of view of other stakeholders only delays and worsens the problem. It is also useful to understand that the failure to understand, appreciate, and take into consideration the points of view of other stakeholders only entrenches the positions of others and makes it increasingly difficult to reach an accommodation later, thus both delaying and worsening the problem.

Gather Assumptions

Assumptions are beliefs that we take for granted. Usually, assumptions operate at the subconscious or unconscious level of thought.

Every thought and problem-solving effort includes assumptions about the environment in which the problem exists. Assumptions include both our own and the assumptions of others (both shared assumptions and opposing assumptions). Many conflicts have occurred in the absence of understanding our or others' assumptions. When the assumption is finally stated, we say "Oh! I didn't know you viewed it this way!" Assumptions are closely related to points of view. In fact, points of view are derived from our assumptions about the facts and our assessment about how things should be. No one ever gets it exactly right. We all color our attitudes about others and our environment by our assumptions about how things should be, rather than simply accepting things for what they are.

The very act of acting out the feeling of anger is an expression of one's discontent over the difference between our view of things as compared to a realization of how things actually are, and a realization that an idea, thing, or person is not within our power to control or change. When one realizes that something to which one is attached cannot be had or controlled in the way one would like, anger and conflict can result.

All reasoning is based upon assumptions. Clearly identify and state your assumptions and try to state why they are justifiable. Consider how our assumptions are shaping our point of view. Consider from what assumptions other stakeholders could be working. Consider how their assumptions could be shaping their points of view. Do this by taking two steps:

1. What do we think is their point of view, and how could these assumptions be shaping that point of view?
2. How could these assumptions shape another point of view that we might not know the stakeholder has? Thus, perhaps we could more fully understand a point of view that the stakeholder has not stated or we did not know that they hold.

Gather Information

All reasoning is based upon data, information, and evidence. It is important to restrict conclusions to those that are supported by data. One should search for information that opposes your position as well as information that supports it. Make sure that all information cited is accurate and relevant and clear to understand. Provide sufficient information to support your findings.

Information may include facts, interview notes, research, evidence, and experiences. Information sources are not necessarily accurate or correct, and it is important to

sort out any information that is found to be incorrect or for which there may be questions of accuracy.

The following are questions that can help guide the process of gathering information:

- What information is needed to answer the questions of the issue?
- What data are relevant to the issue?
- Is more information needed?
- From what sources can we get the information?
- Is the information relevant to our purpose and goals?
- What experiences are relevant?
- What are the sources of the information, data, and evidence?
- What is the certainty of accuracy of the various pieces of information?
- Have we left out any information that is needed?

Examine the Implications and Possible Consequences Related to the Issue

All reasoning leads somewhere or has implications and consequences. Implications are claims or truths that logically follow from other claims or truths. Implications follow from thoughts. Consequences follow from actions.

Trace the implications and consequences that follow from your reasoning. Search for negative as well as positive implications. Ask how these consequences affect the environment, relationships, and so forth. Ask how those changes in the environment affect relations between people and their environment and between people and other people (in order to avoid the law of unintended consequences).

Implications are inherent in our thoughts, whether we recognize them or not. The most successful thinkers think through the logical implication in a situation before acting on it.

Implications can often be seen when we compare one possible action against another. By comparing what might happen if we do this versus that, we can see possible consequences.

Some consequences are more significant than others. It is important to always compare the consequences to the purpose and points of view of stakeholders in order to help assure the success of the outcome.

Implications can also be drawn from facts, sometimes correctly and sometimes with wrong inferences. (“All cats are mortal. Socrates is mortal. Therefore, Socrates is a cat.”) For example, if we ask “What does it mean that prisons are filled more with poor people than the wealthy?” then one could conclude any of the following:

- Poor people are naturally more inclined to criminal activity than wealthy people.
- Poor people do not have access to excellent lawyers.
- Poor people do not have the financial resources to keep them from the edge of financial hardship, thus creating more emergencies in their lives, and thus more possibilities for conflict.
- Poor people do not have the personal relationship resources to fall back on for help in emergencies, thus creating more opportunities for desperate behavior.
- Poor people are poor because of their inability to deal with problems constructively.
- Poor people are uneducated in problem solving.
- It is fruitless to try to help the poor because society cannot overcome such life-long entrenched behaviors.

Thus, it is important to understand that implications are just that — implications, not valid facts — and that those inferences are themselves based upon our own biases, prejudices, and points of view. Thus, iteratively, it is important to consider others' points of view even when considering implications and consequences.

By reviewing implications and extending the implications to their logical consequences, recommendations can be formulated that can optimize outcomes for the stakeholders. We can validate those recommendations using intellectually honest logic and argumentation processes.

Determine What Concepts, Theories, Definitions, Axioms, Laws, Principles, and Models Are Applicable to the Issue

All reasoning is expressed through, and shaped by, concepts and ideas. Concepts are ideas, theories, laws, principles, or hypotheses we use in thinking to make sense of things. In the absence of these, we cannot draw conclusions. This is because these are the benchmark we use to determine if what is happening and what could happen fits our idea of what should happen.

This can be easily illustrated by comparing the thought processes of ordinary citizens of state and terrorist organizations that oppose the leadership of a state. It would be unthinkable for the state to simply destroy the entire country of the state from which terrorists might strike. However, it would not be unthinkable for a terrorist organization to want weapons of mass destruction (nuclear, for example) that could wipe a country entirely off the map. The killing of innocent women and children is unthinkable to a state and changes the feelings of citizens toward their leaders when it occurs.* However the killing of innocent civilians including women, children, and the elderly is considered an effective tool for change by terrorists precisely because of the pressure it puts on governments by their people. As pressure mounts, governments often respond by limiting personal freedoms and conducting investigative and judicial excesses against suspected, though often innocent, civilians, and therefore undermining popular support for the government.

Draw Interpretations and Inferences and Conclusions and Formulate Recommendations

All reasoning contains inferences or interpretations by which we draw conclusions and give meaning to the data. Inferences are interpretations or conclusions we come to. Inferring is what the mind does while trying to figure something out. Inferences should logically flow from the data at hand. We should infer no less or no more than what is implied in the situation. Check inferences for their consistency. Identify any assumptions that are underlying our inferences.

What conclusions are we coming to? Is the inference logical? Are there other conclusions that we could come to that do not fully fit our point of view? What inferences would others come to with another point of view? How did we reach this conclusion? What other alternative conclusions could we reach? Is our reasoning biased? Does this conclusion make perfect sense, or what elements of the problem still remain, and for which stakeholders?

* The American psyche was deeply harmed and offended by the discovery of the behavior of two U.S. Army companies, who massacred 504 innocent civilians, mostly women, children, and the elderly, on March 16, 1968, in the hamlets of My Lai and My Khe of Son My, Vietnam. This event helped turn Americans against the war.

Recommendations should be made after we can map a successful outcome for ourselves and other stakeholders. Or, we can make recommendations that limit the possibility for opposing people to take action against those for whom we serve an interest in the issue.

Pseudo-Critical Thinking*

There is not only good and bad thinking, which are obvious as such, but there is also bad thinking that masquerades as good thinking, causing disastrous results when it is relied upon for important decisions. Often, bad thinking is defended and rationalized in highly sophisticated ways.

Pseudo-critical thinking is a form of intellectual arrogance, masked in self-delusion or deception, in which thinking that is deeply flawed is not only presented as a model of excellence of thought, but is also, at the same time, sophisticated enough to take many people in. No one mistakes a rock to be a counterfeit diamond. It is obviously not a diamond. But a zircon mimics a diamond and is easily taken for one and hence can be said to be a pseudo-diamond. There is much “sophisticated” but deeply flawed thinking that is presented as a model for thought.

Because most people are victims of their own bad thinking, it is very difficult for people to recognize their own thinking as self-serving, incomplete, irrational, or bad. The practice of confusing questions and issues easily diverts people from the relevant to the irrelevant. Many people do virtually no reading. Many cannot speak knowledgeably outside of a narrow field. And many people are not even up to date in their own fields.

Much of what passes as critical thinking is merely the use of logic to address a simple question. There is not much coherent understanding of the role of reasoning and intellectual standards in disciplined thought. The practices of confusing recall with knowledge, confusing subjective preference with reasoned judgment, confusing irrational persuasion over a rational discussion of issues, using vague and ambiguous key terms, and arbitrary scoring result in both invalid and unreliable results.

One of the most common forms of pseudo-critical thinking is the use of logic to address problems rather than a comprehensive process of analysis. Logic is part of analysis and critical thinking; it is not any more a substitute for critical thinking than a wheel is a substitute for a car.

Intellectual Traits[†]

Intellectual traits that make up successful critical thinking include the following:

- Intellectual Humility
- Intellectual Courage
- Intellectual Empathy
- Intellectual Integrity
- Intellectual Perseverance
- Faith in Reason
- Fair-Mindedness

* From The Critical Thinking Community, Foundation for Critical Thinking (www.criticalthinking.org/articles/pseudo-ct-educ-establishment.cfm).

† Foundation for Critical Thinking, “Valuable Intellectual Virtues,” 1996.

The Importance of Integrating Critical Thinking into Everyday Thinking

Critical thinking can be used in virtually every aspect of our lives. Even though most decisions do not have great consequences, we often find that what we assumed to be minor decisions can have major consequences (who we date, what debt we take on, what car we drive when an accident occurs, etc.).

If critical thinking is left to be used only on major decisions, it will likely not be used at all, or when used, the applicant will be ineffective, due to lack of practice. Critical thinking requires practice, like piano playing, math, speaking a foreign language, or any other valuable skill. One cannot learn the principles of critical thinking and be proficient without daily application of the skill any more than one can only read about the vocabulary and grammar of a foreign language and speak proficiently in the language at a conference.

Integrating critical thinking effectively into one's analysis work requires integrating it into one's daily life. This is a two-step process.

- *Step 1:* Grasp the concepts of critical thinking, including its basic ideas, principles, and theories. This is a process of internalization.
- *Step 2:* Begin effectively using the ideas, principles, and theories of critical thinking and make them relevant in the lives of students of critical thinking. This is the process of application. At this stage, one begins to see improvements in reasoning about virtually every subject considered because the person begins to see the world differently, from a standpoint of critical reasoning. The person begins to see fallacies in arguments, weaknesses in the conclusions of colleagues, and so forth. The more the person sees, the more he or she begins to understand and appreciate the value of critical thinking in every aspect of his or her life.

How can one become proficient at critical thinking? I suggest that the person create and place a poster of the concepts of critical thinking prominently in the workplace. Contemplate the elements of critical thinking whenever any decision is at hand.

Even though every decision does not allow time for a fully fledged process of research, evidence gathering, assumption declaration, and consequence consideration, by considering elements of critical thinking in each decision, the person will quickly grasp the principles and also the importance each has to the process of reaching quality conclusions.

To become truly proficient, each week the person should focus on one element of critical thinking and give it constant attention. To wit, for each decision, however small, asking "What assumptions and presuppositions am I working from?" will make you more aware of assumptions.

By asking "What are the other views on this issue?" and "Have I performed adequate research from opposing points of view?" one will become aware of the value of opposing ideas to the decision process, be able to deconstruct invalid arguments from different points of view, and assure that the conclusions put forward will stand up to the scrutiny of opposing points of view.

By asking "What could be the consequences of doing nothing, doing A, B, or C?" one will become more aware of the value of considering alternative actions.

By asking "What can be inferred from this evidence?" and "Does the evidence point to any other conclusions?" one can become more skilled in developing inferences.

Applying Critical Thinking to Risk Analysis

The Risk Analysis Report is the product of analysis. Analysis is the product of thinking. Thinking that is haphazard, unstructured, biased, and incomplete will always result in a Risk Analysis Report that is haphazard, unstructured, biased, and incomplete and which most often has incorrect conclusions that do the client more harm than good by giving the client a perception that risk has been fully analyzed, when that has not happened.

Critical thinking persuades the analyst to maintain focus of purpose, to focus on the issues at hand, and not to be distracted by irrelevant questions having little to do with the issue or purpose. It guides the acquisition of information, data, facts, observations, interview findings, and experiences; it guides the interpretation and inferences of the data; it helps the analyst control the analysis by staying relevant to the concepts, theories, definitions, laws, and principles of the exercise; it helps the analyst to clarify assumptions as such and validate them as true or false and relevant or irrelevant; it helps the analyst draw implications and conclusions; and it helps the analyst to understand, appreciate, and take due consideration of relevant points of view of stakeholders.

In short, it helps ensure complete and accurate analysis. By applying critical thinking processes, the analyst can do the following:

- Better understand and clarify the purpose of the analysis for this specific project.
- Better understand the unique issues of the project.
- Define relevant assumptions that could affect the interpretations of data by different stakeholders.
- Define a full set of relevant risk-related stakeholders, including potential threat actors, and gather their relevant points of view based upon interviews or open source references.
- Gather much more complete information of all types and make sure that the information is completely relevant to the project, including information about potential threat actors, vulnerabilities, asset target value, and so forth.
- Define assumptions and biases that will help to create a more transparent and intellectually honest, unbiased report, complete with interpretations, inferences, implications, and consequences that are unemotional and unbiased by limited points of view.
- Make sure that the analysis is based upon relevant laws, codes, definitions, models, and correct concepts theories and axioms.
- Draw conclusions more accurately, taking into consideration more accurate threat evaluations, budget realities, aesthetic and operational demands, cultural realities, and so forth.

Following the failures of intelligence analysis on weapons of mass destruction in Iraq by intelligence communities around the world, there has been a new emphasis on the application of critical thinking skills in the role of intelligence analysis, especially among those Western governments whose decisions to go to war were based upon the flawed analysis.

More about Critical Thinking

Readers interested in developing critical thinking skills should access: www.criticalthinking.org, which has a wealth of resources.

The Root of Problems*

All problems are the result of an awareness of an impediment to our desired progress toward a goal or are a struggle to avoid suffering. Problems grow from our desire to maintain or grow our position with our environment or with others and the need to overcome obstacles to that growth or maintenance. Conflict evolves out of the ebb and flow of society's natural tendency to move forward from its current position. That move creates change, and change is better for some and worse for others.

This is the most important element to understanding assumptions and points of view. Where change is better, there is acceptance or even gratitude. Where change results in a lessening of someone's position or concept of their position, suffering results. Suffering sometimes evolves itself to conflict as people try to reclaim or expand their position or control what is not easily controllable.

Perception is everything. Where people perceive that their situation is the same or improved, acceptance follows. And where people perceive that their position is harmed or that the effort to effect the change is not worth the resulting benefits, discontent, and conflict can emerge.

All emotional suffering comes from only three things:

1. Attachment to an idea, a thing, or a person
2. Aversion of an idea, a thing, or a person
3. Delusion about an idea, a thing, or a person

From emotional suffering comes conflict. Conflict, especially conflict that does not resolve the underlying issue to the general welfare of all stakeholders, assures the continuation of suffering. We can minimize suffering by accepting what is. Where acceptance is not possible, we can optimize the results using critical-thinking problem solving.

It is also worthwhile to note that the attempt to solve many problems actually masks an attempt to solve one's feelings about the problem. That is, some problems are only problems because we see them as such. They (the problems we see) are not a problem to others because they do not see them as such.[†] Additionally, the existence of a problem in our mind indicates that we are not satisfied about something.

Our overall level of satisfaction can be raised significantly simply by approaching the thing from a standpoint of gratitude rather than from a standpoint of entitlement. The thing that people want to change is fine to those who accept it as it is. For those who are grateful for a thing, its presence brings satisfaction rather than concern.

SUMMARY

Critical thinking applies a scientific process to the act of thinking that helps result in far superior conclusions and helps the thinker to support his or her conclusions with rational and defendable arguments. Critical thinking is not based on a fixed set of procedures but

* By this author.

† “For years, I thought that everyone else in the world was an idiot. Then one day it occurred to me that maybe I was the idiot,” David Letterman.

is based on concepts and principles.* Critical thinking will always help achieve the best possible outcome.

Critical thinking can be used in any field where the quality of conclusions is important, particularly where the application of those conclusions may affect how organizations and people work, live, and interact. Critical thinking helps ensure that personal weaknesses, prejudices, or personal agendas are not forwarded as part of the conclusions. Critical thinking helps to achieve complex objectives and handle problems with multiple dimensions. Critical thinking also helps people achieve intellectual humility and strategically important results.

Critical thinking is important because it enables one to think about a problem more completely and to consider many factors that may not be intuitively apparent.

Nine elements that make up the thinking process include the following:

1. We think for a purpose (we are thinking about some idea, thing, or person).
2. We bring to the thought a point of view.
3. We bring certain assumptions to the thought process.
4. We use information at hand to think about it.
5. The information may include facts, experiences, and data to give our interpretations context.
6. We use concepts, ideas, and theories to interpret the information and give it meaning in the context of what we are thinking about.
7. We interpret the information and draw inferences, implications, and conclusions.
8. We extend our conclusions to think about what would happen if we were to act on our conclusions.
9. The process becomes iterative so that we compare our thoughts about our conclusions to the original data and determine if the outcome of our conclusions is beneficial to our point of view and fits our assumptions.

Critical thinking principles include the following:

- Clarity
- Accuracy or Veracity
- Precision
- Relevance
- Depth
- Breadth
- Logic
- Significance
- Fairness

Critical thinking applies intellectual standards to the elements of reasoning in order to develop intellectual traits. The goals of critical thinking include the following:

- Overcome biases in thinking.
- Be thorough and accurate.

* Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools* (Dillon Beach, CA: Foundation for Critical Thinking Press, 2008).

- Consider all relevant data.
- Apply a methodology to the thinking process to ensure quality results.
- Develop results that are true to the purpose of the issue.
- Develop conclusions and recommendations that take every relevant issue and point of view into consideration.
- Develop conclusions that are optimal outcomes for the participants.

The elements of critical thinking include the following:

- Focus on the Purpose
- Focus on the Issue
- Gathering of Information
- Interpretation and Inference of the Data
- Focus on Concepts, Theories, Definitions, Axioms, Laws, Principles, and Models
- Clarifying and Relating of Assumptions
- Drawing of Implications and Possible Consequences
- Understanding, Appreciating, and Taking into Consideration the Various Points of Views of Relevant Stakeholders

Intellectual traits of critical thinking include:

- Intellectual Humility
- Intellectual Courage
- Intellectual Empathy
- Intellectual Integrity
- Intellectual Perseverance
- Faith in Reason
- Fair-Mindedness

The root of problems include:

All problems are the result of an awareness of an impediment to our desired progress toward a goal or are a struggle to avoid suffering. Problems grow from our desire to maintain or grow our position with our environment or with others and the need to overcome obstacles to that growth or maintenance. Perception is everything. Where people perceive that their situation is the same or improved, acceptance follows. And where people perceive that their position is harmed, discontent and conflict can emerge.

All emotional suffering comes from only three things:

1. Attachment to an idea, thing, or person
2. Aversion of an idea, thing, or person
3. Delusion about an idea, thing, or person

From emotional suffering comes conflict. Conflict, especially conflict that does not resolve the underlying issue to the general welfare of all stakeholders, assures the continuation of suffering. We can minimize suffering by accepting what is. Where it cannot be accepted, we can optimize the results using critical-thinking problem solving.

Some problems are only problems because we see them as such. They (the problems we see) are not a problem to others because they do not see them as such. Our overall level of satisfaction, absent of problems, can be raised significantly simply by approaching the thing from a standpoint of gratitude rather than from a standpoint of entitlement.

CHAPTER 5

Asset Characterization and Identification

INTRODUCTION

In this chapter, you will learn to identify and characterize the organization's assets in the context of critical thinking, which is the basis for all good analysis. This is the basis for criticality and consequence analysis (Chapter 6) and for much of probability analysis (except for threat analysis), all vulnerability analysis, and finally for risk analysis, which is composed of the elements of all three analysis steps above.

THEORY

The first step of risk assessment is to understand the assets at risk, determine their criticality to the mission of the organization, and determine the consequences that could occur if those assets are compromised. Simply put, risk can only exist against assets.

PRACTICE

Asset List

The list of assets you develop will be used in all of the following steps:

- *Asset/Attack Matrix*: Which assets are vulnerable to what types of entry methods, weapons, and attack scenarios.
- *Criticalities and Consequence Matrix*
- *Vulnerabilities Matrix*: Establishing the vulnerabilities of the assets listed.
- *Surveillance Matrix*: Establishing the surveillance opportunities of the assets listed (one component of vulnerability).
- *All of the Asset Target Value Matrices*
 - Terrorism
 - Economic Criminals
 - Violent Criminals

- Subversives
- Petty Criminals
- *Hazards Matrix*
 - Safety Hazards
 - Natural Disaster Hazards
 - Man-Made Hazards
- *Risk Analysis Matrices* (the composite of vulnerabilities and asset target value)

Asset Categorization

The first step in developing all of these matrices is to develop a comprehensive list of assets and to categorize those into their four classes (Figure 5.1). All organizational assets fall into four main categories:

1. People
2. Property
3. Proprietary Information
4. Business Reputation

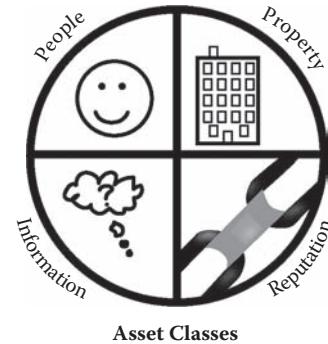


FIGURE 5.1 Asset Classes

People: The people category will include management, employees, contractors, vendors, visitors, and customers. Each type of organization may also have other unique categories worth listing. People are the primary target of terrorism and violent crimes.

Property: The property category will include real property, fixtures, furnishings and equipment, supplies, cash vaults, bank accounts, and so forth. Property is the primary target of economic crimes.

Proprietary Information: Proprietary information includes paper files, computer files, forms, and notes. Proprietary information is also a key target of economic crimes because it provides intelligence needed to conduct a crime or terrorism event.

Business Reputation: Business reputation is self-evident. An organization begins with little, if any, business reputation. What reputation it may have will result from general knowledge or impressions about the principals who started the firm, the marketing campaign, location, type of buildings, and so forth. That is, people get an impression only about what to expect from the organization. As the organization begins to serve its constituency, that impression solidifies or melts as its constituency develops a new impression by actual interaction with the organization, or from hearing stories or news reports about interactions with the organization. Business reputation is a key asset that if lost can destroy an entire organization.*

* www.bloggingstocks.com: Peter Cohan, “Companies that vanished: Arthur Andersen succumbs to the lure of big money,” June 8, 2008. “Arthur Andersen (1913 to 2002) spent decades as a leading accounting and consulting firm. Founded in 1913, it was once a member of the ‘Big 8’ accounting firms, which later became the ‘Big 5.’ Andersen was the accountant for MCI and Worldcom.... The lesson is to resist the lure of big money to pull you away from your values. Enron’s pile of cash was irresistible to Andersen’s leaders. And their lack of moral fiber cost a storied and proud firm its existence.”

For example, one airline may be a standout as news reports on its number one rating are announced and passengers hear from their colleagues about the pleasant experience of using that airline. This may happen even while the industry as a whole is suffering from negative press and word of mouth. However, one airline crash that is related to poor maintenance or management negligence could wipe out all that goodwill and destroy the airline's business. An organization's business reputation is essential to its carrying out its mission in that it creates support in the marketplace for its products or services.

Interviews

I usually begin a risk analysis project with interviews. Interviews are a gold mine of information about the organization's assets, and they help introduce the stakeholders to the purpose and the process and help you gain their willing participation. A typical opening interview is with a key stakeholder, usually the organization's project manager assigned to guide the risk analysis project. Subjects include:

- The organization's mission statement.
- The programs the organization has developed and how those relate to its mission statement.
- The assets the organization has acquired in support of its programs, including:
 - Physical assets
 - Real property
 - Vehicles
 - Fixtures, furnishings, and equipment
 - Information technology equipment
 - People
 - Senior management
 - Management and staff
 - Contractors and vendors
 - Visitors and customers
 - Proprietary information
 - Unique business processes
 - Customer lists
 - Vital records
 - Strategic plans
- The organization's business reputation — Here I ask the interviewee to characterize the organization's business reputation
- The reason this risk analysis is being undertaken.
 - Was there any triggering event that prompted the analysis?
 - Will there be a security program developed or modified resulting from the analysis?
 - Is this an insurance company request?
- What security events have occurred at each property within the last 5 years?
 - Terrorism events or threats
 - Violent crimes
 - Felonies
 - Assaults

- Muggings
- Rapes
- Murders
- Economic crimes
 - Equipment thefts
 - Burglaries
 - Break-ins
 - Robberies
 - Information thefts
 - Vehicle crimes (thefts of or from vehicles)
- Subversive acts
 - Activist organization activities
 - Civil disorder
 - Riots
 - Protests
 - Intimidation
 - Drugs in the workplace
 - Sabotage
 - Corporate spying
- Petty crimes
 - Purse snatching
 - Desk pilfering
 - Pickpocketing
 - Vandalism
 - Prostitution
 - Other petty crimes

Much of this information can come from either the risk analysis project manager or the security director or manager. It is valuable to interview the head of any division or department. Interviews can be either cursory or extensive. They should be in proportion to the scope of the project. I have had projects where interviews took only 2 hours (an office suite in a high-rise building) to 2 weeks (every department of a city government). Keep a list of persons interviewed, including their full name, title, department, and contact information (phone and e-mail). Keep notes — I use either a standard interview form or Microsoft OneNote® (a project organization and note-taking tool).

Facility and Asset Lists

For all of the matrices in this book which will evaluate every aspect of the organization's assets, a full facility and asset list is required. This list should be comprehensive and inclusive. One does not need extreme levels of details, however, due to the excessive number of data analysis points. Redundant data should be avoided. For example, do not include both "equipment" and "office equipment." Generally, the list should include something like the following (example only, indented for clarity):

- People
 - Senior management
 - Management and employees

- Contractors
- Vendors
- Visitors
- Customers
- Property
 - Site
 - Underground parking levels
 - Vehicle entrances
 - Passenger elevator lobbies
 - Tower 1
 - Basement level
 - Loading dock
 - Lobby level
 - Meeting and conference rooms
 - Business center
 - Restaurant level
 - Hotel room levels
 - Premier hotel room levels
 - Passenger elevators
 - Passenger elevator lobbies
 - Freight elevators
 - Freight elevator lobbies
 - Fire stairwells
 - Utility and mechanical areas
 - Tower 2
 - Loading dock
 - Lobby level
 - Anchor tenant offices
 - Free leasehold office levels
 - Passenger elevators
 - Passenger elevator lobbies
 - Freight elevators
 - Freight elevator lobbies
 - Fire stairwells
 - Utility and mechanical areas
 - Retail mall
 - Loading dock
 - Passenger drop-off area
 - Main concourse
 - Events area
 - Back-of-house areas
 - Lo-rise building
 - Lobby area
 - Loading dock
 - Office levels
- Proprietary information
 - Information technology system
 - Electronic security system

- Voice communications systems
- Paper files
- Business reputation

The above is only an example of what types of assets to list. The list should be large enough to be comprehensive but not so large as to duplicate assets of a similar type within a similar area. For organizations with multiple sites, this list can be expanded as required.

Each of the categories of assets (people, property, information, and reputation) above will receive detailed attention as we proceed through the book and into the analysis matrices. Remember, risk analysis can be performed using any quality program, qualitatively in text from detailed notes, or using a detailed matrix as described in this book. I have no agenda to drive one type of analysis over another. All can work equally well in the hands of a good analyst.

As we progress through the book, you will learn how to evaluate each of the organization's assets thoroughly, from many points of view and multidimensionally. The result will be a very thorough analysis. This process can be truncated for very small projects, such as an office suite, but the complete understanding of the analytical process will guide you to a successful conclusion on every project. The use of all of these tools and methods will also assure conformance with any U.S. Department of Homeland Security (DHS)-approved methodology.

If you intend to use the software templates presented in this book as an exemplar of how to perform analysis, those templates will be useful in every project of any size.

Research

Research may include Internet, telephone, and records research. Chapter 3 provides a good foundation for the tools of research.

Surveys

Surveys are most illuminating. In surveys, one finds any and all of the following kinds of information:

- Environmental Context

By environment, I mean everything about the organization as it resides at a specific facility. This includes the physical, security, political, weather, hours of operation, limitations of operation, and nearby factors.

- *Information about the area where the facility resides:* This should include information about the nation, state, city, neighborhood, and street (and water and rail, if applicable). This provides context for the analyst and reader to better understand factors that might not be immediately apparent to unfamiliar readers. For example, if there is only one approach road and the property backs up to a river, this could affect evacuation should it become necessary. Taken with other information, for example, of an up-street neighbor that stores significant amounts of toxic chemicals, this could mean that "shelter in place" rather than evacuation could be the only viable option to a leakage.

- *Political factors:* Political factors are often overlooked but can have a profound effect on an organization's security, especially in countries with fragile internal political relationships and countries that have fragile relationships with their neighbors. For example, any organization in a major city in India or Pakistan is at risk of political events there. A friend of mine was once the U.S. Ambassador to Pakistan when a demonstration erupted into violence. Over a day later, his entire staff emerged from an underground safe room to find that the entire embassy was burned to the ground.
- *Social factors:* Social factors can affect the security of organizations as well. For example in Los Angeles, California, after the Rodney King verdicts, racial tension erupted into riots that destroyed large parts of the city, including many commercial businesses and government offices. Regardless of whether or not there has been any violence in the past, wherever there is any social tension between factions of a city, state, or country, these should be noted, along with indications for contingency for civil disorder planning.
- *Security factors:* These may include police response times and past security events. Any past significant security events should be noted, along with their resolutions. General trends for security in the area, city, and property should be noted.
- *Weather and natural environmental conditions:* These include extremes, averages, rainfall, snow days, potential for natural disasters, and so forth.
- *Hours of operation and occupancy:* The hours of operation and occupancy affect the facility's vulnerability to burglary and nighttime employee abuse. If the facility has different hours of occupancy for different departments, list each.
- *Limitations of operation:* List any development restrictions, hazards, and so forth.
- *Neighboring factors:* Does a neighboring business stock toxic chemicals, what is that business's disaster coordination plan? Is there an embassy of a country that draws large or potentially violent protesters nearby? List any other neighboring factors that could affect safety or security.
- **Property Context**
 - *Information about the property where the facility resides:* Use Google Maps® or another service to plot the location of the facility relative to major environmental features such as rivers, streams, major roads, fire department, and police department.
 - *Road, air, rail, and water ingress/egress:* Evaluate the access routes to the property. List the access routes by category (helipad, water taxi, VIP driveway, loading dock entry, etc.) and any unique attributes vis-à-vis possible vulnerabilities. Review choke-points, sharp turns, and so forth that could pause VIP arrivals and exits, and list what types of vehicles will access the facility along which routes.
 - *Fence-line access:* Where are the pedestrian and vehicle gates along the fence line?
 - *Robustness of natural perimeter defenses:* Note storm walls, water barriers, and so forth.
 - *Robustness of man-made perimeter:* Note the property fence line by path, type and height, quality of maintenance, weaknesses, gate access points, and what lies beyond the gate (road, waterway, pasture, etc.). Also note

overhanging access from bridges and other structures from which a person could jump down into the property.

- *Building types:* List the types of uses and types of construction, including numbers of floors, square feet/meters, and allocation of spaces by departments, functions, and occupancy counts.
- *Access sneak-paths:* List any weak gates, manholes, tunnels, and concealed access points.
- *Access control points and equipment/procedures/hours of operation:* List which building perimeter locations are normally used for access and which are used exclusively for maintenance. Identify the access control procedures for employees, contractors, vendors, and visitors. Identify the hours of operation for each access point and the types of people who may clear through the access point.
- **Organizational Context**
 - The organizational context includes elements of the operation of the organization that impact on the security environment. These include aspects relating to the daily operation of the facility. This is where normal criminal losses occur, as these interactions create the opportunity for crimes against the organization and its staff.
 - *Functional organization chart:* Obtain a functional organization chart. This is a document that shows the hierarchy of management and the departments each manager serves. Also it should show or make reference to a document that identifies the charter or mission of each department and departmental unit. Especially important is the location of the security department or unit in the organization.
 - *Organizational elements:* The organizational elements will detail how each department helps fulfill the overall mission of the organization.
 - *Functions of elements*
 - *Customers:* Who does the organization serve? Who does each department serve? Some departments serve customers outside the organization, and others serve customers who are part of the organization (i.e., other organization departments).
 - *Coordinating entities to deliver the services:* Who do the departments rely on to service their own needs? These outside contractors often have access to sensitive information and physical assets, including organization planning and projections.
 - *Quantity of staff, space allocation:* How is staff allocated by space? How many staff members are in each department?
 - *Access control requirements:* What are the access control needs of each department? What screening is necessary for employees, contractors, vendors, and visitors? Is it possible, for example, to locate all vendor access to a single area to include purchasing and department representatives instead of having vendors visit every department? Is positive access control necessary? That is, does the organization need to control visitors by escort or by issuing them badges that act as access control credentials? Do the visitor access control credentials need to be used to control access both in and out?
 - *Proprietary information protection requirements:* What kinds of proprietary information are kept and used in each department? Is proprietary

information restricted to certain areas, or is there wide access to such information? What is the department's policy regarding visual access to proprietary information while contractors, vendors, and visitors visit the department? What are the policies regarding marking and storage of proprietary information?

- *Hours of operation:* What are the hours of operation for each department? What hours do cleaning, plant maintenance, and other contractors have routine access?
- *Parking:* Is parking space adequate for visitors, staff, management, contractors, and vendors? Is there adequate parking for contractor and delivery trucks? Is there adequate queuing for the loading dock? Do different parking areas operate under different hours of operation?
- *Vehicle access:* How is access to parking and the front entry controlled? Is it possible to limit access proximity to vehicles of different sizes? For example, while much has been made about the need to check the underside of vehicles entering properties, in fact, bombs placed under vehicles are generally very small. They have only ever been used to assassinate the vehicle occupants and have not proven to be a significant threat to others, except for those in the immediate vicinity of the car. Such bombs do not generally pose an overall risk to the facility. It is far more important to limit access by large vehicles, especially trucks, to only areas that are structurally robust.
- *Shipping/receiving — Loading dock:* Ideally, all deliveries for high-risk facilities should take place at a dedicated off-site receiving dock where all deliveries can be properly checked. Then, transit delivery by controlled vehicles bearing seals from the dedicated receiving dock can assure the safety of the facility from unverified vehicles. Failing that, the loading dock should be located well away from the front entrance and away from large expanses of glass façade. Vehicles should be queued, checked, and sealed at some distance from the facility, if possible. It is important to note everything about the physical and operating environment of the shipping/receiving — loading dock area, including risk/theft mitigation strategies. Try to stay around the area long enough to see if these strategies are actually adhered to.
- *Mail/delivery room:* Similar to the shipping/receiving and loading dock, the mail/delivery room handles packages internal to the organization. This is also best handled off-site if possible, but that rarely happens. It is important to locate the mail room in a place that can be easily isolated if hazardous chemicals or biohazards are found in packages. Also, a negative pressurization environment is ideal, drawing air in from the outside and thus containing any biohazard in the mail room. Note the physical and operating environment for the mail room, especially the policies for handling hazardous chemicals and suspicious packages.
- Security Context
 - *Physical security vulnerabilities:* After fully understanding the operating environment, note any physical security vulnerabilities that could be exploited by threat actors in this operating environment. These may include unintended access points; abuse of normal access points by stealth, trickery, or intimidation; and types of assets any threat actor might be interested in.

- *Vetting of contractors, vendors, and visitors:* How are these regular visitors granted access? Are contractor or visitor badges used, or are escorts used for either regular or infrequent visitors? What is the policy regarding regular and infrequent visitors to no-escort areas?
- *Lighting levels:* What are the nighttime lighting levels in parking lots, parking garages, and walkways? During unoccupied hours, are lights left on in any areas to discourage threat actors? Is the landscape near the building lighted sufficiently to display the actions of anyone near the buildings?
- *Security zones:* How is the building divided by security zones (public, semi-public, controlled, and restricted zones)? Are these zones formal or informal? Are they controlled by access control system, security staff, or informal means? Do employees, contractors, and visitors wear access credentials so that their presence by access authorization is clear, or can anyone stray to any area unimpeded?
- *Type of security organization*
 - *Security management:* What is the level of qualifications of the organization's security management? Security management should have the training and experience to conduct its role. This is often not the case, with minimally qualified people placed in this vital role. When I have questioned C-level executives about the qualifications of their vital departments, the executives often talk proudly about the care taken in their selection of the department head and highlight the qualifications of the executive. Then when asking the same question regarding the security chief, the answer is often that the person was promoted to the position from some unrelated function and has received little or no training since, nor has the security staff.
 - *Staff/dogs/contractors:* What is the quantity of security staff, including employees, contractors, and dogs? Is staffing sufficient based upon the number of posts and patrols and staff positions?
 - *Policies and procedures:* Review the organization's security policies and procedures. Note the organization, completeness, and relevance of sections and text to the mission and functional organization of the facilities. Note if the policies and procedures appear to be in constant reference and use or if the security chief has to search to find these. Policies and procedures should make reference to relevant laws, codes, and standards and should be based upon industry best practices where possible and on accepted industry practice at the minimum.
 - *Hours of operation and staffing:* What are the hours of operation and staffing of the security department and unit and its constituent components? What are the hours of operation of security management, customer service office, badging, and hours for post and patrol shifts?
 - *Training of management and staff*
 - Ask about the training for new security staff, and ask about the continuing training program for security management and staff.
 - Security management training should be across all disciplines of security, especially focused on security operations. The organization should have budget for continuing training of its management, especially for courses that offer continuing education units (CEUs).

- All staff training should be based on the policies and procedures. These should be the basis for training, not unrelated. All training should derive from laws, codes, and policies and procedures.
- *Programs*
 - *Posts and patrols:* How many security posts are there? And how many patrols? Are patrols by foot, bike, or vehicle? What are the hours of posts and patrols? Is video utilized to augment patrols? What are guards trained to observe while on patrol? How are notes taken? How do guards communicate the urgent or important findings, and what actions are taken when these are communicated? Are there fixed policies to cover such findings?
 - *Photo ID badging:* Most organizations use security badging to augment their access control program and to help identify users and the areas for which they have access.
 - *Security awareness program:* A security awareness program is vital to spread the security culture in any organization. A good security awareness program should include written and verbal elements. Written elements may include handouts for visitors and employees, a newsletter or e-mailing program including security alerts both unique to the organization and of a general nature, such as warnings about new credit card fraud tactics. These are often highly appreciated by the employees of an organization and help to build the culture of security and enhance the security organization's esteem in the minds of its constituents. Verbal guidance and handouts for visitors and staff help way-finding and help new employees to understand their responsibilities and the security policies of the organization. Review and note the elements and any deficiencies.
 - *Investigations:* Many organizations have need of an internal investigations program to deter internal crime and to detect and prosecute employee, external, and crimes of collusion against the organization. Security management should be trained in investigations and interviewing and should know the laws of both as regards their rights and responsibilities and the rights of those being investigated and those who are peripheral to the investigation.
 - *Law enforcement liaison:* An important and often overlooked element of a good security program is a law enforcement liaison program.
 - *Emergency management program:* Also called a crisis management program, this should include contingency plans for civil disorder, riot, natural disasters of all types, bomb threats and bomb events, shootings, medical emergencies, and more. Review and note the elements and any deficiencies.
 - *Disaster recovery program:* Part of every organization's critical planning includes both a crisis management program and a disaster recovery program. The security unit is essential to both of these. Review and note the elements and any deficiencies.
 - *Intelligence program:* A good intelligence program is an important, if not essential, component of the overall security program for any high-risk facility. The program should include commercial intelligence

news feeds and public agency liaison, such as the Federal Bureau of Investigation's (FBI's) Infragard or U.S. Secret Service liaison program. The organization's security management should receive basic training in intelligence analysis so that they can put the information into the context of their overall risk in order to advise the organization's management on emerging risks and what steps should be taken to counter them.

- *Priority of the security program to upper management*
 - *Budget:* What is the budget of the security organization vis-à-vis the assets they have to protect? Look around the security organization and see how it appears in terms of condition of equipment and organization. These are often cues to the budget or to the efficiency with which the available budget is applied (a cue to the quality of management). Look to see if the security organization is consistent with or substantially below the quality of facilities and equipment of other departments.
 - *Position:* What is the position given to the security chief (director, manager, supervisor, etc.)? Does he or she have a direct-line report to the chief executive officer (CEO) or president? Is the position commensurate with the importance to the facility? I am not advocating that every organization needs direct access to the president or CEO. But where security is a core part of the organization's mission, such as at a financial institution or NGO,* it is essential that it be a direct line of report in order to succeed at its mission.
 - *Organization:* Security will only receive the emphasis it is granted by the management of its department head. For example, if the security unit is placed under the mantle of the facilities management department, it will likely be treated as a commodity, similar to housekeeping and supplies, with the department head striving to cut costs above all other considerations, as is common to facility departments everywhere.
 - *Training and communication:* The manager of the department should be a trained security professional in order to understand the challenges of security and its role in protecting the mission of the organization. For larger organizations and any organization that is a high security risk, the security function should be a department with a direct line reporting to the president or CEO. If not, any message from security management will be filtered by the department head to which it reports. This is assured to dilute, distort, or delete the message that the CEO or president receives and helps assure also that it is not possible for the security chief to counter any thoughtless or uninformed responses by the CEO/president or anyone else in the room at the time the message is rendered. I have seen this happen virtually every time that a department head presented security's message to the CEO or president.

* An NGO is a nongovernmental organization such as the United Nations.

- *Interface between physical and information security programs:* There is often an unfortunate gap between the security program and the information technology security program. This is not helpful to the organization, but as these two functions are often derived from completely different departments, it is natural for such separation to occur. Ideally, both programs should be mutually supporting and should be mutually developed to assure that there is an interface. Wherever possible, I recommend that the security chief have lunch together at least once per week with the information technology security chief so that they can share concerns and develop a close working relationship.

TOOLS

One of the primary benefits of this book is the teaching of a spreadsheet approach to risk analysis. You may use either this approach or commercial software to document your findings and estimates and to perform calculations. But it is useful for understanding the principles of risk analysis to build the databases at least once. Once built, they can be easily modified to fit the needs of any project.

Listing assets is straightforward. Make a comprehensive list of four kinds of assets:

1. People
2. Property
3. Proprietary information
4. Business reputation

For the first three of these categories, list major assets. For example:

- People
 - Senior executives
 - Management
 - Employees
 - Contractors
 - Vendors
 - Visitors
 - Customers
- Property
 - Perimeter
 - Main campus entry/exit
 - Visitor center
 - Service entry
 - East fence
 - North fence
 - Parking structure
 - Basement levels
 - Loading dock
 - Chiller plant

- Office tower
 - Main lobby
 - Employee entrance
 - Elevator lobbies
 - Executive elevator
 - Building management office
 - Floors 2 through 6 corporate headquarter offices
 - Floor 7 finance and real estate
 - Floor 8 personnel
 - Floor 9 executive offices
- Hotel
 - Porte cochere
 - Security checkpoints
 - Main lobby
 - Employee entrance
 - Elevator lobbies
 - Low rise
 - Mid rise
 - High rise
 - Restaurant levels
- Convention center
 - Main lobby
 - Loading docks
 - Administrative offices
 - Convention floor
- Proprietary information
 - Vital records
 - Secret formulas and patents
 - Information technology system
 - Security system
 - Telecommunications system
 - Paper records
- Business reputation has no subsets

The information above is for example only. Information specific to a project will be filled in beginning with Chapter 6. The information created in the asset list will be used to populate most of the other matrices that will be developed, so it pays to be sufficiently detailed.

SUMMARY

Theory

The first step of risk assessment is to understand the assets at risk, determine their criticality to the mission of the organization, and note the consequences that could occur if those assets are compromised.

Practice

The list of assets you develop will be used in all of the following steps:

- *Asset/Attack Matrix*: Which assets are vulnerable to what types of entry methods, weapons, and attack scenarios?
- *Criticalities and Consequence Matrix*
- *Vulnerabilities Matrix*: Establish the vulnerabilities of the assets listed.
- *Surveillance Matrix*: Establish the surveillance opportunities of the assets listed (one component of vulnerability).
- *All of the Asset Target Value Matrices*
 - Terrorism
 - Economic criminals
 - Violent criminals
 - Subversives
 - Petty criminals
- *Hazards Matrix*
 - Safety hazards
 - Natural disaster hazards
 - Man-made hazards
- *Risk Analysis Matrices* (the composite of vulnerabilities and asset target value)

The first step is to develop a comprehensive list of assets and to categorize those into their four classes:

1. People
2. Property
3. Proprietary information
4. Business reputation

It is usual to begin a risk analysis project with interviews. Subjects include the following.

Facility and Asset Lists

Both research and surveys will be needed for the asset list:

- Research may include Internet, telephone, and records research. Chapter 3 provides a good foundation for research tools.
- In surveys, one finds any and all of the following kinds of information:
 - Environmental Context
 - Property Context
 - Organizational Context
 - Security Context

Tools

You may use either this approach or commercial software to document your findings and estimates, or other tools such as the spreadsheets described in this book can be used to perform calculations.

CHAPTER 6

Criticality and Consequence Analysis

INTRODUCTION

At the completion of this chapter, you will understand the difference between criticality and consequences and how to determine both criticality and consequences. You will also understand how consequence analysis is the key to prioritizing security program resources in order to get the best results for the least program expenditure.

Understanding criticality and consequence analysis is the key to applying the limited budget for countermeasures in the most efficient manner. It is imperative that countermeasures be applied to secure the most critical assets first, and then others in descending fashion. Usually this involves a twofold approach, as described below.

TWOFOLD APPROACH

Every project should receive a *baseline security program* and *specific countermeasures to address specific vulnerabilities*, but those programs work best which are designed to assure the best protection for the most critical assets within the context of these two approaches. That is, rather than applying a generic baseline security program, a good analyst will recommend a program that biases the countermeasures to assure the best protection for the most critical assets.

There is much confusion in the security industry between the terms *criticality* and *consequence*. Many security professionals mistakenly use the terms interchangeably. Criticality has to do with the impact that an individual asset has to carrying out the mission of the organization, and consequence identifies the effect that the loss of an asset would have on the organization (see Figure 6.1).

Criticality and consequence ranking can be used as a component of other calculations including asset target value and risk analysis calculations and also countermeasure cost effectiveness.

CRITICALITY

There is only one measure of criticality — the impact that an asset actually has on the carrying out of the mission of the organization. If an asset (person, property, information,

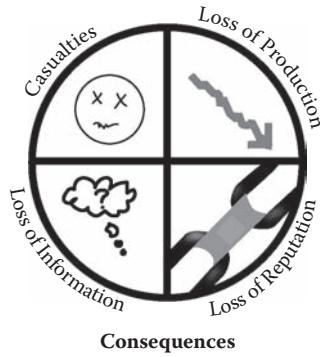


FIGURE 6.1 Consequences

or business reputation) is essential to the mission of the organization, it can be said to be critical.

Basic criticality is the measure or estimate of a business unit or asset's importance to the mission of the organization. Certain assets of an organization are more important than others to the mission of the organization. Criticality may be intrinsic or derivative.

Intrinsic criticality is the extent to which a specific asset is directly important to the mission of the organization, and *derivative criticality* is estimated by the impact that the loss of the asset would have consequentially. For example, the loss of the accounts receivable database might not immediately cause the collapse of the organization; however, the loss of revenues that could occur because the organization cannot prove amounts owed to it, could cause its bankruptcy. So, although the database is not itself a critical component, the consequences make it so.

It is necessary to place a criticality measure on every major asset so that countermeasures can be appropriately derived. Criticality is best estimated not by a security consultant, but by the organization's own senior management.

At a minimum, each major asset should be estimated for the following:

- Absolutely critical to daily operations
- Very critical but operations could continue for up to several days
- Critical but operations could continue at diminished capacity
- Somewhat critical but operations would be seriously impacted
- Not critical but helpful to operations
- Absolutely not critical to the mission

Taking the list of assets developed earlier from the interviews and surveys, the consultant with help from a representative from senior management should address the criticality of each asset as described above. Often a good place to begin is with the organization's disaster recovery plan, for which a criticality analysis will already have been conducted.

Develop a criticality/consequences chart with the assets in rows on the left and the first column labeled "Criticalities." Use the following scale for criticalities:

- 10 Absolutely critical to daily operations
- 7 Very critical but operations could continue for up to several days
- 5 Critical but operations could continue at diminished capacity
- 3 Somewhat critical but operations would be seriously impacted

- 1 Not critical but helpful to operations
- 0 Absolutely not critical to the mission

Place an “X” next to each asset and under the appropriate criticality ranking.

CONSEQUENCE ANALYSIS

For every unwanted event, a range of consequences are possible, and within most of these, there is a range of severity. Possible consequences include the following:

- Mass Casualties
- Loss of Property
- Loss of Production
- Loss of Proprietary Information
- Environmental Impact
- Loss of Business Reputation (confidence in the organization by members of the public)

Similar to the measurement for criticality, the measurement of consequence is best conducted in collaboration with a representative from the organization’s senior management. It is best to consider not what will happen, but what could happen (Murphy’s Law).

Like the criticality analysis, the analyst should prepare a spreadsheet that illustrates a row for every major asset and columns for the possible consequences. Then, after noting a score between 1 and 10 (10 being worst) at every appropriate box, the analyst can determine those assets (targets) with the greatest consequences (Figure 6.2).

Another measure of criticality is the cost to the organization to replace the asset if lost:

- *Absolutely critical* — As the cost to replace would be impossible to bear.
- *Very critical* — Replaceable at a very great cost in dollars or lost production.
- *Critical* — Replaceable at a significant cost in dollars or lost production.
- *Somewhat critical* — The cost would impact other operations or development plans.
- *Not critical* — Easily replaceable.



FIGURE 6.2 Risks Have Consequences

BUILDING YOUR OWN CRITICALITY / CONSEQUENCES MATRIX

For readers who are interested in building their own risk analysis program spreadsheets, continue reading the rest of the chapter. Those readers who wish to use a commercially available software product or who are reading only for interest in the subject of risk analysis may skip the rest of this chapter.

This book will explain each element of risk analysis and countermeasure selection in terms of its theory, practice, and tools. The book will explain in adequate detail how to assemble MS Excel spreadsheets for each element. Those readers who prefer to use a commercial software tool may skip the sections explaining how to build the Excel spreadsheets. For those who are interested in building and using their own world-class risk analysis software tool, the first two tabs on the Excel workbooks are explained in cell-by-cell detail and after that in adequate detail to build the remaining sheets. The first of these is the Consequence Matrix. The Consequence Matrix also includes the basic template on which most other matrices will be built, that is the list of assets/targets.

CRITICALITY / CONSEQUENCE MATRIX INSTRUCTIONS

These instructions should be combined with a close look at the illustrations in this chapter in order to assemble working spreadsheets. It is most useful to place all of the matrices described in this book together into a single Excel workbook. At the bottom of a blank Excel workbook, you will notice that there are several tabs marked Sheet 1, Sheet 2, Sheet 3, and so forth. Right click on the tabs and rename them to match the matrix you are developing as you go through this book. The tab at the far right (Excel 2007) generates new empty worksheets, while on Excel 2003 new worksheets are created by clicking on Insert>Worksheet in the Toolbars at the top of the page.

The instructions that follow will create empty worksheets. You will need to average the values of the columns to form the Score column and rank the rows to fill the Rank column. The row contents given are examples only. You should use the actual assets/targets that are applicable for your facility.

- 1 Open an empty Excel® spreadsheet
- 2 Save as “Consequences”
- 3 Right click on a tab on the bottom of the spreadsheet and select “Rename”
- 4 Rename the tab “Consequences”

- 5 Row 3, Column C. Enter “Project Name”. Bold This. Change the font to 14
- 6 Row 4, Column C. Enter “Consequences Matrix”. Bold This. Change the font to 14
- 7 Row 5, Column C. Enter “Note: Criticality Is for Reference Only”
- 8 Select Column C, Align the text to the right except for the Cells C3, C4, and C5, keep them aligned to the left
- 9 Select Column D, Right Click>Column Width Enter “0.2”
- 10 Row 6, Column C. Enter “Targets”. Bold This
- 11 Row 6, Column E. Enter “Criticality”. Bold This
- 12 Go to Cell E6, Right Click>FormatCells>Alignment>Orientation>Enter 75 Degrees
- 13 Select Column F, Right Click>Column Width Enter “0.2”

- 14 Copy Formatting (use the copy format paintbrush) from E6 through Q6 (this tilts all those cells 75 degrees)
 - 15 Row 6, Column G. Enter “Mass Casualties”
 - 16 Row 6, Column H. Enter “Loss of Property”
 - 17 Row 6, Column I. Enter “Loss of Production”
 - 18 Row 6, Column J. Enter “Loss of Proprietary Information”
 - 19 Row 6, Column K. Enter “Environmental Impact”
 - 20 Row 6, Column L. Enter “Loss of Business Reputation”
 - 21 Select Column M, Right Click>Column Width Enter “0.2”
 - 22 Row 6, Column N. Enter “Score”
 - 23 Select Column O, Right Click>Column Width Enter “0.2”
 - 24 Row 6, Column P. Enter “Rank”
-
- 25 **Row 7, Column C. Enter “People” (Heading for Below). Bold This**
 - 26 Row 9, Column C. Enter “VIP Executives & VIP Visitors”
 - 27 Row 10, Column C. Enter “Employees”
 - 28 Row 11, Column C. Enter “Contractors”
 - 29 Row 12, Column C. Enter “Visitors”
 - 30 Row 13, Column C. Enter “Delivery Personnel”
 - 31 Row 14, Column C. Enter “Transportation Personnel”
 - 32 Row 15, Select Cells C15 through Q15, Right Click>Format Cells>Patterns> choose Gray Color
 - 33 Row 16, Column C. Enter “Property” (Heading for All Property Classes Below). Bold This
 - 34 Select Row 17, Right Click>Row Width Enter 2
 - 35 **Row 18, Column C. Enter “Site” (Heading for Below). Bold & Italic This**
 - 36 Select Row 19, Right Click>Row Width Enter 2
 - 37 Row 20, Column C. Enter “VIP Drop-Off”
 - 38 Row 21, Column C. Enter “Employee Drop-Off”
 - 39 Row 22, Column C. Enter “Visitor Drop-Off — Hotel (South)”
 - 40 Row 23, Column C. Enter “Main South Entry Gatehouse Area”
 - 41 Row 24, Column C. Enter “North Perimeter Fence”
 - 42 Row 25, Column C. Enter “East Perimeter Fence”
 - 43 Row 26, Column C. Enter “South Perimeter Fence”
 - 44 Row 27, Column C. Enter “West Perimeter Fence”
 - 45 Row 28, Column C. Enter “North Perimeter Freight Gate”
 - 46 Row 29, Column C. Enter “East Perimeter Emergency Gate”
 - 47 Row 30, Column C. Enter “West Perimeter Emergency Gate”
 - 48 Row 31, Column C. Enter “Hotel Loading Dock Area”
 - 49 Row 32, Column C. Enter “Hotel East Entrance”
 - 50 Row 33, Column C. Enter “Hotel West Entrance”
 - 51 Row 34, Column C. Enter “Ramp down to Underground Parking”
 - 52 Select Row 35, Right Click>Row Width Enter 2
 - 53 **Row 36, Column C. Enter “Underground Structure” (Heading for Below). Bold & Italic This**
 - 54 Select Row 37, Right Click>Row Width Enter 2
 - 55 Row 38, Column C. Enter “P1 Level Parking”

- 56 Row 39, Column C. Enter “P1 Level Elevator Lobby”
57 Row 40, Column C. Enter “P2 Level Parking”
58 Row 41, Column C. Enter “P2 Level Elevator Lobby”
59 Row 42, Column C. Enter “P3 Level Parking”
60 Row 43, Column C. Enter “P3 Level Elevator Lobby”
61 Row 44, Column C. Enter “P3 Level Utility Rooms”
62 Select Row 45, Right Click>Row Width Enter 2
63 ***Row 46, Column C. Enter “Hotel Tower” (Heading for Below). Bold & Italic This***
64 Select Row 47, Right Click>Row Width Enter 2
65 Row 48, Column C. Enter “Main Lobby Area”
66 Row 49, Column C. Enter “Lobby Level Reception Desk”
67 Row 50, Column C. Enter “Lobby Level Bell Desk and Storage”
68 Row 51, Column C. Enter “Security Checkpoint Outside”
69 Row 52, Column C. Enter “Lobby Level Concierge Area”
70 Row 53, Column C. Enter “Passenger Elevator Lobby”
71 Row 54, Column C. Enter “Stairwells”
72 Row 55, Column C. Enter “Freight Elevator”
73 Row 56, Column C. Enter “Lobby Level Utility Rooms”
74 Row 57, Column C. Enter “Low-Rise Levels”
75 Row 58, Column C. Enter “Mid-Rise Levels”
76 Row 59, Column C. Enter “High-Rise Levels”
77 Row 60, Column C. Enter “Passenger Elevator Lobbies”
78 Row 61, Column C. Enter “Freight Elevator Lobbies”
79 Row 62, Column C. Enter “Utility Rooms”
80 Row 63, Column C. Enter “Mechanical Floor”
81 Row 64, Column C. Enter “Roof”
82 Row 65, Select Cells C65 through Q65, Right Click>Format Cells>Patterns> choose Gray Color
83 **Row 66, Column C. Enter “Proprietary Information”. Bold This**
84 Select Row 67, Right Click>Row Width Enter 2
85 Row 68, Column C. Enter “IT System”
86 Row 69, Column C. Enter “Security System”
87 Row 70, Column C. Enter “RF Communications System”
88 Row 71, Column C. Enter “Paper Files”
89 Row 72, Select Cells C72 through Q72, Right Click>Format Cells>Patterns> choose Gray Color
90 Row 73, Column C. Enter “Business Reputation”
91 **Row 77, Column C. Enter “Legend”. Bold This**
92 Row 78, Column C, Enter “Major Effect”
93 Row 79, Column C, Enter “Medium Effect”
94 Row 80, Column C, Enter “Minimal Effect”
95 Row 78, Column E, Enter “10”. Go to Formats>Conditional Formatting
96 Under Condition 1, choose Cell Value Is between 0 and 3.25
97 Under Condition 1, click on Format Tab then on the Patterns Tab and choose the Color to be Green

- 98 Still in the Conditional Formatting Window, click on the Add> Tab
99 Under Condition 2, choose Cell Value Is between 3.25001 and 6.55
100 Under Condition 2, click on the Format Tab then on the Patterns Tab and choose the Color to be Yellow
101 Still in the Conditional Formatting Window, click on the Add> Tab
102 Under Condition 3, choose Cell Value Is between 6.55001 and 10
103 Under Condition 3, click on the Format Tab then on the Patterns Tab and choose the Color to be Red. Click on “OK”
104 Row 78 Column E, should turn to Red Filled instantaneously
105 Copy Formatting (use the copy format paintbrush) from E78 through E80 (this copy the Conditional Formatting to the cells)
106 Row 79, Column E, Enter “5”. The Cell should turn to Yellow Filled instantaneously
107 Row 80, Column E, Enter “1”. The Cell should turn to Green Filled instantaneously

108 Copy Formatting (use the copy format paintbrush) from E78 to Cell E7 through Cell N7 (this fills the cells with the Green Color).
109 Repeat Step 108 above for Cells E9 down to Cell N14
110 Repeat Step 108 above for Cells E16 through N16
111 Repeat Step 108 above for Cells E18 through N18
112 Repeat Step 108 above for Cells E20 down to Cell N34
113 Repeat Step 108 above for Cells E36 down to Cell N36
114 Repeat Step 108 above for Cells E38 down to Cell N44
115 Repeat Step 108 above for Cells E46 through N46
116 Repeat Step 108 above for Cells E48 down to Cell N64
117 Repeat Step 108 above for Cells E66 through N66
118 Repeat Step 108 above for Cells E68 down to Cell N71
119 Repeat Step 108 above for Cells E73 through Cell N73

120 Row 7, Column E, Enter “=AVERAGE(E9:E14)” (this is the formula to calculate the average of the cells E9 through E14)
121 Copy Cell E7, Select Cells G7 through L7 and paste the formula (this will copy the formula to the selected cells). Do not panic if you get “#DIV/0!” this is because your Matrix is still not filled
122 Repeat Step 121 above for Cell N7 (this will calculate the average of the cells N9 through N14)
123 Row 9, Column N, Enter “=AVERAGE(G9:L9)” (this will calculate the average of the Cells G9 through L9)
124 Copy Cell N9, Select Cells N10 through N14 and paste the formula
125 Row 16, Column E, Enter “=AVERAGE(E18,E36,E46)” (this will give the average of the three selected Headings)
126 Copy Cell E16, Select Cells G16 through L16 and paste the formula
127 Repeat Step 126 above for Cell N16
128 Row 18, Column E, Enter “=AVERAGE(E20:E34)”
129 Copy E18, Select Cells G18 through L18 and paste the formula
130 Repeat Step 129 above for Cell N18
131 Row 20, Column N, Enter “=AVERAGE(G20:L20)” (this will calculate the average of the Cells G20 through L20)

- 132 Copy Cell N20, Select Cells N21 through N34 and paste the formula
- 133 Row 36, Column E, Enter “=AVERAGE(E38:E44)”
- 134 Copy E36, Select Cells G36 through L36 and paste the formula
- 135 Repeat Step 134 above for Cell N36
- 136 Row 38, Column N, Enter “=AVERAGE(G38:L38)” (this will calculate the average of the Cells G38 through L38)
- 137 Copy Cell N38, Select Cells N39 through N44 and paste the formula
- 138 Row 46, Column E, Enter “=AVERAGE(E48:E64)”
- 139 Copy E46, Select Cells G46 through L46 and paste the formula
- 140 Repeat Step 139 above for Cell N46
- 141 Row 48, Column N, Enter “=AVERAGE(G48:L48)” (this will calculate the average of the Cells G48 through L48)
- 142 Copy Cell N48, Select Cells N49 through N64 and paste the formula
- 143 Row 66, Column E, Enter “=AVERAGE(E68:E71)”
- 144 Copy E66, Select Cells G66 through L66 and paste the formula
- 145 Repeat Step 144 above for Cell N66
- 146 Row 68, Column N, Enter “=AVERAGE(G68:L68)” (this will calculate the average of the Cells G68 through L68)
- 147 Copy Cell N68, Select Cells N69 through N68 and paste the formula
- 148 Row 73, Column N, Enter “=AVERAGE(G73:L73)”

Following this, populate the cells with appropriate estimates on a scale of 1 to 10. Then average the Score column and rank the results in the Rank column. I suggest using averaging of rows to create the score because it provides a relative view of the issues at hand for each row of each spreadsheet. As you build your own spreadsheets and begin to work with them, you may find that you prefer another formula for determining the score, but I have found that averaging is simple and results in consistently meaningful display of the relationships of the various rows. The spreadsheet can also be made much more useful if you apply conditional formatting to the data and score cells so that high scores color red, low scores color green, and medium cells color yellow. Conditional formatting is applied differently between various versions of Excel, so it is best to use the Help file or look up “Conditional Formatting Excel 2003” in Google. (Substitute your version of Excel if different.)

Refer back to these instructions as you prepare the data for other spreadsheets, as these instructions apply to all matrices throughout the book.

SUMMARY

Criticality and consequence analysis are key to applying the limited budget for countermeasures in the most efficient manner. It is most useful to sort the final risk calculations by ratings of consequence in order to ensure that countermeasure budgets are applied to the vulnerabilities having the greatest consequences.

It is imperative to understand consequences in order to develop effective security countermeasures; and criticalities are an essential element of consequences.

Criticality is the impact that an individual asset has to carrying out the mission of the organization; consequence identifies the effect that the loss of an asset would have on the organization.

Criticality and consequence ranking can be used as a component of other calculations including asset target value and risk analysis calculations and also countermeasure cost effectiveness.

Every project should receive both a “Baseline Security Program” and “Specific Countermeasures to Address Specific Vulnerabilities.” The second category may include programs to address terrorism such as a countersurveillance and intelligence programs, or may address other problems that are unique to the facility’s industry or location.

Criticality

Basic criticality is the measure or estimate of a business unit or asset’s importance to the mission of the organization. Certain of the organization’s assets are more important than others to the mission of the organization. Criticality may be intrinsic or derivative. Intrinsic criticality is the extent to which a specific asset is directly important to the mission of the organization; derivative criticality is estimated by the impact that the loss of the asset would have consequentially.

Consequence Analysis

For every unwanted event a range of consequences are possible, and within most of these, there is a range of severity. Possible consequences include the following:

- Death
- Injury
- Economic Loss to the Organization
- Economic Loss to the Organization’s Constituents
- Environmental Impact
- Loss of Production or Operations
- Loss of Business Reputation (confidence in the organization by members of the public)
- Loss of Assets

CHAPTER 7

Threat Analysis

INTRODUCTION

Threats are at the core of probability. So, threat analysis is at the core of probability analysis. Probability is the composite of a threat actor with intent, and of capabilities acting upon a vulnerable asset.

The process of probability analysis is the process of first defining capable threat actors and then estimating their possible intent to harm or attack the assets of the organization being analyzed. Probability analysis is discussed in Chapter 9, “Estimating Probability.”

At the end of this chapter, you will have a good working understanding of threat analysis, including the difference between threats and hazards, sources for information about hazards, types of threat actors, sources for threat analysis information, and tools to use in threat analysis.

THEORY

Threats versus Hazards

Many security professionals and their clients confuse threats and hazards. Hazards can be either natural or man-made and are generally unintentional or without malice. Threats are always man-made and intentional and with malice. This chapter begins with a discussion on hazards which is followed by a comprehensive presentation on threats (Figure 7.1).

- *Hazards:* A hazard is a precondition for an accident or a natural event having negative consequences. Hazards may include the following:
 - Safety hazards
 - Security hazards
 - Natural disaster hazards
 - Local or regional political or military hazardsHazards may be environmental or behavioral. Both can establish the preconditions for an unwanted consequence.
- *Safety hazards:* Examples of safety hazards could include an unexpected road obstruction to your neighbor who never looks before backing his car into the street. Safety hazards may include:



FIGURE 7.1 Threats versus Hazards

- Fires due to safety hazards
- Fires due to negligence
- Human errors
- Poor design
- Safety violations (blocked exits, etc.)
- Faulty or poorly maintained buildings, vehicles, and technology
- Institutional failure (a culture of disregard for safety)
- High societal tolerance to safety hazards
- *Security hazards:* Examples of security hazards include:
 - *Persistent rule violators* (e.g., employees who routinely leave perimeter doors open for their convenience for smoking breaks and important documents left lying on desks for any unauthorized person to see)
 - *Environmental factors*
 - For example, if the organization's facilities are located in an area with a high incidence of crime, this is a security hazard.
 - High business culture tolerance for security hazards (institutional failure)
- *Natural hazards:* Natural hazards may include acts of God, such as tornadoes and floods, and other incidents quantifiable in terms of statistical probability, such as mean time between failure (MTBF) of equipment. Natural hazards may include:
 - Earthquakes
 - Hurricanes and tropical storms
 - Tornadoes
 - Hailstorms
 - Thunderstorms and lightning
 - Snow and ice
 - Floods including tsunamis
 - Landslides and mudslides
 - Fires from natural causes
 - Fog
 - Hail

- Heat
- Wind
- Safety hazards
- *Accidents:* An accident is an incident or event frequently involving humans, with negative consequences, caused by the presence of a hazard and a triggering event. Accidents can be prevented in one of two ways:
 1. Eliminate or mitigate the hazard so that the accident cannot occur.
 2. Modify the behavior of the person, machine, or thing initiating the triggering event so that the accident will not occur.
- Either can prevent accidents, but risk professionals should try to do both. In order to modify the preconditions so that the accident cannot occur, one must appreciate that there could be preconditions and identify what they are. Critical thinking in security and safety matters can greatly improve the chances of spotting accident preconditions.
For example, where I do much of my work in the Middle East and in a certain Arabian Gulf state, traffic safety is virtually nonexistent. Despite the fact that people understand that in a collision any unattached objects within the car could propel through the windshield or out an open window, nonetheless in several countries I see almost all small children riding without seat belts, often bouncing and playing in the back seat and sometimes hanging well out of the window. (I have even seen small children reaching out to touch other cars as they go by.) This sets up the preconditions for the loss of the life of the child. All it takes then is a triggering event of someone's bad driving (of which there is plenty).
- *Political and economic risks:* In certain areas, political and economic instability can also affect security conditions. These should also be considered.

Descriptive statistics can provide historical data for frequency of past occurrences and suggest expected levels of future occurrence, but specific accidents cannot be predicted using inferential statistical techniques. Examples include traffic accidents on a bridge, and falls down stairs at facilities. Accidents, by definition, are not malicious acts.

The security analyst should cite data for his or her findings and conclusions. Likelihood and consequence information can be obtained from any of the following sources:

- U.S. Coast Guard
 - National Response Center
 - Marine Accident Database
- Federal Railroad Administration, Railroad Accident Database
- Pipeline and Hazardous Materials Safety Administration
 - Pipeline Accident Database
 - Hazardous Materials Incident Database
- Federal Motor Carrier Safety Administration, Truck Accident Data
- U.S. Bureau of the Census, Demographic Data
- Environmental Protection Agency
 - Hazardous Waste Facility Database
 - National Emission Inventory
 - Toxic Release Inventory
 - Safe Drinking Water Information System
 - Superfund Information System
 - Enforcement and Compliance Database

- National Oceanic and Atmospheric Administration (NOAA)
 - Storm Events Database
 - Drought Information Center
 - Tsunami Database
- U.S. Bureau of Transportation Statistics
 - Political Boundaries
 - Urban Areas
 - Transportation Networks
- U.S. Geological Survey
 - Spatial Hazard Events and Losses Database
 - National Hydrography Dataset
 - Landslide Incidence and Susceptibility Data
 - Earthquake Hazard and Incident Data
 - Volcano Incident Data
 - Tornado Data
- U.S. Fire Administration, Fire Incident Data
- Federal Emergency Management Agency, Flood Data
- Federal Bureau of Investigation, Crime Database
- Local Law Enforcement Data and Statistics
- Cap Index, Inc., Local and Regional Security Historical Data
- A list of current active terrorism threat actors for any region can be obtained from
 - U.S. State Department — Threats to the United States
 - British Foreign and Commonwealth Office (FCO) Home
 - Stratfor — Strategic Forecasts
 - South Asia Terrorism Portal
 - The NEFA Foundation
- *Economic Risks*
 - The Economist Research Database (www.economist.com>ResearchTools>CountryBriefings)
 - U.S. Department of State www.state.gov/mis/list/index.htm
- *Political Risk*
 - The Economist Research Database (www.economist.com>ResearchTools>CountryBriefings)
 - U.S. Department of State (www.state.gov/mis/list/index.htm)

All Hazards Risk Analysis

I recommend an *all hazards risk analysis* approach for major projects which takes all of these factors into consideration.

Since September 11, 2001, there has been a hard shift in risk analysis to a focus on threats of terrorism. This book deals with terroristic threats more completely than most risk analysis books. However, much of this shift to focus on terrorism has come at the expense of the historical focus on security and hazards. This is most unfortunate, because security and hazard risks far outweigh terrorism risks for most facilities.

Although my primary field of focus is projects that have significant risks of terrorism (some of my projects have active threats against specific individuals or facilities), I believe that a risk analyst does his or her client a terrible disservice by focusing primarily (and in

some cases I have seen, only) on terrorism. The client has not been serviced if he or she is spending large amounts of monies to deter or mitigate possible terrorist attacks while ignoring much more likely risks.

Additionally, at the time of writing this book, it is in vogue with many risk analysts to emphasize terrorism risks on virtually every type of facility. Terrorism is certainly a valid risk, but it is not a valid risk for a nontoxic landfill (for which I have seen a risk assessment that dealt only with the threats of terrorism). Not every facility is at risk of terrorism. The risk analyst should focus on appropriate risks and not emphasize terrorism on every project.

A good risk analysis report should present all potential threats and hazards and rank and prioritize them, then focus on those that are most relevant. This should typically include natural hazards, man-made security hazards, and intentional acts related to ordinary decent crime (ODC).*

All security risk management has a common objective: to reduce the possibility or likelihood of undesirable events and their consequences, to protect human life and health, and to improve the quality of life in the environment. I believe that for major projects, a comprehensive listing of hazards and threats is useful and helps the client to not only focus on the most relevant, but to understand the other risks and appreciate the priority placed on the most relevant risks.

Now, on to threats.

- **Threats:** Threats are all man-made. A threat is a group that or an individual who has both the capability of and the intent to cause harm. A threat actor is an individual who or a group that intends to harm people or conduct an attack against a facility or organization or against exemplars of an opposing point of view.

Without a threat actor, there is no risk. Analysts must identify potential threat actors and then decide (with ownership) which level of threat actor the security program should attempt to deter and which it should attempt to protect against. The first step is to understand who could be potential threat actors.

- **Potential Threat Actors:** There are five kinds of potential threat actors. These include the following:
 - Terrorists
 - Economic criminals
 - Nonterrorist violent criminals
 - Subversives
 - Petty criminals
- **Terrorists:** There are five types of terrorists:
 - *Class I Terrorist:* The government-trained professional (including foreign intelligence threats)
 - *Class II Terrorist:* The religious extremist professional
 - *Class III Terrorist:* The radical revolutionary or quasi-religious extremist
 - *Class IV Terrorist:* Guerrilla/mercenary soldiers
 - *Class V Terrorist:* Amateur (civilian, untrained criminal, or militia-vigilante groups)

* John Mortimer, "To catch a thief," *The New York Times* (on the Web), August 24, 1997: "What the British Police used to call O.D.C. (Ordinary Decent Crime) has suffered a sad decline in this era of predominantly indecent and extraordinary offenses...."

- *Economic Criminals*
 - Transnational criminal organizations
 - Organized crime
 - Sophisticated economic criminals
 - Unsophisticated economic criminals
 - Street criminals (gangs)
- *Nonterrorist Violent Criminals*
 - Workplace violence threat actors
 - Angry visitors
 - Sexual criminals
 - Mugging/parking lot violence
 - Civil disorder event violence
 - Deranged persons
- *Subversives*
 - Cause-oriented subversives
 - Political and industrial spies
 - Saboteurs
 - Cults/dedicated activist groups
 - Hackers
 - Invasion of privacy threat actors
 - Persistent rule violators
- *Petty Criminals*
 - Vandals
 - Pickpockets
 - Prostitutes, pimps, and panderers
 - Disturbance causes
- *Threat Actors Detailed Description* — There are five classes of terrorists* as described below:
 - *Class I Terrorist* — The government-trained professional (including foreign intelligence threats):

Government-trained professionals are generally very well trained and equipped and often have substantial support systems that are well integrated into the country where they are working due to support from the intelligence community of the government which supports them. These terrorists are trained to carry out missions with great secrecy, and the high level of training and careful selection of candidates helps assure that few mistakes are made.

Class I terrorists are normally recruited from key party personnel, loyal military member, secret police, and intelligence communities. Such terrorists may be working with official (consular, etc.) or nonofficial cover, including posing as businessmen, students, merchants, immigrants, or opposition group volunteers.

A good example of government-trained professional terrorists was the targeted assassinations of Palestinian Black September terrorists by Israeli Mossad agents following the killings of 11 Israeli athletes at the 1972 Munich Olympic games.

In September of 1972, terrorists from the Black September movement, which was a cover for the Palestinian al-Fatah organization, carried out

* Malcolm Nance, *Terrorist Recognition Handbook*, 2nd ed. (Boca Raton, FL: CRC Press, 2008).

an attack against the Israeli athletes' compound, killing 11 Israeli athletes. Following the massacre, Israel carried out a methodical campaign to assassinate leaders of the Black September guerrilla group of the Palestine Liberation Organization. Israeli Prime Minister Golda Meir authorized the effort and approved each assassination.*

Attacks by Class I terrorists are typically targeted against the leadership or policies of another country and are sometimes designed to be spectacular, as was the Munich athlete compound attack.

- *Class II Terrorist* — The religious extremist professional:

Class II terrorists are religious extremists who swear allegiance to an extremist religious cause. These are civilians who live as terrorists with no other duty or career but terrorism. Operatives train and receive advanced combat skills and training, more pay, benefits for their families, and advanced ideological training.

Special characteristics of Class II terrorists are that they are professionally trained, are experienced, may be martyrdom/suicide candidates, are secretive, learn from their mistakes, and learn from the successes of their opposition.

The best-known Class II terrorism group is Al Qaeda. These groups stage both small and spectacular attacks — the most spectacular being the attacks of September 11, 2001.

- *Class III Terrorist* — The radical revolutionary or quasi-religious extremist:

Radical revolutionary terrorists fit the traditional model of the European and Latin radical revolutionary terrorist of the 1960s and 1970s. In America, the Symbianese Liberation Army (SLA), which kidnapped newspaper heiress Patricia Hearst in 1974, is characteristic of a small Class III terrorist organization.†

Other examples of Class III radical revolutionary terrorist organizations include the Spanish Basque separatist group, ETA‡, the former Irish Republican Army (IRA),§ and the Tamil Tigers of Sri Lanka.¶

Class III terrorists are generally small to medium-sized groups, though some, such as ETA, can be extensive and well organized. Operatives are usually trained inside the group. Many active groups are radical nationalists. Attacks are usually small and of low intensity, typically injuring and killing only a few civilians, though some attacks have been spectacular, such as the IRA attack on July 21, 1972, "Bloody Friday," when 20 bombs detonated in Belfast within an hour, killing nine people and wounding 30.**

- *Class IV Terrorist* — Guerrilla/mercenary soldiers:

Class IV terrorists are generally the most predictable of terrorists because they fall back on basic military training and equipment used in military or paramilitary experience.

* David Hoffman, "Israeli confirms assassinations of Munich massacre plotters; Meir aide's comments in TV interview were censored for a year," *The Washington Post*, November 24, 1993.

† Brian M. Jenkins, "Terrorism and Kidnapping," paper P-5255 (Rand Corporation, June 1974), 1.

‡ *The Economist*, "Talking peace; Spain and ETA," July 8, 2006.

§ *Christian Science Monitor*, "Calls grow to disband the Irish Republican Army," March 17, 2005.

¶ *The Economist*, "The Tiger comes out of his lair; Sri Lanka. (The Tamil Tigers are talking about peace)," April 13, 2002.

** Associated Press, "Death toll, targets, worst attacks from 35-year campaign of Provisional IRA," July 28, 2005.

Class IV terrorists are generally ex-military men who have little education and have been recruited by a military or militia to help carry out their operations.

- *Class V Terrorist* — Amateur (civilian, untrained criminal, or militia-vigilante groups):

These groups have large numbers of people, but they have rudimentary terrorist experience. Some form or join militia groups and can become quite organized.

The Ku Klux Klan in the United States is an example of a class V terrorist organization,* and individuals such as Timothy McVeigh, Theodore Kaczynski, and Eric Robert Rudolph† are examples of individual (“Lone Wolf”) class V terrorists. Timothy McVeigh carried out the bombing against the federal building in Oklahoma City‡; Theodore (“Ted”) Kaczynski was known as the “Unabomber”§; and Eric Robert Rudolph,¶ who bombed Olympic Park during the Olympic games.

Although class V terrorists are the least organized and typically least educated and least well equipped, they are nonetheless a threat that can cause major problems to their targets.

- *Antiterrorism Reference Guides and Resources*

- Malcolm W. Nance’s foundational book, *Terrorist Recognition Handbook*,¹ is the most important book that any security consultant can have if he or she wants to understand terrorism threats. It is essential for the library of all analysts who may write any risk analysis involving terrorism threat actors.
- The International Association for Counterterrorism and Security Professionals (www.antiterrorism.org)
- Force Protection Exhibition and Demonstration (FPED)

- *Economic Criminals*

- *Transnational criminal organizations*^{**}: Transnational criminal organizations are organized crime syndicates that operate across state and national boundaries. The best example of these includes computer crime, the Mafia, and drug and weapons cartels.

Transnational criminal organizations are noted for their organization, their reach, and their breadth and depth as well as their focus on their core business. Transnational criminal enterprises are sometimes violent, as in the case of drug cartels, but usually prefer to maintain a low profile so as not to draw too much attention from law enforcement.

Transnational criminal organizations can threaten an organization or subvert its purpose and may extort or intimidate an organization into serving the purposes of the criminal enterprise.

* *The Pantagraph* (Bloomington, IL), “History of KKK gives warning for today,” April 23, 2006.

† *Telegraph-Herald* (Dubuque, IA), “Worries linger about homegrown ‘lone wolves’”; The arrest of Eric Rudolph rekindles some concerns,” June 4, 2003.

‡ *The Independent* (London), “US executes its Public Enemy No. 1: The Oklahoma Bomber Timothy McVeigh goes to his death in silence,” June 12, 2001.

§ Alston Chase, *Harvard and the Unabomber: The Education of an American Terrorist* (New York: W.W. Norton, 2003).

¶ Daniel Pederson, “A mountain manhunt (hunt for suspected bomber Eric Rudolph),” *Newsweek*, July 27, 1998.

**Federal Document Clearing House, Congressional Testimony, October 1, 1997, Louis J. Freeh, Director, Federal Bureau of Investigation before the House Committee on International Relations.

- *Organized crime*^{*}: Organized criminal enterprises are modest versions of transnational criminal organizations and have many of the same attributes, skills, methods, and tactics. Like transnational criminal enterprises, their goal is that of using career criminals to conduct lifelong business in crime.

Classic organized crime is local to regional, and sometimes national. Many mafia organizations are organized crime versus transnational organized crime due to their limited reach.

Organized crime has focused on drug trafficking, prostitution, loan sharking, and racketeering and has compromised private and public organizations as well as government figures.

Organized criminal groups are highly sophisticated, are able to draw on specialists, and are able to obtain the equipment needed to achieve their goals efficiently. These groups form efficient, hierarchical organizations that can employ highly paid insiders. Targets of organized criminal groups may involve a high degree of risk in handling and disposal such as large quantities of money, equipment, and other goods.[†]

- *Sophisticated economic criminals*: Sophisticated economic criminals include those individuals, gangs, and organizations that apply critical thinking techniques to their criminal planning and operations.

Sophisticated economic criminals include career criminals who specialize in jewels, certain types of retail stores, safe cracking, banks, movie theaters, among others. Many of these criminals are individuals who work alone or in very small gangs. Sophisticated criminals take time to conduct an operation, sometimes conducting research about and surveilling a potential target for many months. Sophisticated criminals think through many aspects of the crime and carefully calculate the risk to minimize the possibility of being caught.

The goal of sophisticated criminals is usually to steal assets, though some may specialize in assassinations or other contract work for an organized crime group. Most sophisticated criminals are either part of an organized crime group or else work alone in order to avoid discovery and capture.

Sophisticated criminals are skilled in the use of certain weapons and tools and are efficient and organized. They plan their attacks and have sophisticated equipment and the technical ability to employ it. Sophisticated criminals are often assisted by insiders. They target high-value assets, frequently steal in large quantities and target assets with relatively low risk in handling and disposal.[‡]

- *Unsophisticated economic criminals*

Unsophisticated economic criminals are unskilled in the use of weapons and tools and have no formal organization. Their targets are those items that meet their immediate needs, such as drugs, money and pilferable items. Unsophisticated criminals are interested in opportune targets that present little or no risk. Breaking and entering or smash-and-grab techniques are common. Theft by insiders is also included in this category.[§]

^{*} Howard Abadinsky, *Organized Crime*, 9th ed. (Florence, KY: Wadsworth/Cengage Learning, 2010).

[†] Ted Krauthammer and Edward J. Conrath, *Structural Design for Physical Security* (Reston, VA: American Society of Civil Engineers, 1999), A-3.

[‡] Ted Krauthammer and Edward J. Conrath, *Structural Design for Physical Security* (Reston, VA: American Society of Civil Engineers, 1999), A-3.

[§] Ted Krauthammer and Edward J. Conrath, *Structural Design for Physical Security* (Reston, VA: American Society of Civil Engineers, 1999), A-3.

- *Street gangs* and street criminals:* Street criminals or street gangs focus primarily on the drug and sex trades and have a history of sometimes extreme violence.

Gangs may include Hispanic gangs; the Crips and Bloods; People Nation and Folk Nation; Jamaican posses; Asian/South Sea Islander gangs; Colombian gangs; Cuban Marielito; motorcycle gangs; racially, ethnically, or religiously oriented gangs; and prison gangs.

Gangs compel discipline and obedience from their members and often recruit the very young and most impressionable. Gangs may destroy neighborhoods and commercial districts with graffiti; belligerent behavior toward civilians; shakedowns of civilians and businesses; pimping, pandering, and prostitution; and the drug culture.

- *Special notes on lone criminals:* Lone criminals are individuals who commit crimes without the knowledgeable aid or assistance of others. Lone criminals include computer criminals, sophisticated criminals, and unsophisticated criminals. Lone criminals may be very successful or chronic petty criminals who seem to always get caught.

Lone criminals have included the Unabomber (Theodore Kaczynski), Eric Rudolph, and the alleged 2001 anthrax attacker Bruce Ivins.[†] Other lone criminals include individual insiders who target proprietary information and company assets.

- *Nonterrorist Violent Workplace Criminals[‡]: Workplace violence threat actors:* These include two main classes:

- *Domestic crimes violent criminals:* Domestic violent workplace crimes account for a large number of violent crimes in the United States and around the world.[§] Domestic violent criminals are individuals who are involved in unstable personal relationships with employees of an organization and who attack the domestic partner in the workplace. Increasingly, this kind of workplace violence is receiving the attention of the human resources industry in order to identify and provide early intervention to possible victims of such violent crimes. This is not only to protect the intended victim, but also innocent bystanders in the workplace who are sometimes targeted either intentionally or randomly.

Violence by such attackers is often sudden and very violent, often involving firearms.

- *Disgruntled employee or ex-employee:* Violence inflicted by coworkers and former workers of an organization may include fighting, threatening behavior, assault, harassment, stalking, and the like.

This type of violent attacker is known to target specific individuals, which may include his current or former manager and specific coworkers the individual feels may have either wronged him or gossiped about him.

* Bill Valentine, *Gang Intelligence Manual: Identifying and Understanding Modern-Day Violent Gangs in the United States* (Boulder, CO: Paladin Press, 1995).

[†] Kevin Whitelaw, “An unsatisfying end to the Anthrax Attacks Mystery: The FBI reportedly was ready to charge an Army scientist, but he apparently committed suicide this week,” *U.S. News & World Report*, August 1, 2008.

[‡] John Douglas and Mark Olshaker, *The Anatomy of Motive: The FBI’s Legendary Mindhunter Explores the Key to Understanding and Catching Violent Criminals* (New York: Scribner; Mindhunters, 1999).

[§] James E. Crockett, *Business Insurance Magazine*, July 5, 1999.

Disgruntled violent employees are almost entirely male and most often use knives or guns to attack their intended victims, though acid and flammable chemicals have also been used.*

- *Angry visitors:* Angry visitors can sometimes cause violence when their unreasonable (and sometimes reasonable) demands are not met. Frustration mounts as they are unable to achieve their desired results, and after escalating their interaction, they may eventually resort to violence.
- *Sexual criminals:* Sexual criminals usually prey on women and children who are in vulnerable circumstances. Sexual criminals may act alone or in a group. Sexual criminals may be playing out a fantasy in their mind, and research indicates that they are likely to experience violent sexual fantasies well before they begin to act them out.[†] According to the American Medical Association (AMA), sexual assault is the most rapidly growing crime in the United States.[‡] The National Victim Center reports that more 700,000 women are raped or sexually assaulted annually.
- *Muggers/parking lot violence/robberies gone wrong:*
 - *Muggers/parking lot violence:* Muggers and parking lot violence can be a problem at any organization where street crime can spill onto the organization's property.
 - *Robberies gone wrong:* Some workplace violence events are related to robberies. This is particularly true of taxis, convenience stores, filling stations, and other stop-and-shop facilities.

In one famous event, gunmen seized 30 hostages at a large electronics store in Sacramento, California. The incident ended after 8 hours when police stormed the store after gunmen “walked systematically down the line shooting hostages.”[§]

In another, two heavily armed and body-armored gunmen robbed a North Hollywood bank and when confronted by police outside, they touched off a gunfight with the police that redefined the use of high-powered weapons in policing situations; this incident remains one of the bloodiest days in U.S. law enforcement history.[¶]

- *Deranged persons and stalkers:* Deranged or mentally ill people can strike out with violence without any notice. Violence can accompany alcoholism, drug abuse, and certain types of mental illness, particularly paranoid schizophrenia.^{**}
- *Stalkers:* Celebrities John Lennon, Jill Dando, and Rebecca Schaeffer were killed by stalkers Mark David Chapman, Barry George, and Robert

* Louis P. DiLorenzo and Darren J. Carroll, “Screening applicants for a safer workplace (part 2),” *HR Magazine*, March 1, 1995; “Janitor Jonathan D’Arcy, enraged when his February paycheck was late, poured gasoline on the company’s bookkeeper and set her on fire.”

† Thomson Gale, “Sexual predation characteristics,” *World of Forensic Science*, 2005 (Highbeam Research, April 23, 2009, www.highbeam.com).

‡ “Why sexual assault is the most rapidly growing crime in the nation,” *Jet Magazine*, 1995 (Highbeam Research, April 23, 2009, www.highbeam.com).

§ Richard C. Paddock and Carl Ingram, “Five killed in Calif. hostage rescue; police storm store where gunmen seized 30 people in foiled robbery,” *The Washington Post*, April 5, 1991.

¶ Bill Coffin, “War zone: The North Hollywood shootout 10 years later:...,” *Risk Management*, March 1, 2007.

**Richard A. Friedman, “Violence and mental illness — How strong is the link?” *The New England Journal of Medicine*, November 16, 2006.

John Bardo, respectively.*†‡ Businesses that cater to celebrities and the wealthy must be constantly aware of the risks their clientele face from celebrity stalkers. Many more ordinary citizens have been attacked, mutilated, and killed by stalkers. In the book *Blind-Sided*, author Gregory K. Moffatt stated:

Research has repeatedly shown that stalkers usually know their victims before the stalking begins. One study on stalking demonstrated that nearly all stalkers knew their victims: 57% of the victims had prior relationships with their stalkers and another 34% of the victims were at least acquaintances before the stalking began. Only 6% did not know their stalkers.§

- *Subversives and Saboteurs*
 - *Cause-oriented subversives*: Cause-oriented subversives may include activist groups with an agenda opposed to a government, religion, cause, or industry. This can include such groups as the Animal Liberation Front (ALF), the Environmental Liberation Front (ELF), and others.
 - *Nonaligned subversives*: Other subversive acts can include civil disorder events that are related to protests or civil riots. For example, the city of Los Angeles, California, was gripped by civil disorder and riots in 1992 following the trial of Rodney King, a black motorist who was beaten by Los Angeles Police Department (LAPD) officers. The beating was caught on camera and played on local television news stations.¶ Many businesses were damaged in the riots that followed.
 - *Political and industrial spies*: Increasingly, organizations are being targeted by political and industrial spies. One article noted that industrial spies play a very big role behind the scenes at World Trade Organization talks.** There have been many cases of industrial and political spies prying into the secrets of large and small organizations.
 - *Hackers*: Hackers may deface Web sites, damage networks, or act as spies to extract important information. In one recent case, hackers stole highly sensitive data on the U.S. Pentagon's newest fighter jet, the Joint Strike Fighter, from military contractor's computers that were connected to the Internet.
 - *Invasion of privacy threat actors*: Paparazzi and celebrity stalkers are the bane of celebrities for their invasion of privacy. Businesses that cater to the wealthy and celebrities are often confronted with aggressive celebrity seekers, photographers, and autograph seekers who interrupt the private moments of

* Tony Barrett, "Why I shot Lennon; I was tired of being a nobody says Mark Chapman." *Liverpool Echo* (Liverpool, England), October 15, 2004.

† "Guilty — Jill Dando's killer gets life," *Evening Standard* (London), July 2, 2001.

‡ "Man is being held in actress's death" (regarding the death of Rebecca Schaeffer), *The New York Times*, July 20, 1989.

§ Gregory K. Moffatt, *Blind-Sided — Homicide Where It Is Least Expected* (Santa Barbara, CA: Greenwood, 2000), 82.

¶ Lou Cannon, *Official Negligence: How Rodney King and the Riots Changed Los Angeles and the LAPD* (New York: Basic Books, 1999).

** Les Blumenthal and Michael Doyle, "Spies bring trade secrets to the table at WTO talks," *Star Tribune* (Minneapolis, MN), November 27, 1999.

their clientele and subvert the purpose of a commercial enterprise for their own purposes.

- *Persistent rule violators:* These are individuals who frequent the organization's facilities either as employees or as visitors and who act as though the organization's assets are their own to use or abuse as they wish. Though warned of rules of conduct, they persist in violating the rules. Such individuals create problems for the organization in several ways:
 - They set a bad example for behavior for others.
 - They often require special attention to accommodate their demands or actions.
 - They often create safety or code of conduct preconditions that could lead to either injuries or to conduct problems on a larger scale. (When one person acts out, it is common to see others follow that person's example.)
 - They are disruptive of a normally orderly environment.
 - Their behavior may be illegal or affect the good business reputation of the organization, in some cases putting the organization at risk of prosecution for not abating the behavior, such as in racial or sexual misconduct cases (e.g., where a manager is abusing his or her power over an employee).
 - Persons who abuse parking privileges, cut in line, demand special treatment, or act abusively toward employees are subversive influences.

Although organizations do not like to have to deal with such individuals, they are a special class. These are individuals who through their own narcissism and belligerence become a law unto themselves and demand that the world accommodate their perspective. Such people are threat actors.

- *Petty Criminals*

- *Definition:* Petty crimes are offenses that are less than felonies and are usually punishable by a fine, a penalty, forfeiture of property, or imprisonment in a jail facility rather than in a penitentiary (misdemeanors).
- *Vandals:* Vandals destroy property's value by defacing it. Vandals have caused millions of dollars in damage to property and have damaged the business opportunities of entire communities.*
- *Pickpockets:* Pickpockets ply their trade in many public places, including in hotels, restaurants, retail malls, parking lots and parking structures, elevator lobbies, and literally anywhere two or more people come into contact and especially where one of those people may be distracted. Businesses that provide such environments can be harmed by the damage to their reputation as a safe environment to frequent.
- *Prostitutes, pimps, and panderers:* Prostitution can affect hotels, retail malls, and other public spaces and can damage the reputation of the business.
- *Other petty crimes include disturbing the peace, public nuisance, and public drunkenness.*

* Joseph Rivera, *Vandal Squad: Inside the New York City Transit Police Department* (Brooklyn, NY: Powerhouse, 2008).

Design Basis Threat

Risk analysts must determine a *design basis threat* (DBT) that will be used as a baseline for the countermeasures. A DBT is the level of threat actor that the countermeasures should be able to address with reasonable effectiveness.

There are actually two DBTs: The first is the DBT that the security program will be designed to protect against, and the second is the DBT that the security program will be designed to deter and mitigate. One can deter against terrorist attack in a commercial environment, but it would be prohibitively costly to protect against one. However, an organization can mitigate some of the potential for damages of a terrorist attack.

For example, in Al Qaeda's attack on the Marriott Hotel in Islamabad on September 21, 2008, a truck carrying 1 ton of explosives detonated 20 meters away from the building due to its having been stopped at that distance by a hydraulic barrier. Fifty-three people were killed in the attack. The truck's explosive charge, which was also surrounded with aluminum powder (accelerating the resulting fire) and artillery shells (increasing the resulting shrapnel), would certainly have killed many more if it had been able to get close to the hotel's main entry.*

However an organization can do much to prevent ODC (ordinary decent crime).† ODC includes economic crimes, nonterrorist violent crimes, subversive criminal acts, and petty crimes. These can all be addressed in a baseline security program.

Figure 7.2 illustrates the characteristics of terrorist and various types of criminal threat actors. This figure illustrates that each type has very different characteristics.

PRACTICE

- *Effectively assess threats*
 - Identify potential threat actors.
 - Identify their motivation, capabilities, and history (thus their level of intent, skills, weapons, and tactics and what types of targets they have chosen in the past).
 - Develop a list of the organization's assets, and determine which of the weapons and tactics are most likely to be of use in attacking the organization.
 - Compare that data to information about the organization's assets to be protected, and determine which potential threat actors are likely to be most effective against the organization.
- *Identify potential threat actors:* An analyst can identify potential threat actors in two steps. First, list the five types of threat actors, listed above. Then identify potential individual organizations and classes of individuals that most fit the descriptions of the five types of threat actors.

For example, as regards potential terrorism threat actors, again there are five types as listed above. Local law enforcement will have a list of each of the potential threat actors who fit the descriptions of the five classes that are active in the

* "It's our 9/11; 53 killed in Pakistan hotel bomb attack," *The Mirror* (London), September 22, 2008: "As sniffer dogs start barking around the truck, the vehicle starts ramming the hotel's hydraulic barrier and guards shout at people to run as a fire breaks out in the cab. Seconds later the screens flash blue as the huge bomb obliterates the area."

† Sean O'Neill and David Lister, "MI5 given task of boosting intelligence on money-making," *TimesOnline* (London), February 25, 2005: "... The IRA has never been a stranger to what people in Northern Ireland used to refer to as 'ordinary decent crime.'"

Offender Characteristics					
Characteristics	Terrorists	Economic Criminals	Violent Criminals	Subversives	Petty Criminals
Depth of Violence					
Mass Casualties	X				
Few Casualties	X		X		
Single Casualties	X	X	X	X	
Injuries	X	X	X	X	X
Property Crimes					
Destruction of Property	X	X	X	X	
Theft of Property		X	X	X	X
Damage of Property	X	X	X	X	X
Information Crimes					
Destruction of Information	X	X		X	X
Theft of Information	X	X		X	X
Damage to Information	X	X		X	X
Crimes against Reputation					
Damage to Business Reputation	X	X	X	X	X
Attack Methods					
May Attack in Plain View	X	X	X		
Usually Attack in Stealth		X		X	X
On Interruption of Attack					
Will Likely Give Up on Interruption	X	X	X	X	X
On Forcible Response					
Will Repel Forcible Response	X				
May Repel Forcible Response	X	X	X	X	

FIGURE 7.2 Offender Characteristics

area of operations of the law enforcement agency. For projects within the United States, a good source of this information is the Federal Bureau of Investigation's (FBI's) local terrorism task force. For other countries, similar sources exist within their local law enforcement agencies.

- *Consult sources:* Other sources are also valuable, including Internet research. This is covered in detail in Chapter 3, “Risk Analysis Skills and Tools.” Numerous reputable organizations exist that have excellent reference material on both terrorism and ODC criminal activity and groups.
- *Identify their motivation, capabilities, and history* (thus their level of intent, skills, weapons, and tactics and what types of targets they have chosen in the

past): Although this changes constantly, an analyst can follow the news and create a bibliography. Better consultants do this in an ongoing fashion. This is also discussed in detail in Chapter 3, “Risk Analysis Skills and Tools.” Other good sources also exist (see footnotes on this page). The books and articles listed here comprise a wealth of resource into the methods and tactics used by terrorists and criminals of all types, and the implications of those methods and tactics on the organizations they attack.

- *Terrorist targeteering screen:* Develop a targeteering list for each of the classes of potential threat actors. Defense departments of various countries have taken this to a fine art. Good sources of targeteering information include Malcolm Nance’s *Terrorist Recognition Handbook*. Nance is one of the world’s leading experts on terrorist targeteering and is referenced by many articles and thesis papers both in and out of the military. (See Figure 7.3.)

In Alicia L. Welch’s 2007 Naval postgraduate school thesis titled “Terrorism Awareness and Education as a Prevention Strategy for First Responders,” she quoted Nance:

The targeteer uses three basic tactical actions in deciding on a specific target, all of which are designed to achieve maximum dramatic impact:

- Speed — The target must be struck quickly to enhance the effect of fear.
- Surprise — The victims must be taken completely unaware; nothing should transmit the impending operation except only the vaguest of threats.
- Violence of Action — The incident should strike terror and fear into the hearts of its victims through the absolute, horrific violence.

* Norman M. Garland and Gilbert B. Stuckey, *Criminal Evidence for the Law Enforcement Officer*, 4th ed. (New York: McGraw-Hill/Glencoe, 1999).

† Malcolm Nance, *Terrorist Recognition Handbook*, 2nd ed. (Boca Raton, FL: CRC Press, 2008).

‡ Joseph Rivera, *Vandal Squad: Inside the New York City Transit Police Department* (Brooklyn, NY: power-House, 2008).

§ John Douglas and Mark Olshaker, *The Anatomy of Motive: The FBI’s Legendary Mindhunter Explores the Key to Understanding and Catching Violent Criminals* (New York: Scribner; Mindhunters, 1999).

¶ Paul F. Cromwell and James N. Olson, *Breaking and Entering: Burglars on Burglary* (Florence, KY: Wadsworth, 2004).

†† Dennis L. Demey, James R. Flowers, and Michael L. Sankey, *Don’t Hire A Crook! How to Avoid Common Hiring (and Firing) Mistakes* (Tempe, AZ: Facts on Demand, 1999).

‡‡ Imre A. Wiener, *Economic Criminal Offenses: A Theory of Economic Criminal Law* (Akademiai Kiado, 1990).

§§ Daryl A. Hellman, *Economics of Crime: Theory and Practice*, 6th ed. (Boston, MA: Pearson Custom, 2006).

¶¶ David P. Farrington, Lawrence Sherman, and Brandon C. Welsh, *Costs and Benefits of Preventing Crime: Economic Costs and Benefits* (Boulder, CO: Westview Press, 2000).

*** Dean De Jong, “Civil disorder: Preparing for the worst,” *The FBI Law Enforcement Bulletin*, March 1, 1994.

††† Patrick J. Ortmeier, *Security Management: An Introduction*, 2nd ed. (Upper Saddle River, NJ: Prentice Hall/Criminal Justice, 2004).

††† Timothy J. Walsh and Richard J. Healy, eds., *Protection of Assets (POA) Manual* (Santa Monica, CA: Merritt Company, 1987). (Available through ASIS International Bookstore 412-741-1495. This four-volume set of books is absolutely recommended.)

¶¶¶ Alicia L. Welch, “Terrorism Awareness and Education as a Prevention Strategy for First Responders,” March 2006, Naval Postgraduate School, Monterey, CA.



FIGURE 7.3 Terrorist Targeteering

In her thesis, she expanded on Nance's work and stated:

The three elements of targeteering include Motive, Opportunity and Means (MOM). Motive: Does the terrorist group have a reason for selecting the target? Does the group have the opportunity to affect a strike against its enemies that is both meaningful and effective? The targeteer will make it a priority to create or wait for the appropriate time, circumstances, and environment to strike. Means: Does the group have the materials, manpower, secrecy, and support to carry out the mission?

From this book, the KSM-Asset Target Value for Terrorism Matrix is an excellent surrogate for determining terrorist targeteering in the absence of more specific data. The KSM-Asset Target Value for Terrorism Matrix was developed by the author as a screen for targeteering for organizations allied with Al Qaeda (many of which were targeted by Khalid Sheikh Mohammed [KSM]). It is derived from evaluation of numerous Al Qaeda attacks and the elements each have in common.

Similarly, the Asset Target Value Matrices for economic and violent crimes presented herein are useful to establish targeteering information for those types of crimes.

- **Asset/Attack Matrix:** Develop a list of the organization's assets, and determine which of the weapons and tactics are most likely to be of use in attacking the organization.

Chapter 5 explained how to develop a list of the organization's key assets. By using the Asset/Attack Matrix (described in Chapter 8, "Assessing Vulnerability"), you will be able to determine which weapons and tactics are most likely to be of use in attacking the organization.

Although the Asset/Attack Matrix is a vulnerability tool, its use is also essential in helping to define the design basis threat. This is because the Asset/Attack Matrix defines which types of weapons and attack scenarios are most likely to succeed against the organization's facilities. By matching this information to the targeting information about the threat actors, you can more easily identify which threat actors are most likely to be interested in this organization's facilities.

A complete listing of terrorist attack tactics and appropriate tactical countermeasures can be found in Nance's 2008 book *Terrorist Recognition Handbook* (2nd ed., pp. 363–385). Some of those countermeasures are appropriate for counterinsurgency environments. See Chapter 16 of this book for appropriate antiterrorism countermeasures that are suitable for government, nongovernmental organizations (NGOs), and commercial environments.

A comprehensive listing of baseline security program countermeasures can also be found in Chapter 16 of this book to address economic crimes, nonterrorism violent crimes, subversives, and petty criminals.

- Compare that data to information about the organization's assets to be protected and determine which potential threat actors are likely to be most effective against the organization.

By matching up the methods and tactics used against the vulnerabilities of the organization, an analyst can identify those potential threat actors who are most likely to take action against the organization. The design basis threat worksheet discussed in this chapter accomplishes this task.

TOOLS

This book presents two software tools to assist in threat analysis:

- *Adversary/Means Matrix*: The Adversary/Means Matrix helps the analyst identify the types of weapons, entry methods, and attack scenarios that are used by various types of threat actors.
- *Asset/Attack Matrix*: The Asset/Attack Matrix helps the analyst identify what types of weapons, entry methods, and attack scenarios would be most effective against the organization's various assets.

The objectives of these tools are as follows:

- *Adversary/Means Matrix*: As the analyst moves into establishing the organization's vulnerabilities, the analyst will need to understand the characteristics, entry methods, and attack scenarios used by various potential threat actors and keep these capabilities in mind as the analyst is identifying exploits for vulnerabilities. For example, a prison is inherently less vulnerable to intrusion than a warehouse because most of the classic entry methods are of no use against a prison.

- *Asset/Attack Matrix:* The Asset/Attack Matrix assists the analyst in identifying the design basis threat by identifying which types of entry methods and attack scenarios could be eliminated due to the unique attributes of the organization's facilities and assets. Also, by helping to identify those assets that are most vulnerable and to which types of weapons and attack scenarios they are most vulnerable, it assists the analyst in focusing risk mitigation recommendations on countermeasures that can mitigate those vulnerabilities.

Adversary / Means Matrix

- *Purpose:* The Adversary/Means Matrix helps the analyst define various potential threat actors and their potential for creating problems for the organization.
- *Functions:* The Adversary/Means Matrix should accommodate all of the following:
 - List and categorize potential threat actors by types and, where possible, by the name of the group. Some can only be identified by type (e.g., sophisticated criminals).
 - Identify their level of professionalism, including their motivation, capabilities, and history; training level including operations* and tradecraft† knowledge; surveillance capabilities; planning skills; and organization and support.
 - List the types of weapons the potential threat actor may have access to.
 - List if possible the types of entry methods this type of threat actor may use.
 - List what types of weapons the threat actor may be known or suspected to use.
 - List typical anticipated attack scenarios.
- *Attributes:* The Adversary/Means Matrix can be created using an off-the-shelf software tool such as SVA-Pro or a build-it-yourself software template, such as Microsoft Excel, Access, or MS Word. In each case, the information listed above should be included. Some analysts prefer a more text-oriented approach, while others prefer a numeric rating. The text-based approach offers more information but is also more difficult and time consuming to read and assess overall data from. Certain tools, such as SVA-Pro, combine both text and numeric ratings and so offer both overview (numeric) and deeper reference when questioning the analysis. A self-developed database approach such as Microsoft Access can also do this.
- *Example:* This section is for those readers who wish to use the Excel risk analysis templates that can assist in performing the analysis for any size of project from small to global and also can be used as report inserts to illustrate the discussion points of the Risk Analysis Report. Although other tools exist as mentioned above, this approach is very low cost (except for your time) and provides results that equal or exceed the most expensive software tools available.

In the first two examples, the master templates will be set up for all other templates throughout the rest of the book, so these will take a little longer to

* Operations Knowledge refers to their ability to carry out a criminal or terrorism operation including use of weapons, suppression and control of subjects, ability to move against the objective, and so forth.

† Tradecraft Knowledge refers to their training in covert operations including surveillance, communications, maintenance of cover or pretense, and so forth.

assemble than all the others in the book, as these will be used as the basis for all others that follow. Once these two are formatted and programmed, all the others can be assembled in short order.

The first tool is called an Adversary/Means Matrix. The second tool is called an Asset/Attack Matrix. These are both used to develop the threat analysis and the design basis threat.

- The Adversary/Means Matrix helps the analyst identify the design basis threat by identifying the type of threat actors who could carry out operations against the organization (terrorism and ODC).
- The Asset/Attack Matrix helps the analyst identify the design basis threat by identifying the types of weapons and attack scenarios that are of most concern to the organization.

By combining the results of both, it becomes clear first what types of weapons and attack scenarios are of the greatest concern and then which types of attackers utilize those attack scenarios and weapons.

Coupled with the later findings of asset target value (which types of facilities are of most interest to which types of attackers), it can become clear whether to establish the design basis threat as terrorism (and what type) or ODC.

In any event, every organization needs what I call a *baseline security program*. Every facility also exhibits certain unique vulnerabilities that should be addressed in addition to the baseline security program, and some (not all) facilities exhibit the historical characteristic of targets of terrorism. For those facilities, terrorism should be the DBT. The DBT then infers the types of countermeasures that must be used to effectively deter or counter the DBT.

The Microsoft Excel templates perform quantitative analysis. Any of the tools mentioned in the previous section can work just as practically. The example shown in Figure 7.4 presents a sheet view of a typical Adversary/Means Matrix for a large project with potential terrorist and criminal threat actors.

It should be noted that the approach of entering both text (qualitative) and numeric (quantitative) data is superior to either text or numeric data alone. The author converts quantitative analysis results into qualitative in the report phase of the work. Software tools such as SVA-Pro accommodate both qualitative and quantitative in the data entry process; however, arguably, its data are much more difficult to digest and process. An analyst can also accomplish simultaneous qualitative/quantitative entry either with a database application or by parallel document entries (text in one document and data in another), thus building the report at the same time as entering the resource data. I do it in sequence (just my personal preference), though you could make the argument that simultaneous data entry is superior, if nonetheless mind-bogglingly tedious. In my mind, the sheer number of data points considered in this approach more than makes up for any other shortcomings.

In any event, critical thinking principles should be applied to the analysis portion prior to report writing in order to help determine the risk level and what types of countermeasures are appropriate. Although the worksheets described herein provide the grinded data for the analysis, they do not perform the actual analysis. That is for the analyst to do.

- *Professionalism:* Professionalism is to threat actors as it is to anything else. The more professional the threat actor, the more dangerous he or she is. More sophisticated countermeasures must be to address the threat actor. For example,

Mega Towers Adversary/Means Matrix															
Characteristics	ADVERSARIES			Entry Methods			Smaller Weapons			Attack Methods	Explosives/Incendiaries		Other	Avg. Rank	Ranking
	Terrorists	Organized Crime Groups	Sophisticated Criminals	Cults/Dedicated Activist Groups	Motivational Subversives	Unsophisticated Criminals	Street Criminals	Transnational Criminal Organization	Economic Criminals		Bladed Weapons	Hand Grenades	Improvised Explosive Device (IED)		
Class I - State Sponsored Terrorist	10	10	10	10	10	10	10	5	10	10	10	10	10	5	10
Class II - Religious Extremist Terrorist	10	10	10	9	9	10	4	10	10	10	10	10	10	4	10
Class III - Radical Revolutionary/Quasi Religious	10	9	9	8	8	8	5	10	10	10	10	10	10	3	9
Class IV - Guerrilla/Mercenary Soldiers	10	7	7	7	7	5	10	10	10	10	10	10	10	3	8
Class V - Amateur Terrorists	7	5	5	5	5	5	2	10	10	10	10	10	10	3	10
Economic Criminals															
Transnational Criminal Organization	8	8	8	8	8	8	8	10	10	10	2	1	1	5	10
Organized Crime Groups	8	8	8	8	8	8	8	10	10	10	2	1	1	5	10
Sophisticated Criminals	7	7	7	7	7	7	1	10	10	10	2	1	1	5	10
Unsophisticated Criminals	4	3	3	3	3	3	1	2	5	10	10	1	1	3	10
Street Criminals	3	3	3	3	3	3	0	2	2	0	0	0	0	0	27
Petty Criminals															
Workplace Violence Threat Actors	7	6	6	6	6	6	1	10	10	8	10	0	0	2	10
Angry Visitors	5	5	5	5	5	5	0	10	10	5	10	0	0	0	10
Sexual Criminals	7	5	5	5	5	5	0	10	10	5	10	0	0	0	10
Muggers/Parking Lot Violence	7	10	10	10	10	10	0	2	10	5	10	0	0	1	11
Civil Disorder Event Violence	8	8	8	8	8	8	0	3	10	5	10	0	0	1	8
Deranged Persons	7	10	10	10	10	10	0	2	10	5	10	0	0	0	11
Subversives															
Cause-Oriented Subversives	7	6	6	6	6	6	0	10	10	5	7	2	0	0	20
Political and Industrial Spies	8	10	10	10	10	10	3	10	10	5	2	0	0	0	14
Saboteurs	8	7	7	7	7	7	3	10	10	5	5	0	0	0	17
Cults/Dedicated Activist Groups	10	8	8	8	8	8	3	10	10	5	4	2	0	0	16
Hackers	7	10	10	10	10	10	1	10	10	3	2	1	0	0	15
Invasion of Privacy Threat Actors	10	8	8	8	8	8	1	10	10	5	4	4	0	0	13
Persistent Rule Violators	5	5	5	5	5	5	0	10	10	5	1	0	0	0	22
Petty Criminals															
Vandals	5	2	2	2	2	2	0	4	10	4	5	2	0	0	26
Pickpockets and Purse Snatchers	3	5	5	5	5	5	0	1	10	4	1	5	1	0	25
Prostitution/Pimping	7	5	5	5	5	5	0	5	10	8	1	3	0	0	23
Other Petty Criminals	7	5	5	5	5	5	0	2	10	4	1	1	0	0	24
Average	9	6	8	8	8	8	5.4	4.8	4.7	0.5	0.4	0.4	0.7	0.6	11.73
Ranking	9	3	1	5	4	6	7	19	20	20	15	8	12	12	2

Ratings:
 High History 10
 Medium History 5
 Low History 1

FIGURE 7.4 Adversary/Means Matrix

Al Qaeda has used tandem heavy trucks to breach hardened perimeters, where the lead truck was equipped with a ramming device and the second truck followed closely behind. Protecting against this type of entry requires more robust barriers. Factors to consider in professionalism include the following.

- Motivation
 - Capabilities
 - History
 - Training level
 - Surveillance capabilities
 - Planning skills
 - Organization and support
- *Access to types of weapons:* The extent of access to weapons is also a factor in establishing the design basis threat. The more weapons the threat actor has access to and training to use, the more dangerous the threat actor is. As with other sections herein, the following are only examples, and these should be modified depending on the environment, type of facilities, and so forth. Weapon categories include:
 - Bladed weapons
 - Small arms
 - Heavy arms
 - Shoulder-fired missiles (rocket-propelled grenades [RPGs], etc.)
 - Mortars
 - Hand grenades
 - Explosives
 - Chemicals
 - Vehicles
 - Watercraft
 - Aircraft
 - Suicide volunteers
 - Computers and hacking skills
- *Entry methods:* Without access by a threat actor, there is no risk, so access control is a key concept in security. Entry methods may vary depending on the type of facility. The following list is an example only. Typical entry methods used by threat actors include:
 - False credentials
 - Social engineering
 - Entry by threat
 - Forced entry
 - Breaking and entering
 - Insider
 - Hacking
- *Threat scenarios used:* Each type of threat actor uses different attack scenarios, and each have different consequences, and thus the categories. Threat scenarios may vary depending on the types of assets and the types of facilities under consideration. The following are examples only. Typical threat scenarios include:
 - Terrorism attack scenarios
 - Improvised explosive devices (IEDs)
 - Suicide bomber
 - Vehicle-borne IED (VBIED)

- Airborne IED
- Waterborne IED
- Dirty bomb
- Nuclear weapon
- Chemical/biological/radiological/nuclear weapons
- Cyberterrorism
- Economic crimes
 - Robbery
 - Burglary
 - Insider theft
 - Proprietary information theft
 - Crimes against the organization's business reputation
 - Computer crimes
- Violent crime attack scenarios
 - Violence against employees
 - Violence against the public on the organization's property
 - Bladed weapons
 - Handguns
 - Available weapons
- Subversive acts
 - Civil disorder
 - Riots
 - Protests
 - Intimidation
 - Drugs in the workplace
 - Sabotage
 - Corporate spying
- Petty crimes
 - Purse snatching/pickpocketing
 - Vandalism
 - Prostitution, pimping, and pandering
 - Other petty crimes
- *How to set up the matrix:* This book explains each element of risk analysis and countermeasure selection in terms of its theory, practice, and tools. The book also discusses in adequate detail how to assemble MS Excel spreadsheets for each element. Those readers who prefer to use a commercial software tool may wish to skip the sections explaining how to build the Excel spreadsheets.

For those who are interested in building and using their own world-class risk analysis software tool, the first two tabs on the Excel workbooks are explained in cell-by-cell detail and after that in adequate detail to build the remaining sheets. The first of these was the Consequence Matrix, and the second is this, the Adversary/Means Matrix. The Consequence Matrix builds the basic matrix on which most other matrices are formed (the list of assets). The Adversary/Means Matrix is built on the list of threat actors.

Following are instructions on how to set up the matrix in Excel. These are basic instructions and will result in a workable matrix that calculates and ranks results. Instructions for setting up the first of these matrices are described in great detail. The instructions for others will be simplified, as the reader will have an understanding after the first matrix of how to set these up and how

they work. Accordingly, bear with the instructions for the first matrix, The Adversary/Means Matrix, as the detail helps assure that all the matrices are set up correctly.

Open Excel to a new worksheet (Tab 2): Enter the data as shown on the figures and as noted below:

- 1 Go to Cell 2B, Enter the Project Name. **Bold This.** Select the Font to 14
- 2 Cell 3B, Enter “Adversary/Means Matrix”. **Bold This.** Select the Font to 14
- 3 Cell 7B, Enter “ADVERSARIES”. **Bold This**
- 4 Cell 8B, Enter “Terrorists”. **Bold This**
- 5 Cell 9B, Enter “Class I — State Sponsored Terrorist”
- 6 Cell 10B, Enter “Class II — Religious Extremist Terrorist”
- 7 Cell 11B, Enter “Class III — Radical Revolutionary/Quasi-Religious”
- 8 Cell 12B, Enter “Class IV — Guerrilla/Mercenary Soldiers”
- 9 Cell 13B, Enter “Class V — Amateur Terrorists”
- 10 Cell 14B, Enter “Economic Criminals”. **Bold This**
- 11 Cell 15B, Enter “Transnational Criminal Organization”
- 12 Cell 16B, Enter “Organized Crime Groups”
- 13 Cell 17B, Enter “Sophisticated Criminals”
- 14 Cell 18B, Enter “Unsophisticated Criminals”
- 15 Cell 19B, Enter “Shrinkage/Pilfering”
- 16 Cell 20B, Enter “Violent Criminals”. **Bold This**
- 17 Cell 21B, Enter “Workplace Violence Threat Actors”
- 18 Cell 22B, Enter “Angry Visitors”
- 19 Cell 23B, Enter “Parking Area Violence”
- 20 Cell 24B, Enter “Rapists/Muggers”
- 21 Cell 25B, Enter “Civil Disorder Event Violence”
- 22 Cell 26B, Enter “Subversives”. **Bold This**
- 23 Cell 27B, Enter “Protestors/Nonviolent Civil Disorder”
- 24 Cell 28B, Enter “Political and Industrial Spies”
- 25 Cell 29B, Enter “Saboteurs”
- 26 Cell 30B, Enter “Cults”
- 27 Cell 31B, Enter “Hackers”
- 28 Cell 32B, Enter “Lone Wolves”
- 29 Cell 33B, Enter “Paramilitary Group”
- 30 Cell 34B, Enter “Persistent Rule Violators”
- 31 Cell 35B, Enter “Petty Criminals” **Bold This**
- 32 Cell 36B, Enter “Vandals”
- 33 Cell 37B, Enter “Pickpockets and Purse Snatchers”
- 34 Cell 38B, Enter “Prostitution”
- 35 Cell 39B, Enter “Other Petty Criminals”
- 36 Cell 40B, Enter “Average”. **Bold This**
- 37 Cell 41B, Enter “Ranking”. **Bold This**
- 38 Cell 42B, Enter nothing (blank cell)
- 39 Cell 43B, Enter “Ratings”. **Bold This**

- 40 Cell 44B, Enter “High Indicator”
- 41 Cell 45B, Enter “Medium Indicator”
- 42 Cell 46B, Enter “Low Indicator”
- 43 Select Column B, align the text to the right except for the two Cells B2 and B3, keep them aligned to the left
- 44 Cell 44C, Enter “10”. Go to Formats>Conditional Formatting
- 45 Under Condition 1, choose Cell Value Is between 0 and 3.25
- 46 Under Condition 1, click on Format Tab then on the Patterns Tab and choose the Color to be Green
- 47 Still in the Conditional Formatting Window, click on the Add> Tab
- 48 Under Condition 2, choose Cell Value Is between 3.25001 and 6.55
- 49 Under Condition 2, click on the Format Tab then on the Patterns Tab and choose the Color to be Yellow
- 50 Still in the Conditional Formatting Window, click on the Add> Tab
- 51 Under Condition 3, choose Cell Value Is between 6.55001 and 10
- 52 Under Condition 3, click on the Format Tab then on the Patterns Tab and choose the Color to be Red. Click on “OK”
- 53 Cell 44C, should turn to Red Filled instantaneously
- 54 Copy Formatting (use the copy format paintbrush) from C44 through C47 (this will copy the Conditional Formatting to the cells)
- 55 Cell 45C, Enter “5”. The Cell should turn to Yellow Filled instantaneously
- 56 Cell 46C, Enter “1”. The Cell should turn to Green Filled instantaneously

- 57 Go to Cell C5, Right Click>FormatCells>Alignment>Orientation>Enter 75 Degrees
- 58 Cell C5, Enter “Motivation”
- 59 Copy Formatting (use the copy format paintbrush) from C5 through BR5 (this tilts all those cells 75 degrees)
- 60 Cell D5, Enter “Capabilities”
- 61 Cell E5, Enter “History”
- 62 Cell F5, Enter “Training Level”
- 63 Cell G5, Enter “Surveillance Capabilities”
- 64 Cell H5, Enter “Planning Skills”
- 65 Cell I5, Enter “Organization & Support”
- 66 Select Columns C through I, Right Click and change the Column Width to be 3
- 67 Cell J5, Enter nothing (blank) — This is the beginning of the “Entry Methods”
- 68 Select Column J, Right Click and change the Column Width to be 0.2

- 69 Cell K5, Enter “Cutting Torch/Burning Bar”
- 70 Cell L5, Enter “False Credentials”
- 71 Cell M5, Enter “Social Engineering”
- 72 Cell N5, Enter “Vehicles”
- 73 Cell O5, Enter “Forced Entry”
- 74 Select Columns K through O, Right Click and change the Column Width to be 3
- 75 Cell P5, Enter nothing (blank) — This is the beginning of the “Attack Methods”
- 76 Select Column P, Right Click and change the Column Width to be 0.2

- 77 Cell Q5, Enter “Bladed Weapons”
78 Cell R5, Enter “Small Arms”
79 Cell S5, Enter “Heavy Arms”
80 Cell T5, Enter “Shoulder-Fired Missiles (RPG)”
81 Cell U5, Enter “Mortars”
82 Cell V5, Enter “Hand Grenades”
83 Select Columns Q through V, Right Click and change the Column Width to be 3
84 Cell W5, Enter nothing (blank) — This is the beginning of the “Explosives/Incendiaries”
85 Select Column W, Right Click and change the Column Width to be 0.2
- 86 Cell X5, Enter “Improvised Explosive Device (IED)”
87 Cell Y5, Enter “Suicide Bomber”
88 Cell Z5, Enter “Truck Bomb”
89 Cell AA5, Enter “Car Bomb”
90 Cell AB5, Enter “Small Watercraft Bomb”
91 Cell AC5, Enter “Large Watercraft Bomb”
92 Cell AD5, Enter “Small Aircraft”
93 Cell AE5, Enter “Large Aircraft”
94 Cell AF5, Enter “Dirty Bomb”
95 Select Columns X through AF, Right Click and change the Column Width to be 3
96 Cell AG5, Enter nothing (blank) — This is the beginning of the “Other”
97 Select Column AG, Right Click and change the Column Width to be 0.2
- 98 Cell AH5, Enter “Chemical Agents”
99 Cell AI5, Enter “Biological Agents”
100 Cell AJ5, Enter “Other Means”
101 Cell AK5, Enter “Cyberstrike”
102 Select Columns AH through AK, Right Click and change the Column Width to be 3
103 Cell AL5, Enter nothing (blank)
104 Select Column AL, Right Click and change the Column Width to be 0.2
105 Cell AM5, Enter “Score”
106 Cell AN5, Enter “Ranking”
107 Select Columns AM through AO, Right Click and change the Column Width to be 6
- 108 Cell C6, Enter “Professionalism”. **Bold this**
109 Group Cells C6 through I6 and click on Merge Cells. This centers the word across the section
110 Cell K6, Enter “Entry Methods”. **Bold this**
111 Group Cells K6 through O6 and click on Merge Cells
112 Cell Q6, Enter “Attack Methods”. **Bold this**
113 Group Cells Q6 through AK6 and click on Merge Cells
- 114 Cell Q7, Enter “Smaller Weapons”. **Bold this**
115 Group Cells Q7 through V7 and click on Merge Cells
116 Cell X7, Enter “Explosives/Incendiaries”. **Bold this**

- 117 Group Cells X7 through AF7 and click on Merge Cells
- 118 Cell AH7, Enter “Other”. **Bold this**
- 119 Group Cells AH7 through AK7 and click on Merge Cells
- 120 Cell AM7, Enter “Avg”. **Bold this**
- 121 Cell AN7, Enter “Rank”. **Bold this**
- 122 Copy Formatting (use the copy format paintbrush) from C44 to Cells C9 down to Cell AM13 (this fills the cells with the Green Color).
- 123 Repeat Step 122 above for Cells C15 down to Cell AM19
- 124 Repeat Step 122 above for Cells C21 down to Cell AM25
- 125 Repeat Step 122 above for Cells C27 down to Cell AM34
- 126 Repeat Step 122 above for Cells C36 down to Cell AM39
- 127 Repeat Step 122 above for Cells K40 through AK40
- 128 Select the Cells from C8 through AN8, Right Click>Format Cells>Patterns>Choose Light Gray Color
- 129 Repeat Step 127 above for Cells C14 through AN14
- 130 Repeat Step 127 above for Cells C20 through AN20
- 131 Repeat Step 127 above for Cells C26 through AN26
- 132 Repeat Step 127 above for Cells C35 through AN35
- 133
- 134 Cell AM9, Enter “=AVERAGE(C9:AK9)” (this will calculate the average of the subject cells). Do not panic if you get “#DIV/0!” this is because your Matrix is still not filled
- 135 Copy Cell AM9, Select Cells AM10 through AM13 and paste the formula
- 136 Repeat Step 134 above for Cells AM15 through AM19
- 137 Repeat Step 134 above for Cells AM21 through AM25
- 138 Repeat Step 134 above for Cells AM27 through AM34
- 139 Repeat Step 134 above for Cells AM36 through AM39
- 140 Cell K40, Enter “=AVERAGE(K9:K39)”
- 141 Copy Cell K40, Select Cells L40 through O40 and paste the formula
- 142 Repeat Step 140 above for Cells Q40 through V40
- 143 Repeat Step 140 above for Cells X40 through AF40
- 144 Repeat Step 140 above for Cells AH40 through AK40

Following this, populate the cells with appropriate estimates on a scale of 1 to 10. Then average the Score column and Rank the results in the Ranking column. I suggest using averaging of rows to create the score because it provides a relative view of the issues at hand for each row of each spreadsheet. As you build your own spreadsheets and begin to work with them, you may find that you prefer another formula for determining the score, but I have found that averaging is simple and results in consistently meaningful display of the relationships of the various rows. The spreadsheet can also be made much more useful if you apply Conditional Formatting to the Data and Score cells so that high scores color red, low scores color green, and medium cells color yellow. Conditional formatting is applied differently between various versions of Excel, so it is best to use the Help file or look up “Conditional Formatting Excel 2003” in Google. (Substitute your version of Excel if different.)

SUMMARY

Threats are at the core of probability. So threat analysis is at the core of probability analysis.

Threats versus hazards: Hazards can be either natural or man-made and are generally unintentional or without malice; threats are always man made and intentional and with malice.

A hazard is a precondition for an accident or a natural event having negative consequences including negligence. Hazards may include:

- Safety hazards
- Security hazards
- Natural disaster hazards
- Local or regional political or military hazards
- Negligent behavior

Hazards may be environmental or behavioral. Both can establish the preconditions for an unwanted consequence. Hazards may include safety hazards, security hazards, natural hazards, accidents, and can also include negligent behavior, which can result in injury, death, or property damage that can be very similar in result to a threat action.

Threats are all man-made. A threat actor is an individual or group that has the capability and intent to harm people or conduct an attack against a facility or organization or against exemplars of an opposing point of view. Threat actions can be either criminal or terroristic.

Without a threat actor, there is no risk. Analysts must identify potential threat actors and then decide (with ownership) which level of threat actor the security program should attempt to deter and which it should attempt to protect against. The first step is to understand who could be potential threat actors.

There are five kinds of potential threat actors:

1. Economic Criminals
2. Nonterrorist Violent Criminals
3. Subversives
4. Petty Criminals
5. Terrorists
 - There are five types of terrorists:
 - *Class I Terrorist:* The government-trained professional (including foreign intelligence threats)
 - *Class II Terrorist:* The religious extremist professional
 - *Class III Terrorist:* The radical revolutionary or quasi-religious extremist
 - *Class IV Terrorist:* Guerrilla/mercenary soldiers
 - *Class V Terrorist:* Amateur (civilian, untrained criminal, or militia-vigilante)
 - Economic criminals include:
 - Transnational criminal organizations
 - Organized crime
 - Sophisticated economic criminals
 - Unsophisticated economic criminals
 - Street criminals

- Nonterrorist violent criminals include:
 - Workplace violence threat actors
 - Angry visitors
 - Sexual criminals
 - Mugging/parking lot violence
 - Civil disorder event violence
 - Deranged persons
- Subversives include:
 - Cause-oriented subversives
 - Political and industrial spies
 - Saboteurs
 - Cults/dedicated activist groups
 - Hackers
 - Invasion of privacy threat actors
 - Persistent rule violators
- Petty criminals may include:
 - Vandals
 - Pickpockets
 - Prostitutes, pimps, and panderers
 - Disturbance causers

Another aspect of threat actors is how they may behave when their attack is interrupted or when met by a response force.

Design Basis Threat

Risk analysts must determine a design basis threat (DBT) that will be used as a baseline for the countermeasures. A DBT is the level of threat actor that the countermeasures should be able to address with reasonable effectiveness.

There are actually two DBTs. The first is the DBT that the security program will be designed to protect against, and the second is the DBT that the security program will be designed to deter and mitigate. This threat is known as an ordinary decent crime (ODC), or in other words, the kinds of challenges a security department is likely to encounter on a day-to-day basis. The second are those exceptional threats that a security department may encounter on an infrequent basis (or never, but that are within the realm of possibility and for which the consequences are so severe that planning and capabilities must be accommodated).

For example, one can deter against a terrorist attack in a commercial environment but it would be prohibitively costly to protect against one. However, an organization can mitigate some of the potential for damages of a terrorist attack.

However, an organization can do much to prevent ODC.* ODC includes economic crimes, nonterrorist violent crimes, subversive criminal acts, and petty crimes. These can all be addressed in a baseline security program.

* Sean O'Neill and David Lister, "MI5 given task of boosting intelligence on money-making," *TimesOnline* (London), February 25, 2005: "The IRA has never been a stranger to what people in Northern Ireland used to refer to as 'ordinary decent crime.'"

Terrorism and unique threats can be mitigated to the extent possible using *Special Countermeasures for Special Threats*.

Practice

One can effectively assess threats in four steps:

1. Identify potential threat actors.
2. Identify their motivation, capabilities, and history (thus their level of intent, skills, weapons, and tactics and what types of targets they have chosen in the past).
3. Develop a list of the organization's assets, and determine which of the weapons and tactics are most likely to be of use in attacking the organization.
4. Compare that data to information about the organization's assets to be protected, and determine which potential threat actors are likely to be most effective against the organization.

Tools

This book presents several software tools to assist in threat analysis:

1. *Adversary/Means Matrix*: The Adversary/Means matrix helps the analyst identify the types of weapons, entry methods, and attack scenarios that are used by various types of threat actors.
2. *Asset/Attack Matrix*: The Asset/Attack Matrix helps the analyst identify what types of weapons, entry methods, and attack scenarios would be most effective against the organization's various assets.
3. *Adversary Sequence Diagrams*: Identifies the path that adversaries must take to reach critical assets and possible exit paths.
4. *Asset/Threat Nexus Matrix*: Identifies where high-value individuals may encounter potential threat actors (think Robert Kennedy and Sirhan-Sirhan in the Hotel Ambassador kitchen or the celebrity CEO in the VIP parking entry).
5. *Asset/Weapons Nexus Matrix*: Identifies what types of weapons can be used in the areas identified by the Asset/Threat Nexus Matrix.

CHAPTER 8

Assessing Vulnerability

INTRODUCTION

At the completion of this chapter, you will be familiar with the Vulnerability Assessment Model, be able to define scenarios and evaluate specific consequences, learn how to use the Asset/Attack Matrix to determine which facility assets are subject to what kinds of attack scenarios, understand the Threat/Target Nexus Matrix that identifies where high-value individuals may possibly encounter potential threat actors within the facility, and also understand the Threat/Weapons Nexus Matrix that identifies which types of weapons can be used at the nexus points identified by the Threat/Target Nexus Matrix, the adversary sequence diagrams which evaluate how threat actors move in a facility, review how that affects the vulnerability assessment, and learn how surveillance affects vulnerability and how to assess surveillance opportunities. Finally, the chapter teaches how to develop matrices that help you assess all these factors that together comprise vulnerability (Figure 8.1).

REVIEW OF VULNERABILITY ASSESSMENT MODEL

Assessing vulnerability used to be easy when the threats were limited to *ordinary decent criminals*. The use of criminal vulnerability assessment in an environment of possible terrorism, however, is woefully inadequate. The method described in this chapter works equally well for both criminals and terrorists and is far more likely to uncover vulnerabilities that terrorists could easily exploit which would be completely unnoticed using criminal assessment methods alone.

- Define Scenarios and Evaluate Specific Consequences
- Evaluate the Effectiveness of Existing Security Measures
- Identify Vulnerabilities and Estimate the Degree of Vulnerability

Let me pause here to remind the reader that this is just one chapter out of this entire book which is dedicated to studying vulnerability. The topic deserves its own book, and in my opinion, Mary Lynn Garcia's (Sandia National Laboratories) is the penultimate book on vulnerability assessment.* I recommend that every reader of this book should own a copy.

* Mary Lynn Garcia, *Vulnerability Assessment of Physical Protection Systems* (Burlington, MA: Butterworth Heinemann, 2006).

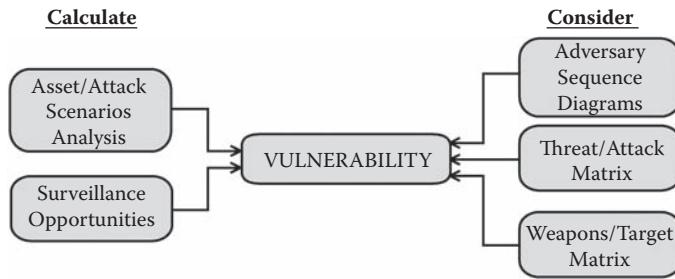


FIGURE 8.1 Vulnerability

DEFINE SCENARIOS AND EVALUATE SPECIFIC CONSEQUENCES

It is necessary to understand that to carry out an attack, whether criminal or terrorist, two things must happen in favor of the attacker. First, the attacker must be able to infiltrate the facility, and second, the attacker must be able to carry out a successful attack. For common criminals, a third factor is present — the ability to leave the facility (undetected if possible). All countermeasures for criminal and terrorism protection should be focused on reducing the probability of success of all of these objectives.

Assessing vulnerabilities for terrorism is more of a challenge than for common criminals. Because terrorist targeteers use simple methods and tactics (scenarios) in unique ways that ordinary people would not easily imagine, it is easy to overlook vulnerabilities in protection systems which a terrorist will easily see and exploit. The challenge then is to review not only vulnerabilities to criminal attacks but also those to existing and possible terrorist attacks. This takes imagination and a process that helps assure that all possible terrorist methodologies are considered.

This is easy to say, but how does one do that? The answer is to evaluate vulnerabilities the same way terrorists do. In evaluating the characteristics of targets of Al Qaeda, Salafist, Lashkar-e-Taiba (LeT), and other militant operatives and managers, including Khalid Sheikh Mohammed (KSM), it becomes clear how terrorist organizations conduct target selection, attack planning, scenario testing, and finally attack operations. Additional insight can be gained from the captured Al Qaeda 180-page manual titled “Military Studies in the Jihad against the Tyrants,” which was found by authorities in the home of an Al Qaeda supporter in Manchester, England, in 2000. This also confirms the KSM-Asset Target Value for Terrorism Model, by this author and as described in detail in this book.

Terrorism methods and tactics are a constantly evolving process but with a relatively stable agenda. As this book is being written, the attacks in Mumbai against the Taj Mahal Hotel, Oberoi, rail stations, and other locations were under way.

This attack is a lesson for all risk analysts everywhere who plan defenses for terrorist attacks. In an article in the *Times of India*, December 28, 2008, Rohan Gunaratna makes an excellent point:

Were the masterminds and perpetrators of the Mumbai carnage influenced by al-Qaida, the chief proponent of global jihad? In future, will sub-continental terrorists prefer to

attack the “crusader and Jewish” target set identified by the global jihadists as opposed to “Indian government and Hindu” targets? The Mumbai attack was unprecedented in target selection; of the five pre-designated targets. Was the target selection influenced by India’s alliance with the US and Israel? The method of operation was classic al-Qaida style — a coordinated, near simultaneous attack against high profile and symbolic targets aimed at inflicting mass casualties. The only difference was that it was a fidayeen* attack, a classic LeT modus operandi. ... groups ... that began with local agendas transformed into groups with regional and international agendas. ... Mumbai has demonstrated that the pre-eminent national security challenge facing both India and Pakistan is terrorism and not each other.

The lesson is clear. That terrorism is becoming a franchise in which the best-organized and best-trained organizations are becoming available to collaborate with less well-trained and imaginative organizations to enhance the overall capabilities of all terrorists everywhere.

The key elements in regional and international terrorism strategies include the following elements (author’s analysis). These elements have been used as a common strategic thread in many regions and countries including Afghanistan, India, Pakistan, Lebanon, Syria, Palestinian Territories, Israel, Indonesia, Thailand, Chechnya, Columbia, Guatemala, Egypt, Jordan, Saudi Arabia, Northern Ireland, and Great Britain. Expect to see them used in Mexico, the United States, and China as time goes forward.

- Create incidents that exploit common vulnerabilities, especially in civilian targets.
- Use the media to help the attackers during and after the attack, and prolong the attacks as long as possible in the media.
- Utilize synchronized attacks to amplify fear, and emphasize the organization and skills of the terrorists.
- Highlight the ineptitude of local police and counterterrorism forces to protect the populace.
- Encourage governments to take repressive measures that will inevitably include innocent members of the public in their efforts to find and suppress terrorism.
- Incite the populace to retaliation, especially during election cycles.
- Destabilize the government.
- Encourage the ascent of militant political parties to power.
- Involve elements of neighboring countries where possible.
- Create conditions for international armed conflict between countries.
- Destabilize any weak regime whose country could be used as a platform for terrorism training and operations.
- Overthrow governments that are friendly to Western governments.
- Keep up the pressure until the above results are achieved.
- Use a strategy of attack, retreat, regroup, attack, retreat, regroup, never faltering from the long-term goals of overthrowing governments friendly to the West.
- Finally, establish Sharia Law Caliphates in place of existing governments in all Muslim countries and in as many other countries as possible.

* Fidayeen: A suicide tactic used by terrorists.

This strategy has been identified by the terrorists, and its footprints can be seen in all the countries identified above.

So, we get back to the core of antiterrorism vulnerability assessment, which is to identify possible threat scenarios and consequences. One of the major weaknesses of most security vulnerability books is that they do not address this important issue. Throughout my career, I have read numerous books that talk about facility penetration; rings of protection; checking windows, shrubs, fences, and so forth, but they do not focus on what kinds of attacks can actually occur. This has resulted in a phenomenon that is almost unique to the United States — that is, facilities that are robustly protected at their points of entrance and which are highly vulnerable almost everywhere else. For example, it is common in the United States to see high-risk facilities that have a single chain-link fence around the facility. In other countries, one would see a double fence with detection between. Western risk analysts generally perceive a psychological barrier as a real barrier. That is, that a chain-link fence or window or gypsum wall is a barrier. These are not barriers but in fact create only momentary inconveniences in the progress of an attacker.

An effective process of Vulnerability Assessment must include the following steps:

- Utilize an Asset/Attack Matrix that identifies which attack scenarios are most likely to be used by what class of threat actors.
- Utilize a Threat/Target Nexus Matrix that identifies what areas are most likely to be used by threat actors to carry out their action.
- Utilize a Weapons/Target Nexus Matrix that identifies types of weapons that are most likely to be used at each threat/target location.
- Review surveillance opportunities for each major asset under consideration.
- Assemble vulnerabilities in light of all of the information above.

Asset / Attack Matrix

An Asset/Attack Matrix identifies which attack scenarios are most likely to be used by what class of threat actors (see Figure 8.2). This matrix has two dimensions: assets and threat scenarios. Like every other matrix discussed in this book, this matrix can be developed in a professional program such as SVA-Pro or by using a spreadsheet program like Microsoft Excel. There are two steps to developing the Asset/Attack Matrix. The first is the list of major assets that were developed in Chapter 5, “Asset Characterization and Identification.” The second is a list of possible threat scenarios which was developed in Chapter 7, “Threat Analysis” (the Adversary/Means Matrix).

This is a good time to review the threat scenarios listed in the threat analysis section to be sure that they are inclusive of every type of attack. For example, many threat scenario lists did not include “moving shooter” attacks before the Mumbai attacks on the Taj and Oberoi hotels in 2008. This type of attack is different than other types of ballistic attacks in that the shooter is not stationary but moves throughout the facility, attacking victims as he moves and taking up sniping positions to attack forces assembling outside, then moving on to a new location in the building. In the Mumbai attacks, the shooters moved zigzag up in the building to the top floors, taking casualties as they went. There are effective countermeasures for this attack scenario, but they are different than for any other type of scenarios and involve deploying barriers within the building that limit the movement of the shooter and contain him to an area where he can be easily taken out by the Special Forces team. This countermeasure also limits casualties to only the area

Mega Towers		Asset/Attack Matrix																					
		Targets		Entry Methods			Weapons			Intermediaries and Explosives			Attach Scenarios			Other			Rank				
		People	6	6	3	3	4	3	7	8	8	8	8	9	8	8	8	7	7	7	6	7	2
	VIP Executives and VIP Visitors	2	2	5	5	7	6	6	6	10	8	8	8	7	10	10	10	10	10	10	8	8	4
	Employees	8	8	6	6	6	6	5	10	10	10	10	10	10	10	10	10	10	10	10	8	9	1
	Contractors	6	6	2	2	5	5	5	7	7	7	7	7	7	7	7	7	7	7	7	7	6	39
	Visitors	6	6	1	2	2	1	3	8	8	8	8	8	8	8	8	8	8	8	8	8	7	23
	Delivery Personnel	8	8	1	1	1	1	1	6	8	6	7	8	6	6	6	6	4	4	3	4	4	51
	Transportation Personnel	8	1	1	1	1	1	1	7	7	6	6	6	6	6	6	6	4	4	3	5	6	50
Tools																							
Cutting Torch/Burnishing Bar																							
False Credentials																							
Property		6	6	3	5	6	8	5	7	9	10	9	10	8	10	10	8	8	4	4	7	8	1
Site		5	5	3	4	6	7	4	4	8	10	7	10	10	10	10	4	4	9	9	8	3	7
Employee Drop-Off		3	3	1	6	8	8	8	8	8	10	8	10	10	10	10	8	8	8	7	7	5	10
Employee Drop-Off		3	3	1	6	8	8	8	8	8	10	8	10	10	10	10	8	8	8	7	10	1	8
Visitor Drop-Off — Hotel (South)		2	2	1	6	6	6	8	8	10	7	10	10	10	10	10	8	8	8	8	7	7	12
Main South Entry Gatehouse Area		2	2	8	8	6	6	8	8	10	7	10	10	10	10	10	8	8	8	8	7	5	8
North Perimeter Fence		8	8	1	1	6	7	2	2	8	10	8	10	5	10	10	1	1	10	10	8	1	1
East Perimeter Fence		8	8	1	1	6	7	2	2	8	10	8	10	5	10	10	1	1	10	10	8	1	1
South Perimeter Fence		8	8	1	1	6	7	2	2	8	10	8	10	5	10	10	1	1	10	10	8	1	1

FIGURE 8.2 Asset/Attack Matrix

of containment. Threat scenarios must be constantly updated to keep up with current attack models.

With assets in rows from the left and threat scenarios in columns to the right, the analyst can estimate the severity of a given attack scenario on the organization's key assets. For example, attacks on people have less effect on the information technology system but can have a dramatic effect on the organization's business reputation.

Threat / Target Nexus Matrix

The Threat/Target Nexus Matrix (Circulation Path/Threat Nexus Matrix) identifies what areas are most likely to be used by threat actors to carry out their action (Figure 8.3).

The Threat/Target Nexus Matrix can be developed either in a professional program such as SVA-Pro or by using a spreadsheet program such as Microsoft Excel. The example herein uses Microsoft Excel, which anyone can use to develop a suitable matrix.

The Threat/Target Nexus Matrix creates a link between areas and possible targets (people who might be targets for a terrorist attack). This uses a different list than the asset-driven matrices such as the Asset/Attack Matrix. In the case of the Threat/Target Nexus Matrix, we want to examine vehicle and pedestrian circulation paths against possible victims.

Different targets (possible victims) and different types of attackers will use different areas, and it is where these areas cross paths that attacks may occur. For example, VIPs will almost always enter through a VIP entry, if one is provided. So the approach by vehicle and pedestrians to the VIP entry area is a critical nexus point for attacks on VIPs.

FIGURE 8.3 Threat/Target Nexus Matrix

VIPs circulate through a building in different ways than normal visitors. The attack on Robert Kennedy in the kitchen area of the Los Angeles Ambassador Hotel is an example of how Sirhan Sirhan understood VIP circulation paths and took advantage of such to isolate his target from the mass of public admirers and corner him into a more vulnerable space. Similarly, the attack by Jack Ruby on Lee Harvey Oswald used circulation path knowledge to create an opportunity to get close to his target. Examples abound. The attack on Rafic Al Hariri in February 2005 in Beirut, Lebanon, illustrated the attackers' foreknowledge of his transportation habits. Most kidnappings happen at locations selected for their characteristics of isolating the victim from movement options. The better the risk analyst understands how circulation paths play an important role in target acquisition, the better the analyst can identify and assess circulation paths for determining where attacks might take place.

One project I worked on involved a “red carpet” area. This is an obvious nexus point for terrorists wishing to cause large numbers of public casualties in the full eye of the media.

The main lobby of buildings, the employee entrance, food circulation paths, housekeeping paths, and delivery paths create opportunities for threat actors to exploit crossing paths with potential victims. Once a victimology profile is understood (what types of victims designated threat actors prefer), a risk analyst can easily understand the areas of a facility that present targets to potential attackers.

Weapons / Target Nexus Matrix

The Weapons/Target Nexus Matrix (Circulation Path/Weapons Nexus Matrix) identifies types of weapons that are most likely to be used at each threat/target location (Figure 8.4).

The Weapons/Target Nexus Matrix can be developed either in a professional program such as SVA-Pro or by using a spreadsheet program such as Microsoft Excel. The example herein uses Microsoft Excel, which anyone can use to develop a suitable matrix.

Similar to the Threat/Target Nexus Matrix, the Weapons/Target Nexus helps the risk analyst understand what types of weapons can be useful to potential threat actors at each of the circulation path nexus points that were identified from the Threat/Target Nexus Matrix.

Not all weapons can be used in all locations. For example, rocket-propelled grenades (RPGs) would have been less useful to the Mumbai moving shooter threat actors than the small arms they carried, because RPGs need distance to work. However, hand grenades are highly useful within a building to clear a room from defenses or to kill victims in a single stroke, especially if they might be armed.

The closer the proximity of the threat actor to the potential victim, the smaller will be the preferred weapon. An AK-47 would have been useless in the Robert Kennedy assassination because it would have identified the attacker as such before he could use the weapon. He chose instead a handgun that was easy to conceal until needed.

In the Columbine High School attack, the threat actors chose propane bombs, which, had they detonated properly, would have caused casualties in the hundreds. Such bombs, though ideal for creating casualties, also created problems in transportation to the attack site, slowing down the attackers and giving some warning to their potential victims. Similarly, the Columbine attacker Eric David Harris kept a journal

Hotel and Convention Center Circulation Paths and Weapons Nexus Points																				
	Tools	False Credentials	Social Engineering	Vehicles	Forced Entry	Small Arms	Heavy Arms	Shoulder-Fired Weapons	Mortars	Hand Grenades	Improvised Incendiary Devices	Improvised Explosive Device	Conventional Bomb	Vehicle Bombs	Dirty Bomb	Suicide Bomber	Chemical Agents	Biological Agents	Other Means	Cyberstrike
PATHS/WEAPONS	Entry Methods									Attack Methods										
										Smaller Weapons			Explosives			Other				
Site																				
VIP Entry Areas	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Employee Entry Areas	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Public			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Transportation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Basements																				
VIP Parking	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	
Public Parking			X	X	X	X				X	X	X	X	X	X	X	X	X	X	
Loading Docks	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X	
Convention Center																				
Retail Circulation			X	X	X	X				X	X	X	X	X	X	X	X	X	X	
Exhibition/Convention Circulation	X	X		X	X	X				X	X	X	X	X	X	X	X	X	X	
Employee Circulation	X	X		X	X	X				X	X	X	X	X	X	X	X	X	X	
Service Areas	X	X		X	X	X				X	X	X	X	X	X	X	X	X	X	
Food Service Circulation	X	X		X	X	X	X			X	X	X	X	X	X	X	X	X	X	
Roof Deck																				
Roof Deck	X	X		X	X					X						X	X	X	X	

Legend

X	Likely Intersection
*	Possible Intersection
■	Intersection with High Risk
■■	Intersection with Medium Risk
■■■	Lower Risk

FIGURE 8.4 Weapons/Target Nexus Matrix

that identified “good hiding places” and areas with poor lighting that could be utilized. The attack was to start at exactly 11:17 A.M., when Harris had calculated the largest possible number of students would be located in the cafeteria.* The lesson here is that it is not only where, but also when opportunities for contact between threat actors and victims arise.

The Weapons/Target Nexus should illustrate what types of weapons the risk analyst should be concerned about in each of the areas considered. This will also limit the number or probable threat scenarios for these areas.

Adversary Sequence Diagram Path Analysis†

The Adversary Sequence Diagram (ASD) Path Analysis (also see this described in detail in Chapter 7, “Threat Analysis”) identifies the pathways from perimeter to target that potential attackers might follow on their way to the target (Figure 8.5).

* http://en.wikipedia.org/wiki/Eric_Harris_and_Dylan_Klebold.

† This is explored in detail in Mary Lynn Garcia’s book, *Vulnerability Assessment of Physical Protection Systems* (Burlington, MA: Butterworth Heinemann, 2006).

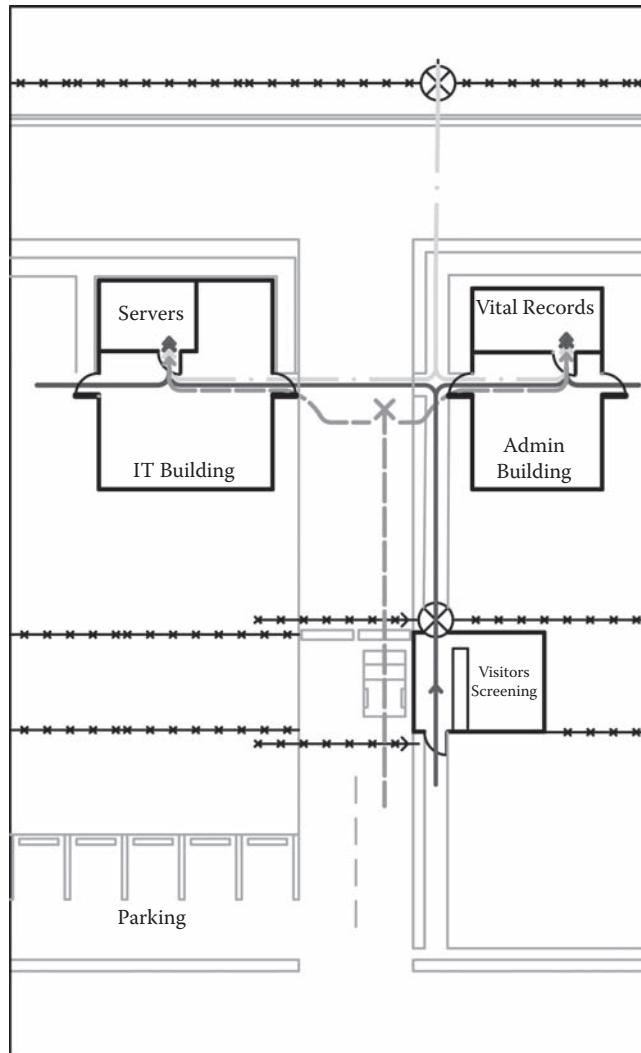


FIGURE 8.5 Adversary Sequence Diagram (ASD)

The ASD Path Analysis can be conducted in either of two ways:

1. Flowchart
2. Graph

To prepare an Adversary Sequence Diagram Path Analysis, one must first identify the locations of all high-value assets within the buildings. Then one should examine all of the entries to the facility, including frontal, side, and rear perimeter entries; underground (utility) entries and overhead entries from adjacent buildings; helicopter fast rope entries; and so forth. Once inside the perimeter, the analyst should evaluate all pathways into the buildings where high-value assets are located. The diagrams should illustrate progressively

the nexus between the locations of high-value assets to the building perimeter entries until all logical pathways are resolved. Finally, the analyst should identify the locations along those pathways where detection, assessment, and delays can be placed.

Surveillance Opportunities Matrix

The Surveillance Opportunities Matrix identifies surveillance opportunities (Figure 8.6). The Surveillance Opportunities Matrix can be developed either in a professional program such as SVA-Pro or by using a spreadsheet program such as Microsoft Excel. The example herein uses Microsoft Excel, which anyone can use to develop a suitable matrix.

Before any terrorist attack or criminal attack is carried out, it is necessary for the attacker to perform some kind of surveillance. This is necessary so that the threat actor can understand what assets there may be to attack, understand what vulnerabilities can be exploited, gain advantage to control the area, obtain cover and concealment while approaching and withdrawing, and all other elements necessary to succeed in the attack.

Whether the intended act is criminal or terrorist, surveillance is required. The more importance success is to the mission and the more complicated the attack location, the more important surveillance is to the operation.

The task of surveillance is also the best opportunity any organization has to prevent an attack that is in the planning stage. Surveillance is a task like any other task. As such, there are certain steps that must be carried out that can identify the act of surveillance.

A threat actor surveilling a potential target is looking for different things than anyone else, except possibly for a risk analyst. Both the surveillant and the risk analyst are looking for vulnerabilities that can be exploited. I have actually been stopped by an astute security manager in an airport because my actions fit the description of surveillance. After showing the security manager my credentials, he understood that my tendency to notice security provisions was industry based and not out of interest of surveillance for planning an attack.

Surveillance has many possible components, only some of which may be used in support of planning an attack. These may include:

- Fixed-visual surveillance
- Mobile vehicular surveillance
- Mobile pedestrian surveillance
- Acoustic eavesdropping
- Electronic surveillance
- Information technology surveillance (multiple modes)
- Interception of information or documents

Using the asset list developed in Chapter 5, “Asset Characterization and Identification,” the risk analyst will develop a spreadsheet identifying the list of assets by rows on the left (broken out by asset class — people, property, proprietary information, and business reputation), and surveillance types by columns, including those identified above, as appropriate.

This matrix will allow the risk analyst to determine what assets are prone to what types of surveillance, and can help the analyst rank those assets most vulnerable to surveillance. The results of this matrix are components for asset target values and risk calculations.

		Surveillance Opportunities Matrix						
		Surveillance Opportunities Matrix						
		Surveillance Opportunities Matrix						
Targets		People	4	3	4	6	6	1
VIP Executives and VIP Visitors		VIP	6	2	4	6	5	39
Employees		Employees	7	7	7	7	7	6
Contractors		Contractors	7	3	5	5	6	23
Visitors		Visitors	7	7	4	3	6	20
Delivery Personnel		Delivery Personnel	10	2	2	2	5	33
Transportation Personnel		Transportation Personnel	10	2	2	7	5	33
Property		Property	8	7	5	2	5	3
Site		Site	9	8	6	3	6	16
VIP Drop-Off		VIP Drop-Off	10	10	2	6	7	8
Employee Drop-Off		Employee Drop-Off	10	8	8	6	6	3
Visitor Drop-Off — Hotel (South)		Visitor Drop-Off — Hotel (South)	10	8	8	3	1	14
Main South Entry Gatehouse Area		Main South Entry Gatehouse Area	10	8	2	7	1	6
North Perimeter Fence		North Perimeter Fence	8	8	6	7	1	23
East Perimeter Fence		East Perimeter Fence	8	8	6	7	1	27
South Perimeter Fence		South Perimeter Fence	8	8	6	7	1	27

FIGURE 8.6 Surveillance Opportunities Matrix

EVALUATE VULNERABILITY

Determining the effectiveness of existing security measures is done differently for existing and new facilities. For existing facilities, a security survey is required. As this is not possible for new facilities, a vulnerability estimate can be made from architectural drawings and renderings.

For new facilities, the process includes the following steps, described in detail below.

- Determine surveillance opportunities
- Determine accessibility
- Identify intrinsic vulnerabilities
- Natural countermeasures
- Physical countermeasures
- Electronic countermeasures
- Operational countermeasures

For existing facilities, a full vulnerability survey is recommended. A vulnerability survey should include the following elements:

- Determine the physical nature of the facility (campus, building, perimeter, etc.).
- Determine the operational nature of the facility (hospital, factory, office building, military base, etc.).
- Determine the functional operating elements of the facility (administration, human resources, marketing, research and development, etc. — list all).
- Determine the distribution of the functional operating elements throughout the facility (marketing — fourth floor, human resources — fifth floor, executive offices — sixth floor, etc.).
- Determine the number and type of people who are distributed through the functional operating elements (employees — all floors, managers — all floors, executives — sixth floor and executive lift, delivery personnel — loading dock and mail room, visitors — lobby, ground floor conference rooms, and executive floor, etc.).
- Then review the facility as described above for new facilities. For existing facilities, this can best be done by a comprehensive walk-about with a knowledgeable security representative. A combination of a security manager and a security supervisor is recommended. The security manager will help to maintain a strategic focus, and the supervisor is more likely to be familiar with the intimate details of the facility.

Survey Points

The commitment of management to the mission of the security organization should be noted. From there, the survey involves observing, questioning, verifying, investigating, and evaluating. Every survey should begin with field interviews of key management, including security management. The history of security events should be available and will be used in the identification of and estimates of the significance of various threat scenarios. Obtain organization charts, a functional description of each business unit, along

with its location in the facility, any satellite activities of the organization, and any outside services that are critical to the organization.

Obtain access to information as to the flow of information in the organization, on paper, financial and through the information technology system. Maintain focus on the problems outlined by management in the opening interviews, as these will be front and center in its mind for the report. Ask about and focus on procedures that have been put in place to deal with problems. Ask if these procedures have largely resolved the problems, or what concerns still exist.

Make a flowchart of the business operations in terms of flow of products, information, money, financial records, and services.

The resulting information can be entered into the vulnerability matrix as described below for quantitative analysis.

From there, the analysis process is the same for existing and new, as described below.

Quantitative Analysis Matrices

Consider surveillance opportunities as described above.

Determine Accessibility

Accessibility is the key to any threat action. Inaccessible assets are safe from attackers. The degree of accessibility is a direct and most important function of vulnerability. No access equals no attack. More access equals a higher opportunity for an attack.

For some types of attacks, any access will do. The assassination of former Pakistani Prime Minister Benazir Bhutto is an example of this. All the attacker needed was a 10-meter proximity to Madam Bhutto in the midst of a large crowd. Suicide bombers need only approximate access. Leave-behind backpack bombs need only access to a crowd. A roadside bomber will place the bomb, wait for an appropriate target to pass by, and then trigger his attack.

For most targeting, a direct line of sight is required for ballistic attacks, RPG attacks, and the like. The more accessible a potential target is, the more easily an attack is carried out. Access equals possibility. More access equals more probability.

Identify Intrinsic Vulnerabilities

Intrinsic vulnerabilities are important to understand and are often overlooked. They are so intuitive that they are most often not considered as a component factor, but only as part of an aggregate of intrinsic vulnerability and other countermeasures. This is important to understand because the environment can change, and when it does, so does the vulnerability equation.

Intrinsic vulnerabilities are those vulnerabilities that an asset has in the absence of any other countermeasures. That is, if the asset is sitting in an open field with no building or other protection, what kinds of attacks can be carried out against it? Different assets have different intrinsic vulnerabilities.

For example, people are subject to ballistic attacks, bombs, fire, and armed robberies, but paper files are less vulnerable to ballistic attacks, but still vulnerable to bombs,

fires, and burglaries (it is rare for an armed robbery to occur for which the target is a file). Cyber attacks do not directly attack people or property but are targeted against the Information Technology system. Each asset should be scored for its intrinsic vulnerability on a scale of 1 to 5 or 1 to 10.

Natural Countermeasures

After consideration of intrinsic vulnerabilities, we begin to consider the effect that natural countermeasures have on the vulnerability. Examples of natural countermeasures include the following:

- A liquefied natural gas (LNG) terminal that is surrounded on the land side with a storm berm (a 21-foot, 7-meter-high raised levy to keep hurricane storm surges out) also has a natural countermeasure against the entry of conventional vehicles.
- A facility on a small island with only ferry access makes access and getaway more difficult as it creates a “choke point” through which all threat actors must come and go.
- Any facility located on a waterway is only accessible by watercraft on that side.
- A facility located on a hillside cliff has very limited access from that side.

Most often, natural countermeasures affect access to assets. The deterrent or access attributes of natural countermeasures should be subtracted from the asset’s intrinsic vulnerability.

Evaluate Effectiveness of Existing Security Measures

Existing man-made security countermeasures also limit vulnerability. Man-made countermeasures should also be subtracted from the intrinsic vulnerabilities. Man-made countermeasures may include:

- Physical countermeasures
- Electronic countermeasures
- Operational countermeasures

Sometimes man-made countermeasures overlap natural countermeasures, and sometimes they complement each other. For example, a fence on top of the LNG terminal storm berm will not serve to keep out any vehicles that cannot themselves climb the storm berm. The mitigating effect of the fence on vehicle access is negligible. However, the limiting effect on pedestrians may be significant because they can climb the storm berm more easily than can a vehicle.

There are three types of man-made countermeasures:

1. *Physical Countermeasures:* Physical countermeasures include locks, doors, gates, lighting, signage, fences, walls, and fixed and deployable barriers.
2. *Electronic Countermeasures:* Electronic countermeasures include alarm systems; access control systems; video systems; and communications systems including electronic signage, telephones, public address systems, and two-way radios. Electronic countermeasures can also include long-range acoustic weaponry,

visible light weaponry, electronic jamming equipment, and information technology threat countermeasures.

3. *Operational Countermeasures:* Operational countermeasures include all uses of security staffing (posts, patrols, reserve staff), security dogs, security policies and procedures, countersurveillance programs, investigations, and security intelligence programs.

All of these should be subtracted from intrinsic vulnerabilities, paying attention to the overlapping and complementary effects of countermeasures on the same asset.

The Vulnerability Calculation Spreadsheet

The vulnerability calculation is based upon the threat scenarios and identifies the most likely locations for attacks by reviewing both the Threat/Target Nexus locations and the Weapons/Target Nexus locations. Once we know what types of threat actions can occur and the most likely locations for each of these, we can focus on the vulnerabilities of not only the entire facility, but especially the most likely locations for attacks of each type by each type of threat actor. This level of granularity and accuracy is considered unobtainable by many security analysts, but we will review exactly how to achieve it.

The vulnerability calculation spreadsheet adds surveillance and intrinsic vulnerability and subtracts the mitigating effects of natural and man-made countermeasures, including physical, electronic, and operational countermeasures.

Create a new spreadsheet tab using the Asset/Consequences spreadsheet as a basis. Name the spreadsheet tab Vulnerability Calculations. Include the following columns:

- List of Targets (Assets)
- Access Opportunities
- Surveillance Opportunities (referenced from the Surveillance Opportunities Matrix)
- Intrinsic Vulnerability
- Existing Natural Countermeasures
- Existing Man-Made Countermeasures
 - Hi-Tech
 - Lo-Tech
 - No-Tech

Add Surveillance, Access, and Intrinsic Vulnerability (each from 1 to 10). Subtract Existing, Hi-Tech, Lo-Tech, and No-Tech countermeasures (each from 1 to 10). The result is the vulnerability of each asset from 1 to 10 (Figure 8.7).

Qualitative Analysis Section

Following the interviews, records gathering, survey, and quantitative analysis, it is important to condense the information into a qualitative analysis. Quantitative analysis information is easily reduced by stepping through the process and noting significant elements of each step, including significant information from the interview, records, survey, and

Mega Towers Vulnerability Matrix										
Targets										
	Accessibility	Surveillance	Intrinsic Vulnerability	Natural Countermeasures	Physical Measures	Electronic Measures	Operational Measures	Score	Rank	
People	8	7	3	8	3	1	6	5	3	
VIP Executives and VIP Visitors	5	2	1	7	6	1	8	4	44	
Employees	8	10	4	10	5	1	8	7	18	
Contractors	8	3	4	5	5	1	3	4	51	
Visitors	8	10	4	10	1	1	8	6	22	
Delivery Personnel	8	7	2	8	1	1	3	4	44	
Transportation Personnel	8	7	2	8	1	1	3	4	44	
Property	8	7	5	7	6	5	4	6	1	
Site	8	8	6	6	5	5	4	6	24	
VIP Drop-Off	7	6	6	8	5	5	5	6	22	
Employee Drop-Off	10	0	7	10	7	8	7	8	2	
Visitor Drop-Off — Hotel (South)	10	10	7	10	8	8	7	9	1	
Main South Entry Gatehouse Area	8	8	7	10	8	8	7	8	4	
North Perimeter Fence	8	8	4	2	3	3	2	4	44	
East Perimeter Fence	8	8	4	2	3	3	2	4	44	
South Perimeter Fence	8	8	4	2	3	3	2	4	44	
West Perimeter Fence	8	8	4	2	3	3	2	4	44	
North Perimeter Freight Gate	8	8	4	6	5	3	2	5	35	
East Perimeter Emergency Gate	8	6	6	6	5	3	2	5	35	
West Perimeter Emergency Gate	8	6	6	6	5	3	2	5	35	
Hotel Loading Dock Area	7	8	6	6	4	3	2	5	35	
Hotel East Entrance	7	8	7	10		8	7	8	5	
Hotel West Entrance	7	8	7	10		8	7	8	5	
Ramp down to Underground Parking	7	3	4	6	4	3	3	6	5	
<i>Underground Structure</i>	7	7	5	8	4	3	3	5	34	
P1 Level Parking	7	7	6	8	4	3	3	5	27	
P1 Level Elevator Lobby	7	7	5	8	4	3	3	5	30	
P2 Level Parking	7	7	6	8	4	3	3	5	27	
P2 Level Elevator Lobby	7	7	5	8	4	3	3	5	30	
P3 Level Parking	7	7	6	8	4	3	3	5	27	
P3 Level Elevator Lobby	7	7	5	8	4	3	3	5	30	
P3 Level Utility Rooms	6	6	3	8	4	3	3	5	41	
<i>Hotel Tower</i>	9	6	5	8	6	5	7	17		
Main Lobby Area	10	10	6	8	8	6	6	8	7	
Lobby Level Reception Desk	10	7	6	10	10	10	6	8	2	
Lobby Level Bell Desk and Storage	8	6	6	8	8	6	6	7	14	
Security Checkpoint Outside	10	7	3	4	3	3	3	5	41	
Lobby Level Concierge Area	10	6	3	8	8	8	8	7	13	
Passenger Elevator Lobby	10	6	6	8	8	8	6	7	9	
Stairwells	10	5	3	8	8	8	6	7	14	
Freight Elevator	7	3	3	8	8	6	4	6	25	
Lobby Level Utility Rooms	7	2	3	8	8	3	3	5	40	
Low-Rise Levels	10	7	7	8	8	6	6	7	9	
Mid-Rise Levels	10	7	7	8	8	6	6	7	9	
Hi-Rise Levels	10	7	7	8	8	6	6	7	9	
Passenger Elevator Lobbies	10	7	4	8	8	8	8	8	8	
Freight Elevator Lobbies	7	5	4	8	8	3	4	6	25	
Utility Rooms	8	4	3	8	8	3	3	5	30	
Mechanical Floor	7	4	3	8	8	3	3	5	35	
Roof	6	6	7	8	7	6	6	7	18	
<i>Proprietary Information</i>	6	6	5	6	7	3	7	5	2	
IT System	8	8	3	10	10	1	6	7	18	
Security System	8	8	7	6	10	1	8	7	14	
RF Communications System	7	7	7	5	5	6	7	6	21	
Paper Files	1	1	1	1	1	4	5	2	52	
<i>Business Reputation</i>	2	6	2	2	2	6	5	4	4	
Legend										
Major Effect										
Medium Effect										
Minimal Effect										

FIGURE 8.7 Vulnerability Matrix

quantitative analysis. This is just a process of putting raw data into words, formatted in a fashion that flows logically.

Vulnerability Detail Spreadsheet

Finally, the risk analyst should create a comprehensive list from the vulnerability calculations for every vulnerability to be addressed. This is quite straightforward, and its value will become apparent when we proceed to Chapter 18, “Security Effectiveness Metrics.” Begin with the list of assets that have been broken down into asset categories (people, property, proprietary information, and business reputation), and of course those have been broken down into subcategories (Property > sub-Perimeter > sub-North Perimeter, East Perimeter, South Perimeter, West Perimeter, Perimeter Entries > sub-Main Public Entry, Service Entry, Employee Entry, VIP Entry, etc.; Main Building > sub-Ground Floor > sub-Main Entry, Lobby, Elevator Lobby, etc.). Now in a spreadsheet as described above, with assets listed in rows to the left, list the vulnerabilities found for each asset row in a new column next to the asset.

Vulnerability Detail Matrix

The Vulnerability Detail Matrix identifies possible vulnerabilities (Figure 8.8). The Vulnerability Matrix can be developed either in a professional program such as SVA-Pro or by using a spreadsheet program such as Microsoft Excel. The example herein uses Microsoft Excel, which anyone can use to develop a suitable matrix.

Additionally, between the asset listing and the vulnerability listing, create two new columns labeled Infiltration Vulnerability or Attack Vulnerability. Classify the vulnerability appropriately in one or the other, or both with an “X”.

Finally, be sure to include columns for criticality and consequence ranking.

Now, you should have a spreadsheet that lists the following by columns:

- Assets by General Classes
- Subclasses of Assets under Each General Class
- Criticality Ranking for Each Asset (from the Consequences Matrix)
- Consequence Ranking for Each Asset (from the Consequences Matrix)
- Infiltration/Attack Vulnerability Columns
- The Vulnerability Ranking from the Vulnerability Matrix
- A Written Description of the Vulnerability

This matrix will be used as the basis for the Countermeasures Effectiveness Matrix in Chapter 18 and for the Cost-Effectiveness Matrix in Chapter 19.

SUMMARY

Review of the Vulnerability Assessment Model

Assessing vulnerability used to be easy when the threats were limited to *ordinary decent criminals*. The use of criminal vulnerability assessment in an environment of possible terrorism, however, is woefully inadequate. The short version of a quality vulnerability assessment model includes the following:

		Vulnerability Matrix								
		Mega Towers								
		Targets								
		People	Property	Site	Accessibility	Surveillance	Natural Countermeasures	Physical Countermeasures	Electronic Measures	Operational Measures
		8	7	5	3	8	3	1	6	5
		VIP Executives and VIP Visitors	VIP Drop-Off	Employee Drop-Off	Employee Drop-Off — Hotel (South)	Visitor Drop-Off — Hotel (South)	Main South Entry Gatehouse Area	North Perimeter Fence	East Perimeter Fence	South Perimeter Fence
		5	8	7	10	7	10	8	8	8
		Employees	Employees	Contractors	Contractors	Visitors	Delivery Personnel	Transportation Personnel		
		8	10	3	4	10	5	5	1	1
		Contractors	Contractors	Visitors	Visitors	Delivery Personnel	Transportation Personnel			
		8	10	4	4	10	8	1	1	1
		Visitors	Visitors	Delivery Personnel	Delivery Personnel	Transportation Personnel				
		8	7	7	2	8	1	1	3	4
		Delivery Personnel	Delivery Personnel	Transportation Personnel						
		8	7	7	2	8	1	1	3	4
		Transportation Personnel								

- Define scenarios and evaluate specific consequences.
- Evaluate the effectiveness of existing security measures.
- Identify vulnerabilities, and estimate the degree of vulnerability.

Define Scenarios and Evaluate Specific Consequences

In interviews and interrogations with Al Qaeda, Salafist, Lashkar-e-Taiba (LeT), and other militant operatives and managers including Khalid Sheikh Mohammed (KSM), it becomes clear how terrorist organizations conduct target selection, attack planning, scenario testing, and finally, attack operations.

An effective process of vulnerability assessment must include the following steps:

- Utilize an Asset/Attack Matrix that identifies which attack scenarios are most likely to be used by what class of threat actors.
- Utilize a Threat/Target Nexus Matrix that identifies what areas are most likely to be used by threat actors to carry out their action.
- Utilize a Weapons/Target Nexus Matrix that identifies types of weapons that are most likely to be used at each threat/target location.
- Review surveillance opportunities for each major asset under consideration.
- Review vulnerabilities in light of all of the information above.

Surveillance has many possible components, only some of which may be used in support of planning an attack. These may include:

- Fixed visual surveillance
- Mobile vehicular surveillance
- Mobile pedestrian surveillance
- Acoustic eavesdropping
- Electronic surveillance
- Information technology surveillance (multiple modes)
- Interception of information or documents

Evaluate Vulnerability

Determining the effectiveness of existing security measures is done differently for existing and new facilities. A security survey is required for existing facilities, but for new facilities a vulnerability estimate can be made from architectural drawings and renderings.

For new facilities, the process includes the following steps.

- Determine accessibility
- Identify intrinsic vulnerabilities
- Natural countermeasures
- Physical countermeasures
- Electronic countermeasures
- Operational countermeasures

For existing facilities, a full vulnerability survey is recommended. A vulnerability survey should include the following elements:

- Determine the physical nature of the facility (campus, building, perimeter, etc.).
- Determine the operational nature of the facility (hospital, factory, office building, military base, etc.).
- Determine the functional operating elements of the facility (administration, human resources, marketing, research and development, etc. — list all).
- Determine the distribution of the functional operating elements throughout the facility (marketing — fourth floor, human resources — fifth floor, executive offices — sixth floor, etc.).
- Determine the number and type of people who are distributed through the functional operating elements (employees — all floors, managers — all floors, executives — sixth floor and executive lift, delivery personnel — loading dock and mail room, visitors — lobby, ground floor conference rooms and executive floor, etc.).
- Then review the facility as described above for new facilities. For existing facilities, this can best be done by a comprehensive walk-about with a knowledgeable security representative. A combination of a security manager and a security supervisor is recommended. The security manager will help to maintain a strategic focus, and the supervisor is more likely to be familiar with the intimate details of the facility.

The Vulnerability Calculation

The vulnerability calculation adds surveillance and intrinsic vulnerability and subtracts the mitigating effects of natural and man-made countermeasures, including physical, electronic, and operational countermeasures.

Qualitative Analysis Section

Following the interviews, records gathering, surveys, and quantitative analysis, it is important to condense the information into a qualitative analysis. Quantitative analysis information is easily reduced by stepping through the process and noting significant elements of each step, including significant information from the interview, records, survey, and quantitative analysis. This is just a process of putting raw data into words, formatted in a fashion that flows logically.

Infiltration and Attack Vulnerabilities

Finally, the risk analyst should create a comprehensive list from the vulnerability calculations of every vulnerability to be addressed. In a spreadsheet, with assets listed in rows to the left, list the vulnerabilities found for each asset row in a new column to the right of the asset column. Then create two columns: Infiltration Vulnerability or Attack Vulnerability. Now, place an “X” in the appropriate column under Infiltration Vulnerability or Attack Vulnerability.

CHAPTER 9

Estimating Probability

INTRODUCTION

At the end of this chapter, you will understand the issue of probability for all types of threat actions, how to obtain statistical data for criminal action probability, and how to estimate probability for terrorism, economic crimes, violent crimes, subversive crimes, and petty crimes. (Risk factors are presented in Figure 9.1.)

Basic Risk Formula

$$\text{Risk} = \text{Probability} * \text{Vulnerability} * \text{Consequence}$$

or

$$\text{Risk} = (\text{Probability} + \text{Vulnerability} + \text{Consequences})/3$$

Classical risk analysis methodologies, including all of the U.S. Department of Homeland Security (DHS)–approved methodologies, assume the existence of a threat actor, times probability, times the vulnerability to be the risk. (This calculation works equally well by summing the three variables and averaging the result.)

Likelihood

The existence of a threat actor is presumed (no threat actor means no threat action), and vulnerability can be estimated from data at hand, but probability, or likelihood, is virtually impossible to calculate for terrorism acts, although we will discuss methods of estimating likelihood in this chapter.

In most communities, data are available from reliable sources to help the risk analyst estimate violent and nonviolent crimes, including felonies and misdemeanors (more about that later in this chapter).

But for terrorism, the picture is different. For terrorism, the challenge is one of determining the probability or likelihood of an event. This is for all practical purposes impossible, but still it must be estimated to make a legitimate case for antiterrorism expenditures. It is impossible, because unlike criminal incidents, where occurrences are common enough to build up a solid database that can be extrapolated to the facility in question with

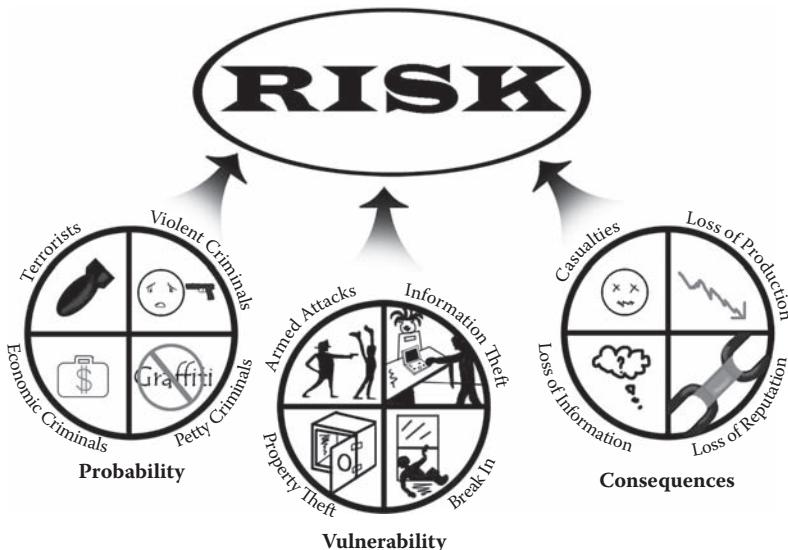


FIGURE 9.1 Risk Factors

statistical surety, the only sure way to determine that a terrorist attack will occur would be to have clear and present intelligence of an attack being planned against a specific facility. This sort of intelligence almost never occurs, and when it does, it is obviously better to disrupt the attack plan than to begin building defensive countermeasures.

Even though we can use statistical data to determine the likelihood of a criminal attack, the same is not possible for terrorist attacks. There are simply an insufficient number of terrorist attacks to build a useful predictive database. But, they do occur, and when they occur they are catastrophic to an organization. The loss of lives, business continuity, facilities, and business reputation is both tragic and arguably avoidable. The absence of an attack does not mean that there will not be an attack. It also does not mean that there will be an attack. But the continued existence of terrorist groups with agendas that include organizations that fit the description of yours infers that the organization you are serving could be a target. That emphasizes the need for preventative risk management planning.

Additionally, terrorism is not monolithic. No two terrorist organizations have exactly the same agenda. No two have the same target preferences. No two use exactly the same mix of methods and tactics. No two will select the same target or attack it in the same way. So it is also necessary to understand the most likely terrorist organization(s) to consider.

Terrorism Probability Estimates and Surrogates

How then can a risk analyst estimate probability for terrorism? It is not uncommon for risk analysts to simply state that the probability for a terrorist attack equals 1 and simply assume that it will occur. However, this does not answer the question of where the most resources should go. With two-lane K12 barriers costing well over \$100,000 each, and blast-resistant glazing costs running into the hundreds of thousands, and fencing costs also running into the hundreds of thousands, should an organization protect everything

equally? Or would it be better to understand what assets are most attractive to the most likely terrorist organization(s)? I think so. This allows the risk analyst to focus his or her recommendations for countermeasures onto those countermeasures and those attributes of the organization that will do the most to deter an attack from the most likely source of an attack.

RESOURCES FOR LIKELIHOOD

Viewing the Range of Possible Threat Actors

As stated above, there are multiple types of threat actors, and each is interested in different aspects of the organization. This is important because what is attractive to a suicide bomber is not likely attractive for a pickpocket or information technology criminal. What is most interesting for a paramilitary terrorist organization is not likely to be the most interesting for a disgruntled employee. Transnational organized crime groups do not want to disrupt the operations of the organizations they feed upon. Prostitutes are more interested in the hotel restaurant or bar than in the porte cochere or lobby.

It is necessary to understand the threat actors and the things that interest them the most in order to understand what should be protected. As a risk analyst, your job is to recommend countermeasures that most of all make the organization an unattractive playing field for both criminals and terrorists. You cannot do that unless you understand what it is about the organization that is attractive to their intentions.

- Terrorist Threat Actors (also see Chapter 7)
 - *Terrorism Classes:* All terrorists are not equal. Terrorists join their causes for different reasons and have different objectives. Those differences determine what type of facility they want to target and in what way they will attack it. Terrorists form into five classes*:
 - *Class I Terrorist:* The government-trained professional (including foreign intelligence threats)
 - *Class II Terrorist:* The religious extremist professional
 - *Class III Terrorist:* The radical revolutionary or quasi-religious extremist
 - *Class IV Terrorist:* Guerrilla/mercenary soldier
 - *Class V Terrorist:* Amateur (civilian, untrained criminal, or militia-vigilante groups)
 - *Class I Terrorist:* The government-trained professional (including foreign intelligence threats) is among the most potent threat actors for assassinations, sophisticated bombings, and abductions. Their area of operations is generally international or regional. Training, equipment, and discipline are all very high. The support structure is excellent. Planning and execution are highly professional. Intelligence sources to support them are keen. Examples of Class I terrorists include those who carried out the Pan Am Flight 103 bombing over Lockerby, Scotland.

A second subgroup of Class I terrorists include those who are trained by a quasi-government organization or under the knowing eye of a legitimate government. Such includes the Munich massacre of 1972, perpetrated by Black

* Malcolm Nance, *Terrorist Recognition Handbook*, 2nd ed. (Boca Raton, FL: CRC Press, 2008), Chapter 2.

September, which were trained by Yasser Arafat's Palestinian Liberation Organization* and Lashkar-e-Taiba (LeT), which were trained in Pakistan at one time under the knowing eye of the Pakistani Inter-Services Intelligence (ISI) Agency.

- ***Class II Terrorist:*** The religious extremist professional is arguably the most dangerous in terms of the number of casualties. Religious extremists swear dedication to an extremist cause in the name of their religion and have sworn allegiance to a group that is dedicated to destroying others who do not share their extremist view of their religion. This may include their own and other governments, those of its own and other religions who do not share their radical interpretation of their religion, and also other ethnic groups who it sees as infidels. Examples of class II terrorists include Al Qaeda, Hezbollah, Hamas, and LeT.
- ***Class III Terrorist:*** The radical revolutionary or quasi-religious extremist — examples include the Red Army Faction, Basque Separatist and Homeland Movement (ETA), and certain individuals such as "... Yigal Amir, a radical right-wing Orthodox Jew who opposed the signing of the Oslo Accords and believed that he was saving his country from a dire fate."[†] Amir assassinated Israeli Prime Minister Yitzhak Rabin on November 4, 1995.
- ***Class IV Terrorist:*** Guerrilla/mercenary soldier — examples include Hutu Guerrillas who massacred rival Tutsis and the Janjaweed of Sudan who were drawn from nomadic Arabic-speaking African tribes. Janjaweed have massacred, raped, and tortured hundreds of thousands of Darfur's sedentary population and rebel groups reportedly at the behest of the Sudanese government. Other examples include the child soldiers of Ivory Coast, Colombia's FARC, and Abu Sayyaf Group (Philippines). Other examples include transnational organized criminal groups that conduct "narcoterrorism," such as Pablo Escobar's organization. Such individuals and groups serve political puppets and carry out atrocities in furtherance of the cause of their masters. Such groups usually attack in small or large groups and use military weaponry.
- ***Class V Terrorists:*** Amateur (civilian, untrained criminal, or militia-vigilante groups) Amateur terrorists include Timothy McVeigh and Terry Nichols who bombed the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma (radical antigovernment terrorists) and Eric Robert Rudolph, also known as the Olympic Park Bomber (a radical Christian Terrorist associated with the White Supremacist Christian Identity Movement). Around the world, militia organizations and individuals with radical leanings attack symbols of their hatred. Such groups and individuals usually use small explosives and firearms.
- The risk analyst should constantly maintain familiarization with all classes of terrorist threats within his or her area of operation. Knowledge of agendas, size, potency, preferred weaponry, methods, and tactics should all be known to the risk analyst beforehand. It is important to understand the agenda and preferred targets of each type of terrorist organization that is operating in his or her area of consulting operations.

* Aaron Mannes, "Black September — How terrorism got its start," *National Review Online*, September 11, 2006.

† http://en.wikipedia.org/wiki/Yitzhak_Rabin.

- From the list of active terrorist organizations that are operating in the area of the facility, the risk analyst must determine two things:
 1. Which of these is interested in facilities like the one under consideration?
 2. What methods and tactics do these groups use to attack their targets?
- Those most interested in the facility type in question will become obvious as we begin to delve into the Asset Target Value Matrices.
- The second is important so that the correct attack scenarios are used in the Asset/Attack Matrix.
- It should also be noted that terrorist organizations sometimes change target models and methods of attack. An example of this was the Mumbai attacks by Lashkar-e-Taiba (LeT) of 2008. This attack was a radical departure for LeT in both targets and methods from previous attacks. However, having said that, if one ran LeT through the Asset Value on Terrorism (KSM Model) described below, one would find that all of the targets of that attack came up as high probabilities from LeT's terrorist agenda, so the model works even when tactics change, because their agenda had not changed, only their tactics.
- Criminal Threat Actors
 - *Economic criminals:* Economic criminals, like terrorists, come in many types:
 - *Transnational criminal organizations:* These organizations are a superset of Organized crime which operates across national boundaries. Obvious examples include the Medellin and Cali drug cartels. Transnational criminal enterprises engage in nuclear smuggling, drug trafficking, trafficking in persons, intellectual property (IP) crimes, and money laundering.
 - *Organized crime:* Organized crime groups operate primarily within a nation's borders and focus on criminal enterprises that are more locally based. Organized crime groups may have ties to transnational crime organizations, but treat them as a service for money laundering, or to facilitate the group's operations when traveling outside the country of origin. Examples of organized crime groups include the various groups of the Mafia in the United States and Europe. Typical activities include targeting businesses through the use of extortion, theft, and fraud, including hijacking cargo trucks, robbing goods, smuggling, bid-rigging, counterfeiting money or products, gambling, prostitution, drugs, gunrunning, murder for hire, and human trafficking.*
 - Sophisticated economic criminals use surveillance and planning to carry out economic crimes as individuals or as small closely knit groups. Examples include the Great Train Robbery of 1963, Internet criminals who collect and sell consumers' identities, real-estate criminals, check fraudsters, Ponzi scheme criminals, and jewel thieves.
 - Unsophisticated economic criminals, also known as opportunistic criminals, use little planning and sophistication in carrying out their crimes. Examples include common burglars, pickpockets, muggers, con men, and the like.
 - *Information technology (IT) criminals:* IT criminals may or may not be economic criminals. IT criminals use computers and the Internet to conduct crimes that may include breaking into other computers, stealing data, interrupting active network communications and placing themselves between the

* http://en.wikipedia.org/wiki/Criminal_Organization.

users, fake Web sites designed to garner personal information, destruction of data, and the like.

- *Nonterrorist violent criminals:* Even though all terrorists use violence, not all violence is terrorism. Almost anyone can be prompted to violent action, but for those with less impulse control, this may happen more often. Violent criminals may act out of planning or spontaneously. Violence may be used as a means to control the victims during the carrying out of a crime or as an end in itself.
- *Subversives:* Subversives are individuals working against the interests of the organization. These may include political or industrial spies, disturbance causers (including civil disorder), and persistent rule breakers.
- *Petty criminals:* Petty criminals are a class of unsophisticated criminals who may or may not be economic criminals. These often include vandals, pick-pockets, and prostitutes and pimps.
- Each class of criminals uses targeteering that is relatively consistent for the class. Thus, a potential target can be estimated for its asset target value by using those attributes as an estimating rule.

CRIMINAL VERSUS TERRORISM LIKELIHOOD RESOURCES

General Comparison for Resources

As stated above, there are no useful databases for terrorism to estimate the likelihood of the facility in question being of interest to a potential terrorist. This is the central question for terrorism risk analysis: Is a specific facility likely to be of interest to a given terrorist organization?

Terrorism Asset Target Value Estimates

In the early days after September 11, 2001, government risk analysts searched for a formula that could help them determine whether or not a terrorist organization might be interested in targeting specific classes of facilities.

- *CARVER+Shock*
 - As governments often do, they turned to the military to learn about targeting. As militaries often do, they relied on their own, tried and true method of targeteering as a rule. For many years, U.S. Special Forces used the CARVER method of target selection. “CARVER is a nationally recognized target analysis and vulnerability assessment methodology used extensively by all military services and the Intelligence Agencies.”* CARVER stands for criticality, accessibility, recuperability, vulnerability, effect on population, and recognizability.
 - “CARVER is a target selection methodology originally designed by U.S. Special Operations Forces to determine the value of a target to military attackers. The CARVER target selection factors assist planners and operators in identifying choke points and critical damage points.”†

* www.homelanddefensejournal.com/hdl/CARVER-Methodology-june.htm.

† <http://www.sarma-wiki.org/index.php?title=CARVER#History>.

- After 9/11, the military added a seventh tool that helps evaluate “... the combined health, economic, and psychological impacts of an attack, or the SHOCK attributes of a target.”*
- To use CARVER or CARVER+Shock, one evaluates the components of a facility using the seven attributes, ranked on a scale of 1 to 10 for each, and then averages the sum of the estimates for each component. This shows the analyst what component of a facility would be best to target for military purposes.
- The problem with both CARVER and CARVER+Shock is that they are made by and for military special forces and both do a very good job of determining what targets would be good for military operations (i.e., to take a facility out of operations for as long as possible). CARVER and CARVER+Shock, however, do nothing to help the analyst understand if a target would be interesting to a particular terrorist organization due to the fact that terrorists are not necessarily interested in taking out a facility but are very interested in communicating through the use of violence.
- Terrorists use violence as language. The language of violence causes a public debate, not only about the terrorist act, but also about the causes of it and what can be done about it. Terrorists speak through violence to the public directly, past the national leadership. The language of violence can affect elections, such as in Spain in 2004 after the Madrid train bombings,[†] terrorism can affect the stability of governments as evidenced by Pakistani President Asif Ali Zardari’s statement, “Terrorists wanted to destabilize Pakistan ...”[‡] Terrorists may want to drive out foreign nationals and foreign workers from their own lands.[§]
- If a risk analyst wants to know what component of a facility to strike in order to take out the facility for a long time, CARVER and CARVER+Shock are good tools. But if a risk analyst wants to know if a terrorist organization would be interested in this facility, CARVER and CARVER+Shock are woefully inadequate.
- *KSM-Asset Target Value Model:* Responding to this, I developed the KSM-Asset Target Value Model, named after Khalid Sheikh Mohammed, who was the principal architect of the 9/11 attacks. KSM selected the targets for the September 11, 2001, attacks and also had a principal or influencing role in the 1993 World Trade Center attack, Operation Bojinka, an aborted 2002 attack on Los Angeles’ U.S. Bank Tower, the Bali Bombings, the failed bombing of American Airlines Flight 63, the Millennium Plot, and the murder of Daniel Pearl. KSM knows well Al Qaeda’s model for targeting, and reports of his interrogations have him saying that during his first targeting meeting, Bin Laden discussed targeting. Discussions included economic, political, and military targets. Interrogations of KSM have become a wealth of information about how Al Qaeda operates and selects its targets. The specifics of Al Qaeda targeting include a list that includes the following:

* www.ngfa.org/pdfs/Carver_Shock_Primer.pdf.

† www.pbs.org/newshour/updates/europe/jan-june08/spain_03-07.html.

‡ www.geo.tv/10-21-2008/27336.htm.

§ James Brooke, “Attacks in Peru drive out foreigners,” *The New York Times*, January 15, 1990, “The killing of two French sightseers in Peru’s Andean highlands on Friday highlights how terrorist attacks are forcing a wide withdrawal of foreign aid workers, archaeologists and tourists from remote areas of this country’s mountainous interior.”

- Does the target fit the strategic objectives of Al Qaeda?
- Are mass casualties possible?
- Can the attack generate prolonged media coverage, especially of the attack itself?
- Is the target of economic importance?
- Is the target of cultural importance either to the constituent community of the victim or the constituent community of Al Qaeda or both?
- Is the target highly vulnerable to attack?
- What is the probability of success of the attack?
- Does this attack benefit recruiting and fund raising for Al Qaeda?

Using this model, one can easily see how all past attacks by Al Qaeda and attacks in which Al Qaeda have contributed planning and organization have all fit the KSM Targeting Model. For example, the Mumbai attack of 2008 against rail, theater, hotels, hospitals, and Jewish center, fit all these criteria. The 2001 World Trade Center attack was planned in such a fashion that the television cameras of the world would be focused in live coverage on the towers when the second plane struck, causing shock and impact far beyond a postevent account of the attack by the media.

Al Qaeda have been experts at exploiting obvious vulnerabilities. Few risk analysts before September 11, 2001, seriously considered attacks by airplanes on high-rise buildings. But in hindsight, the attack mode was obvious to all who previously rejected such.

To use the KSM Targeting Model, create a spreadsheet with rows on the left identifying the facility and its key assets. Then create columns above for each of the targeting criteria. Score each cell from 1 to 10, sum columns for each asset, and average the sum. Then rank the results by individual asset and by asset class (people, property, information, and business reputation).

The proof of the KSM Targeting Model is in evaluating it against targets that have been struck by Al Qaeda and Al Qaeda-related groups. Without exception, all of their targets fit the model.

Similar models can be built for each terrorist group by analyzing their public statements and interrogation reports of senior leaders for the organization's agenda and targeting preferences, thus creating a model for each organization that is accurate for use. Terrorist organizations are surprisingly open about their targeting preferences, but a risk analyst must interpret these public statements into strategic criteria.

Use the KSM Model for any facility in near proximity to the project as an attack on a facility can have devastating effects on nearby facilities.

CRIMINAL INCIDENT LIKELIHOOD ESTIMATES

There are two main sources for criminal criteria estimates: *criminal statistics* and *asset target value estimates*.

Criminal Statistics

The best source is actual criminal statistics, which should be used whenever available. Criminal statistics should include records that go back at least 5 years and should cover the following types of crimes:

- Major crimes
 - Murders
 - Rapes
 - Assaults
 - Major economic crimes
- Minor offenses
 - Vehicle crimes
 - Misdemeanor crimes

Few local authorities maintain records in a fashion that is easily usable by risk analysts, and some question the validity of police records that might have been falsified in order to qualify for higher federal funding. Failing availability of crime statistics from local authorities that are complete, organized, and reliable, in many areas analysts can turn to private sources such as CAP Index, Inc.[®]. Such sources offer highly organized and graphically presented data that are useful for risk analysis.

Alternatively, in the absence of usable data, an analyst can use an asset target value estimate, similar to that used for terrorism.

Economic Crime Asset Target Value Estimate

The elements for economic crime asset target value estimates include the following:

- Is there an opportunity for economic gain?
- What is the probability for success?
- What is the probability for escape?
- What is the probability for escape without subsequent capture?

Remember, this is not a vulnerability analysis but rather an estimate of how attractive key assets are to economic criminals. Vulnerability may be a factor in the probability of success, along with other factors including hours of operation, accessibility, and vigilance. Depending on the type of economic crime, the size of the organization planning the crime, and the sophistication of the criminal, and the assets in question, what may be a low probability of success for one type of economic criminal may be a high probability of success for another offender.

The analyst should consider the type of economic crime that would be most concerning to the organization and use that as a baseline for estimating.

To use the Economic Crime Asset Target Value Model, create a spreadsheet with rows on the left identifying the facility and its key assets. Then create columns above for each of the targeting criteria. Score each cell from 1 to 10, sum columns for each asset, and average the sum. Then rank the results by individual asset and by asset class (people, property, information, and business reputation).

Nonterrorism Violent Crime Asset Target Value Estimate

As stated above, terrorists use violence, but not all violent crimes involve terrorism. Violent crimes include planned and spontaneous murders, rapes, aircraft hijacking, child abuse, elder abuse, kidnapping, happy slapping, and police brutality.

Violent crimes are often committed by people with poor impulse control. Often these are people who have difficulty controlling their own lives and so attempt to control those around them. Often when such a person fails to maintain control, they resort to violence instead of just “moving on.”

One example of such is David Pardo, who arrived at the front door of his former in-laws’ home on Christmas Eve wearing a Santa suit. The door was opened by an 8-year-old girl whom he shot in the face. He then proceeded through the home that was filled with about 25 holiday visitors and killed a total of 9 in the extended family, including his former wife, both her parents, and others. He then used a custom-made incendiary device to set the home on fire, which then burned to the ground. Even though the extent of Pardo’s obsession is not common, it is common for many domestic partners to resort to violence when their lives go wrong.

Other clues to violent behavior include drunkenness, acute depression, schizophrenia, psychopathic personality, brain damage, flawed brain chemistry and genetic defects,* and criminals who use violence to control their victims during the execution of a crime, such as in the case of home invasion robberies.[†]

Whatever the cause, almost all violent criminals use some judgment in committing their crimes. The lone exception is the rage-aholic who may attack anyone nearby without concern for the consequences. Rage-aholics are typically highly mentally disturbed individuals, often paranoid schizophrenics who are so out of touch with reality at the time.[‡]

Most violent criminals who are aware of their actions use certain criteria to determine if and when to conduct a violent attack. These include the following:

- Is there an available surveillance position to reconnoiter the target before finally selecting it?
- Is access identification required before entry? (No violent criminal wants to be identified, so any form of identification including cameras and ID checks are a strong deterrent to violent crimes.)
- Is forcible entry possible?
- Is there any sneak-path for entry, exit, or both?
- Is the asset or subject vulnerable to direct physical attack or intimidation through the use of force?
- Can entry be made through social engineering? (“Hello, I accidentally damaged your car with mine, could you open the door so that I can give you my insurance information?”)
- What is the probability of success of the physical attack? (Is the victim likely to be overwhelmed by force, or am I about to attack Chuck Norris?)
- What is the probability of escape? (Yes, I may be able to strike down the elderly woman to get her purse, but what about the 50 people at the festival who would see me do that?)

* Michael Bernstein, “Latest research on possible causes of violent behavior explored in C&EN article,” *Medical News Today: Public Health*, June 3, 2003.

[†] www.fdle.state.fl.us/OSI/CrimeBriefs/HomeInvasion/Home Invasion.pdf.

[‡] www.schizophrenia.com/New/Dec2002/violenceDec02.htm.

To use the Violent Crime Asset Target Value Model, create a spreadsheet with rows on the left identifying the facility and its key assets. Then create columns above for each of the targeting criteria. Score each cell from 1 to 10, sum columns for each asset, and average the sum. Then rank the results by individual asset and by asset class (people, property, information, and business reputation).

Petty Crimes Asset Target Value Estimate

For some facilities, particularly those hosting masses of the public, such as hotels, convention centers, retail malls, and the like, petty crimes are a constant concern. Even for facilities such as factories and distribution centers, a constant stream of vandalism and graffiti can be a deterrent to good business.

For such facilities, it is useful to consider petty crimes asset target value. Criteria may change from one type of facility to another, so the Asset Target Value Matrix will not be constant. For example, hotels tend to attract prostitution and pimps, and retail malls may have a problem with pickpockets and purse snatchers.

The risk analyst should develop an Asset Target Value Matrix that focuses on the type of petty criminal the facility will confront.

SUMMARY

The two most common versions of the risk formula include the following:

$$\text{Risk} = (\text{Probability} * \text{Vulnerability} * \text{Consequence})$$

or

$$\text{Risk} = (\text{Probability} + \text{Vulnerability} + \text{Consequence})/3$$

Both versions yield proportionally similar results.

Likelihood

The existence of a threat actor is presumed (no threat actor equals no threat action), and vulnerability can be estimated from data at hand, but probability or likelihood is virtually impossible to estimate for terrorism acts.

Probability estimation for criminal acts is more straightforward. In most communities, data are available from reliable sources to help the risk analyst estimate violent and nonviolent crimes, including felonies and misdemeanors either from police department criminal statistics or from the CAP Index.

- *Terrorist Threat Actors*
 - Terrorists form into five classes:
 - *Class I Terrorist*: The government-trained professional (including foreign intelligence threats)
 - *Class II Terrorist*: The religious extremist professional

- *Class III Terrorist:* The radical revolutionary or quasi-religious extremist
- *Class IV Terrorist:* Guerrilla/mercenary soldier
- *Class V Terrorist:* Amateur (civilian, untrained criminal, or militia-vigilante groups)
- The risk analyst should constantly maintain familiarization with all classes of terrorist threats within his or her area of operation. Knowledge of agendas, size, potency, preferred weaponry, methods, and tactics should all be known to the risk analyst beforehand. Especially important is to understand the agenda and preferred targets of each type of terrorist organization that is operating in his or her area of consulting operations. *Remember, the focus must be on the most attractive target in the vicinity, not only the facility which is under analysis. A strike on a nearby target can have devastating results on nearby facilities.*

If reliable crime statistics are not available, then the risk analyst can use the asset target value as a surrogate for crime statistics. In such cases, the nature of criminal threat actors must also be understood.

- *Criminal Threat Actors*
 - *Economic criminals:* Economic criminals, like terrorists, come in many types:
 - Transnational criminal organizations
 - Organized crime
 - Sophisticated economic criminals
 - Unsophisticated economic criminals, also known as opportunistic criminals, use little planning
 - Information technology (IT) criminals
 - Nonterrorist violent criminals
 - Petty criminals

Terrorism Asset Target Value Estimates

Common asset target value estimating tools for terrorism include:

- *CARVER+Shock*
- *KSM Asset Target Value Model* (used for the facility and its nearest attractive target):
 - Does the target fit the strategic objectives of Al Qaeda?
 - Are mass casualties possible?
 - Can the attack generate prolonged media coverage, especially of the attack itself?
 - Is the target of economic importance?
 - Is the target of cultural importance either to the constituent community of the victim or the constituent community of Al Qaeda or both?
 - Is the target highly vulnerable to attack?
 - What is the probability of success of the attack?
 - Does this attack benefit recruiting and fund-raising for Al Qaeda?

Criminal Incident Likelihood Estimates

There are two main sources for criminal criteria estimates: criminal statistics and asset target value estimates.

Criminal Statistics

The best source is actual criminal statistics, which should be used whenever available. Criminal statistics should include records that go back at least 5 years and should cover the following types of crimes:

- Major Crimes
 - Murders
 - Rapes
 - Assaults
 - Major economic crimes
- Minor Offenses
 - Vehicle crimes
 - Misdemeanor crimes

Failing availability of crime statistics from local authorities that are complete, organized, and reliable, in many areas analysts can turn to private sources such as CAP Index, Inc.

Alternatively, in the absence of usable data, an analyst can use an asset target value estimate, similar to that used for terrorism.

Economic Crime Asset Target Value Estimate

Economic crime asset target value estimates include the following:

- Is there an opportunity for economic gain?
- What is the probability for success?
- What is the probability for escape?
- What is the probability for escape without subsequent capture?

Nonterrorism Violent Crime Asset Target Value Estimate

Most violent criminals seem to use the following criteria to determine if and when to conduct a violent attack:

- Is there an available surveillance position to reconnoiter the target before finally selecting it?
- Is access identification required before entry?
- Is forcible entry possible?
- Is there any sneak-path for entry, exit, or both?
- Is the asset or subject vulnerable to direct physical attack or intimidation through the use of force?
- Can entry be made through social engineering?
- What is the probability of success of the physical attack?
- What is the probability of escape?

Petty Crimes Asset Target Value Estimate

For some facilities, particularly those hosting masses of the public, such as hotels, convention centers, retail malls, and the like, petty crimes are a constant concern. A constant stream of vandalism and graffiti can be a deterrent to good business for any commercial facility.

A Petty Crimes Asset Target Value study can be enlightening for any facility. Criteria may change from one type of facility to another, so the Asset Target Value Matrix will not be constant. For example, hotels tend to attract prostitution and pimps, while retail malls may have a problem with pickpockets and purse snatchers. The risk analyst should develop an Asset Target Value Matrix that focuses on the type of petty criminal the facility will confront.

CHAPTER 10

The Risk Analysis Process

INTRODUCTION

As presented in Chapter 2, the U.S. Department of Homeland Security (DHS)-approved risk assessment methodologies vary substantially in the formulas used. The two most complete methodologies are the American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA) methodology and the Sandia methodologies (all of which use the same formula).

However, all of the better DHS-approved methodologies have the same two things in common:

1. They all use the elements of probability, vulnerability, and consequence.
2. They all result in comparatively similar findings, even considering the differences in the formulas and approaches.

The key to the approval by DHS appears to be that the ranking of risks should be similar, not that the formulas result in exactly the same numbers. *The mathematical relationship, not the mathematical result, is important.*

This is also illustrated by the fact that the API/NPRA methodology can be interpreted in a table, rather than in a formula, where the table ranks its findings by position in the table (no actual mathematical result).

In the end, the objective is all about providing the evidence for countermeasure selection decisions. Thus, the ranking rather than the formula matters.

The Sandia model and approach to risk analysis are highly respected. But for most commercial, governmental, industrial, and critical infrastructure projects, the cost of the Sandia-style analysis with its abundant team of subject matter experts is not bearable to the project.

For most organizations, a competent risk analyst or a small team of experts can achieve the same general results at completely affordable costs using either the Sandia formula or the API/NPRA model.

We will begin to look at how to achieve those results using a simple spreadsheet program.

OBJECTIVE

Remember, the actual formulas used do not matter as long as the relationships of the variables remain the same. We can substitute the Sandia and the various versions of

Sandia API/NPRA Comparison (0 to 1)			
Risk	Probability	Vulnerability	Consequence
Sandia R = P*(1 - V)*C			
0.42	1	0.6	0.7
0.25	0.7	0.6	0.6
0.08	0.5	0.4	0.4
0.04	0.4	0.3	0.3
API/NPRA			
Using R = P * V * C			
0.49	1	0.7	0.7
0.25	0.7	0.6	0.6
0.08	0.5	0.4	0.4
0.04	0.4	0.3	0.3
Using R = (P + V + C)/3			
0.80	1	0.7	0.7
0.63	0.7	0.6	0.6
0.43	0.5	0.4	0.4
0.33	0.4	0.3	0.3

FIGURE 10.1 Comparison of Sandia and American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA) Formulas

API/NPRA formulas for the same risk values, and the risk relationship always remains the same. (See Figure 10.1 for a comparison of Sandia and API/NPRA formulas.)

Examples

Further, except for the Sandia model, which must use component numbers between 0 and 1, with API/NPRA and other similar models, we can use any component numbers such as 0 to 1; 0 to 10; 0 to 100; or 0 to 1,000,000; and the risk relationship will always remain the same. Also note that the Sandia model uses $(1 - V)$ instead of V because the component numbers are fractions of one, and using three variables with fractions of one will result in inverse relationships. (Risk would appear to reduce as vulnerability goes up.) For API/NPRA, all assumed formulas use 1 to 5; 1 to 10; and so forth. If one were to use 0 to 1 for API/NPRA, then one would also have to use $(1 - V)$ instead of V in the formula.

Sandia API/NPRA Comparison (0 to 10)			
Risk	Probability	Vulnerability	Consequence
Sandia R = P*(1 - V) * C		(1 - V)	
0.42	1	0.6	0.7
0.25	0.7	0.6	0.6
0.08	0.5	0.4	0.4
0.04	0.4	0.3	0.3
API/NPRA			
Using R = P * V * C			
490	10	7	7
252	7	6	6
80	5	4	4
36	4	3	3
Using R = (P + V + C)/3			
8.00	10	7	7
6.33	7	6	6
4.33	5	4	4
3.33	4	3	3

FIGURE 10.2 Comparison Using 0 to 10 Component Numbers

All of the examples presented in Figures 10.2 through 10.4 result in relatively similar risk rankings. Though the actual risk results may vary slightly, the relationships always remain the same.

The balance of this book will use the API/NPRA methodology formulas for simplicity. It would be confusing to compare Sandia and API/NPRA throughout the rest of the book. However, rest assured that the principles taught herein work equally well using both formulas, and in fact, work equally well using any methodology that combines probability, vulnerability, and consequence to comprise risk. (No other approach results in a valid risk result.)

Displaying Risk Formula Results

In the API/NPRA methodology, the formula is expressed as a matrix of probability and vulnerability (two dimensions), then ranked later by consequences. I always thought that

Sandia API/NPRA Comparison (0 to 100)			
Risk	Probability	Vulnerability	Consequence
Sandia R = P*(1 - V) * C			
0.42	1	0.6	0.7
0.25	0.7	0.6	0.6
0.08	0.5	0.4	0.4
0.04	0.4	0.3	0.3
API/NPRA			
Using R = P * V * C			
490000	100	70	70
252000	70	60	60
80000	50	40	40
36000	40	30	30
Using R = (P + V + C)/3			
80.00	100	70	70
63.33	70	60	60
43.33	50	40	40
33.33	40	30	30

FIGURE 10.3 Comparison Using 0 to 100 Component Numbers

was a bit abstract, so I developed a method to express all three dimensions in one spreadsheet. I do that by showing consequence in three levels with different text **Bold = High**, *Italics = Medium*, and Standard Text = Low. (See Figure 10.5 for a presentation of the V² Summary Matrix.)

The spreadsheets taught in this book are capable of illustrating all three dimensions. Alternatively, these can be reduced using any of the formulas above and illustrated as a list or as an array.

THE COMPLETE RISK ANALYSIS PROCESS

So far, we compared the best risk analysis methodologies and found that their results are comparable. API/NPRA provides wide latitude in how risk is calculated and always results in comparable results. As such, I typically utilize the API/NPRA methodology for most risk analysis projects, and it fits the needs of most DHS-sponsored projects. The steps shown herein meet or exceed all risk analysis methodologies except for Sandia, which is too excessive in its depth for most commercial applications.

Sandia API/NPRA Comparison (0 to 1)			
Risk	Probability	Vulnerability	Consequence
Sandia R = P*(1 - V) * C			
0.30	1	0.6	0.5
0.35	1	0.7	0.5
0.40	1	0.8	0.5
0.45	1	0.9	0.5
API/NPRA			
Using R = P * V * C			
0.30	1	0.6	0.5
0.35	1	0.7	0.5
0.40	1	0.8	0.5
0.45	1	0.9	0.5
Using R = (P + V + C)/3			
0.70	1	0.6	0.5
0.73	1	0.7	0.5
0.77	1	0.8	0.5
0.80	1	0.9	0.5

FIGURE 10.4 Comparison Using Different Component Numbers

The results that will be achieved include:

- Step-by-step spreadsheet process to risk results
- The results can be expressed either in numbers or graphically
- Prioritization of risk results, which will be illustrated in Chapter 11

Now the resources that have been assembled and how they contribute to the risk analysis calculation will be reviewed. Each of these has an important role in the overall risk calculation.

We step through the calculation by first determining what types of threat actors constitute a threat to the facility in question.

Then, the probability is reviewed (the aspects of the facility which make it a likely target for the different threat actors).

The facility's vulnerability is reviewed next (the aspects of the facility that could be exploited by a threat actor).

Facility Name	ASSET TARGET VALUE (Probability)		
VULNERABILITY	HIGH	MEDIUM	LOW
	HIGH <i>Most Consequence Assets are Bold/Italics</i> <i>Medium Consequence Assets shown in Italics</i> Least Consequence Assets are shown Normally	Medium ATV and High Vulnerability	Low ATV and High Vulnerability
MEDIUM	High ATV and Medium Vulnerability	Medium ATV and Medium Vulnerability	Low ATV and Medium Vulnerability
LOW	High ATV and Low Vulnerability	Medium ATV and Low Vulnerability	Low ATV and Low Vulnerability

FIGURE 10.5 V² Summary Matrix (ATV Stands for Asset Target Value)

Finally, the consequences are reviewed. Risk only occurs if there are consequences to the action; the more significant the consequences are, the greater is the risk. Risk should also be prioritized by consequences.

Probability Factors

- Threat Considerations
 - Terrorist organization targeteering*
 - Adversary/Means Matrix†
- Asset Target Value Considerations
 - Crime Statistics‡
 - CAP Index Report
 - CARVER+Shock Matrix§
 - KSM-Asset Target Value for Terrorism Matrix¶
 - Circulation Path/Threat Nexus Matrix**
 - Circulation Path/Weapons Nexus Matrix††
 - Economic Crimes Matrix‡‡
 - Violent Crimes Matrix§§
 - Petty Crimes Matrix¶¶

* Identifies which terrorist organizations are operating in the region of the facility and whether or not they have shown any interest in this type of facility.

† Illustrates potential threat actors (for terrorism) and their relative capabilities.

‡ Crime statistics and CAP Index Reports provide ratings for the address only, not for individual assets at the address.

§ Basic terrorism calculation.

¶ Advanced terrorism calculation.

** Determines where threat actors and high-value individuals may encounter each other.

†† Determines what types of weapons can be used at the locations where threat actors and high-value individuals could encounter each other.

‡‡ Determines the attractiveness of various assets/locations for different types of economic crime threat actors.

§§ Determines the attractiveness of various assets/locations for different types of violent criminals.

¶¶ Determines the attractiveness of various assets/locations for different types of petty criminals.

Vulnerability Factors

- Asset/Attack Matrix*
- Circulation Path/Threat Nexus Matrix†
- Circulation Path/Weapons Nexus Matrix‡
- Attack Path Analysis§
- Surveillance Matrix¶
- Vulnerability Matrix**

Consequence Factors

Analyze the consequence factors using the Criticality and Consequence Matrix.††

THE RISK ANALYSIS PROCESS

Returning to the basic risk formula, remember that of the various forms of valid risk formulas, the simplest form of the formula is:

$$R = (P + V + C)/3$$

or

$$\text{Risk} = (\text{Probability} + \text{Vulnerability} + \text{Consequences})/3$$

Now we will build up the components to the result.

Probability Factors

- Probability includes a capable threat actor combined with the intent to attack a facility under question. The first element of risk is threat identification. As there are multiple types of threat actors, the first step is to consider the design basis threat (that threat against which the security program is designed to defend).
- The most serious threat actors are terrorists. Of the five kinds of terrorists, not all are likely to be interested in the facility in question. So, the first question is What group of terrorists might be interested in targeting the facility in question? This information can be derived from terrorist organization targeteering histories. Targeteering involves two main factors:

* Determines which assets are most susceptible to various attack scenarios.

† Determines where threat actors and high-value individuals may encounter each other.

‡ Determines what types of weapons can be used at the locations where threat actors and high-value individuals could encounter each other.

§ Determines the path or paths that potential attackers might take, analyzes the capability of protective systems to deal with the attack, and guides the analyst to what types of countermeasures might be required to cope with an attack along the path.

¶ Determines which assets are most susceptible to various surveillance methods.

**Determines overall vulnerability (including existing countermeasures).

††Illustrates criticality and consequences for ranking.

1. The area of operations (AO) of the terrorist organization.
 2. The characteristics of the facility, vis-à-vis the agenda of the terrorist organization.
- *Area of operations information:* Few terrorist organizations operate worldwide. Most have a primary or active area of operation. For each region of the planet, the AO will be different. This may change from time to time. The best organizations for information as to which terrorist organizations are operating in the region of the facility in question include:
 - Jane's World Insurgency and Terrorism Service
 - The Nine Eleven Finding Answers (NEFA) Foundation
 - Terrorism Center for Defense Information
 - Raman's Terrorism Analysis
 - The U.S. Department of State Diplomatic Security Services (US-DOS-DSS)
 - British Foreign and Commonwealth Office (FCO)
 - *Targeteering information:* Targeteering is the preference of a type of target and attack scenario by a terrorist organization or threat actor. This information is more complex and may be somewhat more difficult to discern than simple AO information. In general, though, for larger and more active terrorist organizations where there is a history of strikes against targets, much may be written on the types of facilities struck by the organization. For less active or newer terrorist groups, little may be available. One should also be concerned about emerging terrorist threat actors who have not yet acted. These are the most difficult to get information on due to their lack of action. Targeteering information is rarely discussed in news articles and official reports. One may not be able to find precise targeteering information (as such) about a specific terrorist organization in any public report. However, targeteering information on existing active terrorist organizations can be derived from past attacks.
 - *Terrorist group attack scenarios:* Each terrorist organization has its own preferred attack scenarios. Some, such as Abu Sayaf (Philippines), may prefer kidnappings, and others, such as Islamic Jihad (Gaza), may prefer suicide bombings. It is important to note that even though a specific type of attack scenario may not ever have been used in a specific geographic region, that attack scenario may have, in fact, been used by that organization in other regions. In such cases, the risk analyst would be well advised to include the attack scenario in the list of possible attack scenarios for the region where it has not ever been used. Additionally, terrorist organizations often work together to develop skills and resources. For example, Al Qaeda worked with both the Taliban and Lashkar-e-Taiba (LeT) in Pakistan to develop and enhance the sophistication of their attack scenarios. Even though neither of these organizations had used coordinated attacks and suicide bombers previously, the use of these tactics could be predicted as news reports of the alliance of these groups spread in advance of the use of these tactics. Finally, it is also useful to scan terrorism news blogs such as NEFA and the Investigative Report on Terrorism daily to note the emergence of new terrorist groups and note their agendas, which can imply targeteering information.
 - The other types of threat actors include:
 - Economic criminals
 - Violent criminals
 - Subversives
 - Petty criminals

For each of these threat actors, probability can be determined either from historical data (crime statistics, etc.) or from asset target value. Asset target value is the estimation of the degree of compliance with the factors that make an asset interesting to a particular type of threat actor.

For all classes of criminal threat actors, an Asset Target Value Matrix has been developed and is discussed in this chapter. The Asset Target Value Matrix can also be applied to terrorists using the KSM (Khalid Shaikh Mohammed) Asset Target Value Model and, to a lesser extent, the CARVER+Shock Asset Target Value Model.

The point of crime statistics is crime forecasting. We study the undesirable results of history in order to avoid them in the future. We avoid them by moving “off the railroad tracks” of the freight train that will come again on the same track. By studying how the train has come in the past, we can hear its sound, feel the vibration of the tracks, and move away from its path. When it comes to crime, history does repeat itself. Criminals of a certain type target again and again in certain predictable ways.

Historical data can be assembled using either crime statistics or CAP Index Reports. Crime statistics can be obtained from local law enforcement with varying results. Some jurisdictions keep meticulous records and segment that information into data that can allow for highly refined searches. Other jurisdictions provide data that some would say are designed to confound any analyst. If the data cannot be combined into searches such as facility types, locations, and types of crimes, then they are of little practical use.

CAP Index is a crime statistic product available on the Internet that offers graphically oriented data in a uniform fashion. This is a very useful product especially when available local law enforcement data are not so useful. The CAP Index is available at: www.CAPIndex.com.

DIAGRAM ANALYSIS

- The Adversary Sequence Diagram (ASD) and Path Analysis identifies the pathways from perimeter to target that potential attackers must follow on their way to the target asset. These help to identify the locations within the facility that should be studied for vulnerabilities and where aggressors can be detected, assessed, and delayed.
- The Circulation Path/Threat Nexus^{*} identifies the locations within a facility where high-value individuals might encounter potential threat actors.
- The Circulation Path/Weapons Nexus Matrix[†] identifies the types of weapons that could be used in the locations where threat actors might encounter high-value individuals.
- The Circulation Path/Threat Nexus and Circulation Path/Weapons Nexus analyses can be performed either graphically using diagrams or as matrices. To perform these graphically, one will evaluate drawings and diagram the pathways taken by both high-value individuals and potential threat actors. To define these

^{*} Determines where threat actors and high-value individuals may encounter each other.

[†] Determines what types of weapons can be used at the locations where threat actors and high-value individuals could encounter each other.

in a Threat Nexus Matrix, one must create a matrix that shows nexus points as rows and both high-value individuals and other classes of individuals as columns; for the Weapons Nexus Matrix, one would create a matrix showing nexus points as rows and types of weapons as columns. Then for the Threat Nexus Matrix, one places an “X” at each cross point where high-value individuals might be found and where other types of individuals might cross the path of the high-value individuals. For the Weapons Matrix, one would place an “X” at each nexus point for the type of weapon that could be used at that location. This identifies not only where VIPs might encounter potential threat actors, but also what type of weapon might be used at that location.

ASSET TARGET VALUE MATRICES

When historical data useful for statistics are not available, probability can be estimated from Asset Target Value Matrices. Asset target value analysis lends itself well to quantitative analysis.

Additionally, and perhaps more importantly, asset target value analysis lends itself extremely well to quantitative analysis but diagrammatic processes and targeteering do not. Accordingly, I use diagrammatic processes, crime statistics, CAP Index, and targeteering information as precursor studies preliminary to performing asset target value studies. Together these methods comprise a much more thorough approach to estimating probability.

One should use a separate Asset Target Value Matrix for each type of threat actor within the design basis threat. I know analysts who analyze only for terrorist threats or only for terrorism and a few economic threats. However, no security program can be successful which deals only with terrorism or major economic crime. The security program director will have to cope with a wide range of criminal and subversive activity on the facility, and so the risk analyst should help the program director by preparing a risk profile for all types of threat actors, including all types of anticipated criminal activity. Many people misperceive the design basis threat as only the *worst* threat that the security program must counter, but no security program can be effective if it is not prepared to counter every type of threat actor it will face. In fact, the design basis threat is a range of threats up to and including the worst threat that the security program must counter and not only that threat, as some ill-informed risk analysts seem to believe.

For each Asset Target Value Matrix, the analyst should prepare a spreadsheet matrix that includes all of the assets and security nexus points categorized by logical groupings as rows and the asset target value characteristics as columns. The right-most two columns should be a Score and Ranking as shown in the example below.

- *Asset Target Value Matrices:* The asset target value categories (Figure 10.6) for each of the various types of matrices are shown below:
 - CARVER+Shock Matrix
 - Criticality
 - Accessibility
 - Recoupability
 - Vulnerability
 - Effect

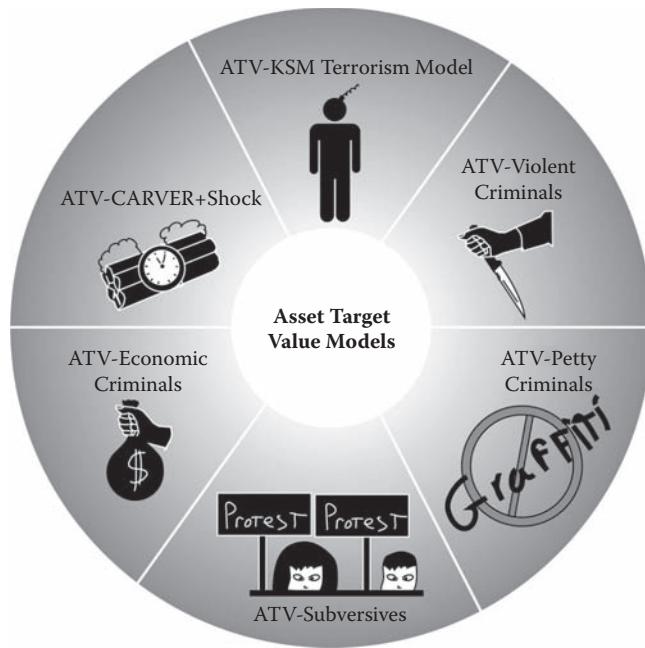


FIGURE 10.6 Typical Asset Target Value Categories

- Recognizability
- Shock
- *KSM Asset Target Value for Terrorism Matrix*
 - Fits the strategic objective of the terrorist organization
 - Mass casualties possible
 - Media event possible
 - Target is of economic importance
 - Target is culturally important
 - Vulnerability
 - Probability of success
 - Success on target has recruiting and fund-raising value
- *Economic Crimes Matrix*
 - Economic gain possible
 - Probability of success
 - Probability of escape
 - Escape without subsequent discovery
- *Violent Crimes Matrix*
 - Surveillance possible
 - Access identification required
 - Forcible access is possible
 - Sneak-path access is possible
 - Target is vulnerable to physical attack
 - Vulnerable to social engineering
 - Probability of success
 - Probability of escape

- *Subversives and Petty Crimes Matrix*
 - Useful environment for exploitation
 - Can establish temporary domain over environment
 - Can go largely unnoticed
 - Minimum resources applied to resolving my crimes
 - Acceptable penalties for discovery

PROBABILITY SUMMARY MATRIX

The results of all of the individual Asset Target Value Matrices should be summarized together in a Probability Summary Matrix. This matrix, like most others, should list all assets (targets and public and VIP/threat actor nexus points) as rows and the scores of all the Asset Target Value Matrices as columns. The Probability Summary Matrix will include columns for the final scores from the following Probability Matrices, including:

- CARVER+Shock Matrix
- KSM Asset Target Value for Terrorism Matrix
- Economic Crimes Asset Target Value Matrix
- Violent Crimes Asset Target Value Matrix
- Subversives and Petty Crimes Asset Target Value Matrix

For example, the result cells (Scores) of the CARVER+Shock Matrix should reference the Probability Summary Matrix CARVER+Shock column. The result cells (Scores) of the KSM-Asset Target Value for Terrorism Matrix should reference the Probability Summary Matrix, and so forth, until the results of all of the constituent probability matrices are represented into the Probability Summary Matrix. An example of a Probability Summary Matrix is shown in Figure 10.7.

VULNERABILITY COMPONENTS

It saddens me to see risk analysts pull a vulnerability rating out of the air. This is done so often that most people in the industry think that is how it should be done. The truth is quite the opposite. Like everything else about risk, vulnerability is a composite of many elements. Unless one considers all those elements, one cannot estimate vulnerability.

Some of the elements for probability are also useful for considering vulnerability. This is not extraordinary, as this presents only a different point of view on the same subject. Even though these have been considered before under probability, they are worth considering again from a vulnerability standpoint. The core elements include the following:

- Aspects to Consider While Reviewing Vulnerability
 - What kinds of attacks are the assets vulnerable to?
 - Where on the facility could high-value individuals come into contact with potential threat actors?
 - What kinds of weapons could be used in areas where high-value individuals might interact with potential threat actors?

Mega Towers						
Probability Worksheet						
Targets		Criminal Threats	Terrorism Threats	Score	Rank	
	People	7	6			
VIP Executives and VIP Visitors		6	7	6	10	
Employees		8	9	8	1	
Contractors		8	5	6	9	
Visitors		8	6	7	6	
Delivery Personnel		7	5	6	19	
Transportation Personnel		7	5	6	19	
Property		5	5	5	4	
Site		5	5	5	28	
VIP Drop-Off		6	7	7	7	
Employee Drop-Off		7	8	8	2	
Visitor Drop-Off — Hotel (South)		7	7	7	5	
Main South Entry Gatehouse Area		7	6	6	14	
North Perimeter Fence		4	5	4	45	

FIGURE 10.7 Probability Summary Matrix

- What paths would adversaries have to take to reach the assets of the facility from outside its perimeter?
- Vulnerability Components
 - What surveillance opportunities exist for each asset?
 - Finally, we roll up all these and other factors when considering all of the constituent elements of vulnerability, including:
 - Accessibility
 - Surveillance (from above)
 - Intrinsic vulnerability
 - Natural countermeasures
 - Physical countermeasures
 - Electronic countermeasures
 - Operational countermeasures

Vulnerability Tools

- The Asset/Attack Matrix lists all of the facility assets and the same threat scenarios that were considered under the Adversary/Means Matrix. The Adversary/Means Matrix provides insight into what types of threat scenarios various threat actors may use, and the Asset/Attack Matrix provides similar insight into what types of threat scenarios each asset is vulnerable to.

- The Circulation Path/Threat Nexus Matrix was used for probability considerations in order to determine the possibility of attacks against high-value individuals (VIPs) within a facility. Similarly, the same matrix gives insight into areas of vulnerability in the facility that would otherwise go unnoticed.
- The Circulation Path/Weapons Nexus Matrix was used for probability considerations in order to understand the types of weapons that might be used in areas where high-value individuals might encounter potential threat actors. The other side of that coin is the vulnerability that such an encounter would present. It is important to consider not only what assets are at risk in a facility, but where and to what threat scenarios.
- The Adversary Sequence Diagram Analysis illustrates the pathways that threat actors must take from the property perimeter to reach an asset. This gives insight not only into probability, but also into vulnerabilities that must be addressed along those pathways. The Adversary Sequence Diagram is also useful when considering potential countermeasures that can be used to detect, assess, and delay threat actors.

All the elements above are not direct contributors to the vulnerability calculation but are preparatory to the quantitative calculations. The following two elements are used to perform quantitative analysis.

- Surveillance is a basic element of vulnerability. Surveillance is a prerequisite of all threat actions by all threat actors. No security program can be effective which does not fully consider surveillance in its risk and countermeasure elements. Yet, I rarely find surveillance being given serious consideration. I have reviewed countless countermeasure programs that never mention surveillance. An understanding of surveillance is especially important for terrorist act prevention.

The Surveillance Matrix lists the assets by category from previous matrices and the various elements of surveillance in columns, including:

- Fixed visual surveillance opportunities
- Off-site mobile visual surveillance opportunities
- Acoustic eavesdropping opportunities
- Electronic surveillance opportunities
- Information technology (IT) system surveillance opportunities
- Opportunities for interception of documents and information
- The Vulnerability Matrix combines the results of the Surveillance Matrix with the other factors listed above to create a composite picture of overall target (asset) vulnerability. The results of this matrix are also used in the CARVER+Shock Matrix, the KSM Asset Target Value for Terrorism Events Matrix, and the Risk Summary Matrix. This is done by referencing the vulnerability cells of those matrices to the comparable “Score” cell of the Vulnerability Matrix. In this fashion, the vulnerability data are computed automatically into the other matrices.

Consequence Components

The three legs of risk comprise probability, vulnerability, and consequences. But often, consequences are not fully studied. There are several dimensions to consequences as there are to other factors we studied. The consequence factors are estimated using the Criticality and Consequence Matrix, the factors for which are listed below:

- *Criticality to Business Operations:* How critical is the asset in question to the mission of the organization? Is the asset truly critical, or does it serve a supporting role that could be replaced in part or in whole by other resources? Score 1 to 10, 10 being absolutely critical, such that the mission could not be carried out without the presence of this asset.
- *Casualties:* Could an attack result in casualties? If so, how severe could casualties be? Would it result in mass casualties or perhaps just a single injury? Score for severity 1 to 10, 10 being large numbers of mass casualties and 1 being a single injury.
- *Loss of Property:* Could property be lost in an attack on this asset? If so, how severe could that be? Would the severity be as much as the loss of an entire campus (such as the attack on the World Trade Center in 2001) or just on a single asset such as a computer workstation? Score for severity 1 to 10, 10 being the loss of many buildings or much property of very high value.
- *Loss of Production:* Could an attack result in loss of production or loss of support operations to the mission of the organization? If so, how severe could that loss be? Score 1 to 10, 10 being the worst such as total unrecoverable loss of operations resulting in the permanent collapse of the organization and 1 being very minor disruption for a short period of time such as a few days.
- *Loss of Proprietary Information:* Could an attack result in the loss of proprietary information? If so, how severe could that loss be? Score 1 to 10, 10 being worst, such as total exposure of mission-critical information such as strategic product development that would permit competitors to gain a significant advantage.
- *Loss of Business Reputation:* Could an attack result in loss or exposure of highly sensitive information, which if released out of context could result in unrecoverable loss of business reputation (such as the complete private financial data of all customers of a financial institution), or in other ways damage the good business reputation of an organization? Score 1 to 10, 10 being worst.

Risk Formulas

Risk calculation is a two-step process. The basic formula combines probability, vulnerability, and consequences to determine unranked risk. That is, it is possible to have an asset for which probable events are highly likely and which is relatively highly vulnerable, but for which the consequences are quite low. This could score highly on risk and yield a possible misrepresentation of overall risk.

To mitigate this result, use a second step that ranks the final risk results by order of consequences. This assures that the final risk rankings are relevant to the consequences so that budgets for countermeasures are allocated by consequences rather than by probability or vulnerability. There are also other methods that may be appropriate for certain projects that are discussed in Chapter 11.

Risk Results (Unranked)

Finally, we have arrived at the risk calculation stage. The Risk Calculation Matrix follows the form of most previous matrices. That is, all relevant assets (targets and VIP-public/threat actor nexus locations) are listed as rows, and the columns will include the scores of three other matrices:

Mega Towers					
Risk Calculation Worksheet (Unsorted)					
Targets	Probability	Vulnerability	Consequences	Score	Rank
People	7	5	4	5	3
VIP Executives and VIP Visitors	6	4	4	5	24
Employees	8	7	6	7	2
Contractors	6	4	4	5	29
Visitors	7	6	5	6	12
Delivery Personnel	6	4	2	4	39
Transportation Personnel	6	4	2	4	39
Property	5	6	3	5	4
Site	5	6	4	5	21
VIP Drop-Off	7	6	5	6	10
Employee Drop-Off	8	8	7	8	1
Visitor Drop-Off — Hotel (South)	7	9	5	7	4
Main South Entry Gatehouse Area	6	8	3	6	9
North Perimeter Fence	4	4	3	4	46
East Perimeter Fence	4	4	3	4	43
South Perimeter Fence	4	4	3	4	43

FIGURE 10.8 Unranked Risk Results

1. Vulnerability Matrix
2. Probability Summary Matrix
3. Consequences Matrix

To score the Unranked Risk Matrix (Figure 10.8), one can multiply probability by vulnerability by consequences to achieve a score, or one can use “(Probability + Vulnerability + Consequences)/3” as a score. Both will yield roughly similar results. Regardless of which is used, the final ranking by consequences will generally assure that they are all sorted correctly for countermeasure budget allocation.

It is often useful to create two unranked risk results models (one for terrorism and a separate one for criminal risks). These are combined for simplification of the illustrations in this book.

In the next chapter, we will look at how to rank the risk results for more meaningful evaluation and especially how to create the V² Matrices that will help illustrate risk to decision makers. The V² Matrices are one of the most valuable tools in helping decision makers reach consensus on how to best budget to protect the organization.

SUMMARY

The better DHS-approved methodologies have the same two things in common:

1. They all use the elements of probability, vulnerability, and consequence.
2. They all result in comparatively similar findings, even considering the differences in the formulas and approaches.

The key to the approval by DHS appears to be that the ranking of risks should be similar, not that the formulas result in exactly the same numbers. *It is the mathematical relationship, not the mathematical result, that is important.*

DISPLAYING RISK FORMULA RESULTS

In the API/NPRA methodology, the formula is expressed as a matrix of probability and vulnerability (two dimensions), and then ranked later by consequences. This can be shown in a nonabstract way in one spreadsheet. By showing probability in columns, vulnerability in rows, and consequences in three levels with different text **Bold** = High, *Italics* = Medium, and Standard Text = Low, all the elements can be shown in one simple spreadsheet.

The Complete Risk Analysis Process

The steps shown herein meet or exceed all risk analysis methodologies except for the deep Sandia model, which is too excessive in its depth for most commercial applications.

The results that will be achieved include:

- Step-by-step spreadsheet process to risk results
- Results can be expressed either in numbers or graphically
- Prioritization of risk results, which will be illustrated in Chapter 11

The process includes the following:

- Step through the calculation by first determining what types of threat actors constitute a threat to the facility in question.
- Review probability (the aspects of the facility which make it a likely target for the different threat actors).
- Review the facility's vulnerability (the aspects of the facility that could be exploited by a threat actor).
- Finally, review consequences. Risk occurs only if there are consequences to the action, and the more significant the consequences are, the greater is the risk. Risk should also be prioritized by consequences.
- Prioritize the risk by consequences.

Prioritizing Risk

INTRODUCTION

Every organization must prioritize their security budgets. Determining exactly how to do this has caused security directors, managers, and C-level executives more grief than almost anything else about security. Arguments ensue as different stakeholders jockey to forward their agendas. And agendas abound. Various departments have their interests and often compete with security for the same budget.

First, understand that prioritization is all about developing budget and determining the schedule for implementation. As this subject is discussed, remember the purpose — prioritization is the first step. The second step is getting budget commitment and scheduling the implementations. The first is a requirement for the second, and the second will not be successful without the first.

Two skills become paramount:

1. Prioritizing risk.
2. Communicating priorities effectively to management to gain their support.

In this chapter, you will:

- Learn five common ways to prioritize risk, including the best practices method, which is prioritization by consequences.
- Learn how to formulate arguments to gain consensus on budget priorities.

PRIORITIZATION CRITERIA

There are five potential ways to prioritize risk. By request of colleagues, these are all discussed, but it is my opinion that the only correct way to prioritize risk is to sort the fundamental risk analysis on consequences. The complete list of approaches includes the following:

1. Natural Prioritization (Prioritizing by Formula)
2. Prioritization by Probability
3. Prioritization by Consequences
4. Prioritization by Criticality
5. Prioritization by Cost (Not Recommended)

NATURAL PRIORITIZATION (PRIORITIZING BY FORMULA)

Both the Sandia formula and the American Petroleum Institute/National Petrochemical and Refiners Association (API/NPRA) formula facilitate intrinsic prioritization. For Sandia, the formula is: Risk = Probability * (1–Vulnerability) * Consequence. For API/NPRA, the formula is: Risk = Probability * Vulnerability * Consequence, or (Probability + Vulnerability + Consequence)/3.

These formulas will result in perfectly actionable results. However, this can sometimes result in items of very high vulnerability and very high probability but very low consequence rising to the top of the risk chart. The analyst can further prioritize the results in order to focus and guide the implementation process. Different organizations place different emphasis on each element. For example, a good security program is composed of two main elements:

1. A baseline security program (focused on day-to-day risks and reinforcing good behavior)
2. Special countermeasures to address unique vulnerabilities (usually focused on terrorism, or a criminal problem that may be unique to the area, industry, or facility)

The baseline security program is a comprehensive program of elements that deter, detect, delay, respond, and collect evidence, intended primarily to reduce the overall probability of occurrence. Such programs include a full complement of countermeasures, including hi-tech, lo-tech, and no-tech countermeasures. These are woven into a comprehensive security program that addresses all of the day-to-day risks and known criminal risks (economic crime, violent crime, and petty crimes). Similar to an organization's accounting effort, marketing program, or research and development program, the baseline security program should be developed.

Special countermeasures are focused on dealing either with threats of terrorism or with criminal activity that is unique to the area, property, or industry. Certain industries, such as transport or depot firms, have known risks that are unique to their industry (transport — hijackings, depot — smuggling). And some areas or properties may have regional problems that are unique (vandalism, gang activity, remote dark parking lots, etc.). (Refer to the example of special countermeasures in Chapter 13.)

The extent of the baseline security program and of special countermeasures to address unique vulnerabilities may be driven by probability, consequences, criticalities, or cost.

PRIORITIZATION OF RISK

Often organizations place different emphasis on prioritization, depending on their circumstances. For example, organizations that face little risk of terrorism but which are located in a high-crime area often want their risk prioritized by probability, while critical infrastructure facilities should address risks by consequences.

Two other ways to prioritize risk are criticality and cost. These are not recommended because criticality is an incomplete and arguably poor surrogate for consequences, and cost should be examined after either probability or consequences prioritization is addressed. Those organizations that address cost as a primary priority completely miss the point of the exercise. A security program may be “boxed” into a budget, but threat actors will not be. Therefore, the security program that is built to a budget as a first priority is doomed to fail at its inception.

Security programs that are prioritized by criticalities also miss the point. Criticalities and consequences do not necessarily go hand in hand. A program may be critical to the operation of the organization, but may pose a small risk of consequences. For example, the accounting program (a critical asset) is so easily backed up, that although it is very high on the criticality list, its loss is almost certain not to occur. Thus, prioritizing countermeasures to further protect the information is a waste of monies. However, a “red carpet area” at an entertainment complex may be low in criticality, but the consequences of a suicide bomber making a political statement at a red carpet event could have drastic consequences for the organization’s business reputation.

Prioritizing by Probability

To prioritize risk by probability, one would first organize risk by formula and then sort the risks by probability. Using the spreadsheet model discussed herein, one would simply use the probability column of the Risk Analysis Matrix to sort the entire array. This will result in a comprehensive listing of risk to targets, sorted by probability.

Prioritizing by Consequences

To prioritize risk by consequences, one would first organize risk by formula and then sort the risks by the ranking of consequences. Using the spreadsheet model discussed herein, one would simply use the consequences column of the Risk Analysis Matrix to sort the entire array. This will result in a comprehensive listing of risk to targets, sorted by consequences.

Prioritizing by Criticality

To prioritize risk by criticality, one would first organize risk by formula and then sort the risks by criticality. You can do this by creating a new spreadsheet using the raw risk analysis spreadsheet as a template and then adding a column for criticality from the Criticality and Consequences Matrix. Then sort the whole array by criticality.

Prioritizing by Cost

There are two ways to prioritize by cost. One is simple and direct, and the other is more scientific.

1. *Simple Cost Prioritization:* To prioritize by cost in the simple manner, one would develop risk by formula and then develop a list of security countermeasures. After budgeting the total list of countermeasures, one would consider cost reductions to a target number based on how those countermeasures relate to the highest risks. That is, for example, one might consider an access control reader to an entire department rather than to individual doors in the department. Both approaches address the risk of unwanted visitors, but one does so at much lower cost.
2. *Process-Driven Cost Prioritization:* In the more process-driven approach to prioritize the risk by cost, one would first organize the risk by formula and then add a column for vulnerabilities with a row under each risk for each threat scenario relating to each risk. For each vulnerability, develop a list of countermeasures that address the vulnerability. Countermeasures may include those that control access, detect, assess, delay, assist in response, or collect evidence. Each of these will have a cost associated with it and a rating for effectiveness. Chapters 18 and 19 will explain the process of security effectiveness metrics and cost-effectiveness metrics usage.

COMMUNICATING PRIORITIES EFFECTIVELY

Making the Case

Virtually every organization is under financial challenges. Understanding that many program directors are vying for the same budget dollars, it is necessary for the security program manager to make a clear case for security program budget dollars.

I often say that accounting and security programs have much in common. They both are required to comply with codes and regulations and limit the organization's exposure to risks (in one case, financial risk, and in the other, security risks).

But accounting organizations make a far better case for their needs and successes than do most security organizations. We can change that. The very process of developing a comprehensive risk analysis will go a long way toward making the case. Though many may read no more than the executive summary, it should include a summary paragraph of each section and graphics illustrating the risk summary. The proposed countermeasure budget should be based on a comprehensive solution with a caveat that it can be adjusted to accommodate implementation phasing.

- Developing the Arguments
 - *Determine the priorities of management:* This simple but often overlooked item is essential to targeting management's interests in budgeting arguments. Priorities can be determined from annual statements, memos issued by management to employees, and by directly asking executive management to outline their priorities for the next fiscal year in an e-mail. They will appreciate your interest.
 - *Identify points of view of stakeholders and acknowledge them:* For the security program to get its own share of the overall budget, you will have to contend with other organization stakeholders who have their own priorities and agendas. By understanding these, you can make the case for security program countermeasures in the context of all these other competing agendas. By preparing the argument in this context, and acknowledging the points of view,

all of which need executive management's attention, you are more likely to succeed than if the argument is made in the absence of this information. This helps executive management to place the security program in the context of the overall organization's needs. This is one of the most important elements of a successful presentation.

- *Provide a list of consequences:* The only reason to have a security program is to prevent the undesired consequences of not having a security program. This is what risk analysis is all about. By identifying all risks and consequences, executive management can develop the priorities of its budget. It is useful to create a comprehensive list of consequences and pose the question to executive management as to which of the consequences would be acceptable losses. This is not a rhetorical question, and it is not intended to provoke management. It is a logical question directly related to prioritizing budgets. Remember, all risks can be dealt with in one of several ways:

- You can accept the loss.
- You can duplicate the asset.
- You can insure the asset (transfer the risk).
- You can protect the asset.

Executive management needs to make these decisions about all assets, and this list gives it the tools to do so.

- *Provide tiered countermeasure budgets versus solutions:* Chapter 17 — “Countermeasure Selection and Budgeting Tools,” Chapter 18 — “Security Effectiveness Metrics,” and Chapter 19 — “Cost-Effectiveness Metrics,” will assist in preparing a workable tiered plan. The tiered plan should present achievable goals versus budgets and explain clearly what cannot be achieved (what risks will be accepted) for deferred budgets. Chapter 18 includes a spreadsheet tool (the Decision Matrix) that helps present what can and cannot be achieved with various budget options. Management needs to understand what risks they are accepting for budgets that they defer or program elements they decide not to budget.
- *Let management draw its own conclusions.*
- *Use a Decision Matrix:* Use a Decision Matrix to help committees reach a consensus when there is no agreement on the choice of a particular approach. Chapter 17 explains and illustrates the use of the Decision Matrix.

BEST PRACTICES RANKING RISK RESULTS

To achieve the final risk rankings, we simply copy the Unsorted Risk Summary Matrix and perform a sort on the Consequences column so that the results descend from the highest consequence targets to the lowest.

Finally, we have truly meaningful results on which the allocation of countermeasures can be based. However, there is one more final step to complete the analysis. We will make it ready for presentation to decision makers. Most decision makers have a basic understanding of risk. However, for a large facility, particularly a campus of buildings, a proper risk analysis can easily generate over 10,000 individual points of analysis (each cell on each matrix). This can be a mind-numbing amount of data to consider. Even the Ranked Risk Analysis Matrix for some projects I completed has contained an astonishing 1,200-plus points of analysis, and even a modest project can result in a Ranked Risk

Analysis Matrix of over 300 points of analysis. This is just too much data for decision makers to process quickly. The result is all too often that poor decisions can result by “deferring decisions till we can fully consider this,” to simply asking for a more readily digestible form of the data. That is what the V² Matrices were designed to accomplish.

Displaying the Ranked Results as a Visual Graphic

The V² Matrix in its simplest form assembles the data from the ranked risk results into a color-coded graphic form that is easily digestible by nontechnical decision makers (see Figure 11.1). In its most complex form, it creates the ability for decision makers to “drill-down” into the data to see detail behind the recommendations.

The V² Matrices typically include a Summary Matrix (matrix of risk rankings by building) and Detail Matrices (matrices for each individual building or area).

To create the Summary Matrix, go back to the Unsorted Risk Matrix and select the major headers from that matrix. These will include people, property, proprietary information, and business reputation. Also include minor headers for each area of the property within the facility, such as tower 1, tower 2, hotel, parking, site, and so forth.

From that information, looking at the Unsorted Risk Matrix and at an empty V² Matrix, place the first header (people) into the cell related to its score for vulnerability and probability, based upon the colors of the cell. If probability is medium and vulnerability is high, place people into the medium probability/high vulnerability cell. Then

Mega Towers					
Risk Sorted Worksheet					
Targets	Probability	Vulnerability	Consequences	Score	Rank
	People	7	5	4	5
Employees	8	7	6	7	2
Visitors	7	6	5	6	12
VIP Executives and VIP Visitors	6	4	4	5	24
Contractors	6	4	4	5	29
Delivery Personnel	6	4	2	4	39
Transportation Personnel	6	4	2	4	39
<hr/>					
Property	5	6	3	5	4
Site	5	6	4	5	21
Employee Drop-Off	8	8	7	8	1
VIP Drop-Off	7	6	5	6	10
Visitor Drop-Off – Hotel (South)	7	9	5	7	4
Hotel East Entrance	6	8	5	6	6
Hotel West Entrance	6	8	5	6	6
North Perimeter Freight Fence	6	5	5	5	20

FIGURE 11.1 Sorted Risk Results

Facility Name			
	Asset Target Value (Probability)		
Vulnerability	High Medium Low	Medium Medium ATV and High Vulnerability Medium ATV and Medium Vulnerability Medium ATV and Low Vulnerability	Low Low ATV and High Vulnerability Low ATV and Medium Vulnerability Low ATV and Low Vulnerability
High	<i>Most Consequence Assets are Bold/Italics</i> <i>Medium Consequences Assets shown in Italics</i> Last Consequences Assets are shown Normally		
Medium	High ATV and Medium Vulnerability	Medium ATV and Medium Vulnerability	Low ATV and Medium Vulnerability
Low	High ATV and Low Vulnerability	Medium ATV and Low Vulnerability	Low ATV and Low Vulnerability

FIGURE 11.2 V² Summary Matrix (ATV Stands for Asset Target Value)

code the font for the word “People” as “Normal Text,” “*Italics Text*,” or “**Bold Text**,” depending on whether its consequence rating is low, medium, or high. Do this for each major heading, and you will have a graphical array that lists the information in three dimensions: X for probability, Y for vulnerability, and consequence shown as different text types. This provides a very easily digestible summary of the overall risk rankings.

Even though the V² Summary Matrix (Figure 11.2) is good at providing an overall picture of risk for the entire project, it is not granular enough to make budgeting decisions based on it. For that, we need to create a separate V² matrix for each subarea, including:

- People
- Each individual property area (building, remote site, etc.)
- Proprietary information
- Business reputation

Together, these provide the reviewer with a drill-down look at risk rankings. Therefore, tower 1 may be listed on the V² Summary Matrix, and there will also be an individual V² Matrix labeled tower 1 (with its areas also arrayed), and so forth for all of the assets of the facility.

This approach provides a comprehensive analysis and results in exceptionally understandable summaries.

SUMMARY

Every organization must prioritize their security budgets. Prioritization is all about developing a budget and determining the schedule for implementation. Two skills are paramount:

1. Prioritizing risk
2. Communicating priorities effectively to management to gain their support

Prioritization Criteria

There are five potential ways of prioritizing risk. However the best way to prioritize risk is by sorting the fundamental risk analysis on consequences.

Natural Prioritization (Prioritizing by Formula)

Both the Sandia formula and the API/NPRA formula facilitate intrinsic prioritization. For Sandia, the formula is: Risk = Probability * (1-Vulnerability) * Consequence. For API/NPRA, the formula is: Risk = Probability * Vulnerability * Consequence, or (Probability + Vulnerability + Consequence)/3.

All three of these formulas will result in perfectly actionable results by themselves. However, this can sometimes result in items of very high vulnerability and very high probability but very low consequence rising to the top of the risk chart. Different organizations place different emphasis on each element.

A good security program is composed of two main elements:

1. A baseline security program (focused on day-to-day risks and reinforcing good behavior)
2. Special countermeasures to address unique vulnerabilities (usually focused on terrorism, or a criminal problem that may be unique to the area, industry, or facility)

The extent of the baseline security program and of special countermeasures to address unique vulnerabilities may be driven by probability, consequences, criticalities, or cost.

Communicating Priorities Effectively

Making the Case

Virtually every organization is under financial challenges. Understanding that many program directors are vying for the same budget dollars, it is necessary for the security program manager to make a clear case for security program budget dollars.

- Developing the Arguments
 - Determine the priorities of management.
 - Identify points of view of stakeholders and acknowledge them.
 - Provide a list of consequences.
 - Provide tiered countermeasure budgets versus solutions.
 - Let management draw their own conclusions.
 - Use a Decision Matrix to help committees reach a consensus when there is no agreement on the choice of a particular approach.

Best Practices — Ranking Risk Results

To achieve the final risk rankings, we simply copy the Unsorted Risk Summary Matrix and perform a sort on the Consequences column so that the results descend from the highest consequence assets to the lowest.

Displaying the Ranked Results as a Visual Graphic

The V² Matrix assembles the data from the ranked risk results into a color-coded graphic form that is easily digestible by nontechnical decision makers. By using the V² Matrix on each facility and then summing that to the entire project creates the ability for decision makers to “drill-down” into the data to see detail behind the recommendations.

The V² Matrices typically include a Summary Matrix (matrix of risk rankings by building) and Detail Matrices (matrix for each individual building or area).

The Summary Matrix is created by using the Unsorted Risk Matrix and the major headers from that matrix (people, property, proprietary information, and business reputation). The matrix should also include minor headers for each area of the property within the facility, such as tower 1, tower 2, hotel, parking, site, and so forth.

MAKING THE V² MATRIX

Reviewing the Unsorted Risk Matrix and at an empty V² Matrix, place the first header (people) into the cell related to its Score for vulnerability and probability, based upon the colors of the cell. If the probability is medium and the vulnerability is high, place people into the medium probability/high vulnerability cell. Then code the font for the word “People” as “Normal Text,” “*Italics Text*,” or “**Bold Text**,” depending on whether its consequence rating is low, medium, or high. Do this for each major heading and you will have a graphical array that lists the information in three dimensions: X for probability, Y for vulnerability, and consequence shown as different text types. This provides an easily digestible summary of the overall risk rankings.

While the V² Summary Matrix is capable of providing an overall picture of risk for the entire project, it is not granular enough to make budgeting decisions. For that, we need to create a separate V² Matrix for each subarea, including:

- People
- Each individual property area (building, remote site, etc.)
- Proprietary information
- Business reputation

Together, these provide the reviewer with a drill-down look at the risk rankings. So, tower 1 may be listed on the V² Summary Matrix and there will also be an individual V² Matrix labeled tower 1 (with its areas also arrayed), for all of the assets of the facility. This approach provides a comprehensive analysis and results in exceptionally understandable summaries.

SECTION

II

Policy Development before Countermeasures

Security Policy Introduction

INTRODUCTION

At the completion of this chapter, you will understand the role that security policies have in the development of all aspects of a security program; what the differences are between policies, standards, guidelines, and procedures; and why security policies should be developed before decisions on other countermeasures are finalized. This is the first of three chapters dealing exclusively with security policies, which emphasizes the importance of the role of security policies in the overall security program.

THE HIERARCHY OF SECURITY PROGRAM DEVELOPMENT

Many years ago, I wrote an article for a security technology magazine titled “How to Plan, Design and Implement a Bad Security System.” The focus of the article was that most security systems have no design but are, in fact, a scattering of cameras, card readers, and alarms with no coherent purpose, serving no set of security policies.

It is easy to create a bad security program. It takes no planning. In fact, the lack of planning virtually guarantees a bad security program. There are several steps that, if taken, can also virtually guarantee a good security program. These steps are as follows:

- Perform a competent risk assessment
 - Identify threats
 - Identify vulnerabilities
 - Identify consequences
 - Calculate and prioritize risks
- Identify appropriate countermeasures
 - Outline security policies (goals and objectives)
 - Develop a security plan that should include the following:
 - A baseline security program
 - Detailed security policies and procedures
 - All other countermeasures derived from policies and procedures
 - Special countermeasures to address unique vulnerabilities
- Apply the countermeasures in conformance with the security policies
- Measure the security program performance against the security policies (security metrics)



FIGURE 12.1 Policies Form the Basis for Problem Solving

WHAT ARE POLICIES, STANDARDS, GUIDELINES, AND PROCEDURES?*

A policy is a very brief high-level statement that states the organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area (Figure 12.1). A policy should state a problem or objective and outline a plan of action to mitigate the problem.

Policy attributes include the following:

- Compliance is required (mandatory).
- Failure to comply results in disciplinary action.
- Focus is on desired results, not on means of implementation.
- Policy is further defined by standards and guidelines.

Policies always state required actions and may include pointers to standards and guidelines.

- *Policies require compliance (mandatory):* This is the most basic fact differentiating policies and guidelines. Guidelines are general in nature and provide for exceptions to be determined by the person interpreting the guideline. That is, a person can judge for him- or herself whether or not conditions are right for following a guideline, but no such judgment can be made regarding policies. Policies do not allow for exceptions of personal judgment.
- *Failure to comply with a policy results in disciplinary action:* Policies are not only mandatory, but they have provisions for disciplinary action if they are not followed. Each policy should state the disciplinary action (loss of job, loss of position, financial penalty, loss of parking privilege, negative comment in personnel file affecting raise evaluation, etc.). One of the easiest ways to determine if a statement is a policy is to ask what is the disciplinary action corresponding to the policy.

* The introduction section and some other portions are resourced from SANS Institute and Cisco Systems (www.sans.org/resources/policies/policy_primer.pdf).

- *Policies should focus on desired results, not on means of implementation:* Each security policy should state a problem and the desired result. Means of implementation should be left to countermeasures, which may include technological solutions, signage, architectural or landscaping solutions, or procedures.
- *Policies may be further defined by standards and guidelines:* Standards and guidelines amplify policies to make them more clear and understandable. For example, a standard may expand on an aspect of a policy to explain it further and break it down into its component parts. Guidelines may give a framework for implementation and should “guide” the user to better understand how to conform to the policy.

Most policies are supported by procedures. Procedures define “how” to implement a policy. Procedures may be rules for action directed either to the security unit or the organization’s users. Procedures are more specific than guidelines, which allow for the user’s interpretation. Procedures define what a person must do to comply with a policy. Procedures may also be implemented as guidelines.

Other Key Documents

Standards, guidelines, procedures, position papers, and guiding principles play a role in defining the overall security program. A brief explanation of each follows:

- Standards
 - Standards are a mandatory action or rule, designed to support and conform to a specific policy.
 - A standard should make a policy more meaningful and effective.
 - A standard must include one or more accepted specifications for hardware, software, or behavior.
- Guidelines
 - Guidelines are general statements, recommendations, or administrative instructions designed to achieve the policy’s objectives by providing a framework within which to implement procedures.
 - A guideline can change as needed based upon the environment and should be reviewed more frequently than standards and policies.
 - A guideline is not mandatory, rather it is a suggestion of a best practice. Hence, “guidelines” and “best practice” are in some ways interchangeable.
 - Guidelines help convey “best practices” to users.
 - Guidelines are meant to “guide” users to adopt behaviors that increase the security posture of the organization but which are not as yet required.
 - Guidelines may be used as a “trial balloon” before instituting the guideline as a policy.
- Procedures
 - Procedures are statements of actions required by users in order to assure conformance to policy.
 - Procedures define “how” to carry out policies or are the mechanisms to enforce policy.
 - Procedures help eliminate the problem of a single point of failure (e.g., an employee suddenly leaves or is unavailable when most needed).

- Procedures, unlike guidelines, are mandatory.
- Procedures are equally important to policies. For example, a badging policy would require the use of photo ID badges at a facility. The badging procedure would describe the process for creating new photo ID badges, distributing them, maintaining them, and collecting them when an employee or contractor leaves.
- There is not always a one-to-one relationship between policies and procedures.
- Position Paper
 - A position paper describes the security unit management's position on emerging issues and technologies.
 - Position papers often act as a precursor to policy.
 - Position papers may be used where a policy may never be developed.
 - Position papers can also fill the gap between policies and guidelines.
- Guiding Principles
 - These are statements of philosophy, direction, or beliefs of the organization.
 - Guiding principles serve to "guide" people in making the right decisions in the organization's interests, including:
 - What policies and standards are needed
 - What technologies are appropriate
 - How goals should be accomplished
 - Guiding principles are not policies but serve to help management form thoughtful and comprehensive security policies and procedures.
 - Highest-level guiding principles
 - Security unit will embody integrity.
 - Security unit will be available when needed.
 - Everyone is responsible for security, especially department managers.
 - Limit access to the facilities only to those persons who are authorized.
 - Limit risk to the organization through cost-effective risk mitigation.
 - Security measures should be proactively implemented.
 - Security should be propelled through security awareness.
 - Information technology security and physical security should work together to create a more secure environment for people, property, proprietary information, and the organization's business reputation.
 - Wherever possible, the security unit should use technology rather than personnel to grant access, except where direct interaction with the user is compelled by access control requirements (vehicle, weapons and explosives screening, visitor and employee badging, etc.).

The Key Role in Policies in the Overall Security Program

Policies Define All Other Countermeasures

A good set of policies will define all security program countermeasures. Any countermeasure that is not supported by a security policy is an indication of either of the following:

- A poorly conceived countermeasure
- A missing policy

In the first case, there is no need for the countermeasure, and its presence may actually be detrimental to the goal of good security. Some countermeasures are put in place to address temporary problems and then become accidentally permanent.

In the second case, where the case for the countermeasure is obvious, and there is no supporting policy, it indicates that policies have not been fully considered and should be revised to include the case for this countermeasure.

Under every circumstance, every countermeasure should be supported by an underlying security policy. This is important for the following reasons:

- Defending against Legal Challenges
- Defending against Challenges by Users

Legal Challenges

In the case of a lawsuit, it is common for plaintiff's attorneys to examine the security countermeasures and their basis in law or security policies. Where countermeasures exist in one part of a facility that might have mitigated a security event in another part of the organization's facilities, a skillful attorney can make a compelling case that the use of the countermeasure could have mitigated the plaintiff's injuries and that the application of a countermeasure in one part of a facility indicated the organization's awareness of the need for the countermeasure. And the fact that the countermeasure was not uniformly applied indicates negligence on the part of the organization's management. Thus, the absence of a security policy for a countermeasure can create the conditions under which an organization can be successfully sued, where a security event occurs elsewhere that might have been mitigated by the presence of a countermeasure that was not applied because there was a missing policy.

Challenges by Users

It is common for users to challenge applications of security procedures and technical countermeasures such as cameras. The ability to cite an underlying security policy obviates any complaint about a security procedure or countermeasure. For the persistent complainer, a security officer can cite not only the policy, but also the disciplinary action that will result in noncompliance with the policy. This is an effective means of achieving compliance. Thus, the occasional complainer can actually serve to underscore compliance for any bystanders who hear the exchange between the complainer and the security officer.

There is another category of complainer that this approach is especially effective in dealing with, one who is particularly difficult to deal with — the organization manager who complains loudly and publicly about a security procedure in the presence of other users. This complainer can be intimidating to security officers, and that is his intent. He is intending on creating a special exception to policy for him alone, whether it be permission to park in an area where there is a concern about vehicle-borne improvised explosive devices (VBIEDs), or checking bags at a screening point. The loud manager is a direct challenge not only to the security officer, but also to security management and moreover to the mission of security of the organization. Such challenges must be dealt with effectively. The ability of the security officer to quote security policy by policy number and text can effectively put down such challenges. Every officer should be drilled in policy until he or she knows each without reference to paper. This is part of basic

training. In the few cases where a manager continues to challenge the security officer after policy is quoted, the case should be referred to the security unit chief.

It is not uncommon for such managers to fabricate claims of misbehavior by the security officer's interaction with the manager at the checkpoint. I recommend that all security checkpoints be observed and recorded for both video and audio in order to provide supporting evidence of the security officer's appropriate behavior, as it is common to see claims of misbehavior by security officers by policy challengers. When the manager's superiors are presented with the audio or video evidence of a manager's misbehavior after his claim of a security officer's misbehavior, the manager's claim not only dissolves into vapor, but any future claims are also rendered suspicious. The manager moves suddenly from a position of assumed correctness to a position of having to defend his own inexcusable actions. Such video is best presented to his superiors in the presence of the manager, as the effect of his retreat when faced by evidence of his own behavior is that much more pronounced. After one such occurrence, the word gets out to other managers that such behavior at a security checkpoint can be counterproductive to their careers.

Benefits to Having Proper Policies

There are numerous benefits to having well-defined security policies. The list below is a summary of the key reasons:

- Policies dictate a uniform standard of behavior for all, including users and security staff. No one is exempt — not visitors, not managers, not ordinary users, and not security staff.
- Policies provide a basis for enforcement. If there is no policy against a behavior, then there is no misbehavior. An organization can only prohibit behavior that is proscribed by a policy.
- Policies exemplify the organization's commitment to security. The fact that an organization has taken the time and consideration to create policies regarding security illustrates that organization's management's position on security. That organization takes security seriously and has well-considered policies on security.
- Policies provide a benchmark for measurement (and a basis for security management metrics). Policies are the basis against which all behaviors having to do with security are compared. Additionally, security policies provide the basis for judging the effectiveness of the security organization, and its management. The security organization that does not achieve policy compliance is not by any measure effective.
- Policies help provide consistency across business units and facilities and eliminate variances of interpretation by security staff. One of the most important aspects of any security program is its ability to uniformly apply security policy across all business units and facilities, and equally for management, employees, contractors, vendors, and visitors. The existence of uniform security policies helps assure uniform compliance. This improves security and business productivity and, very importantly, reduces the chance for litigation due to nonuniform application of security principles between facilities or business units.

- Policies give the security staff the backing of management. Because policies derive from a process that finalizes with senior management authorization, each policy has the backing of the organization's senior management.
- Provide a basis for training. Security management, supervisors, and officers all need basic and continuous training in order to define and constantly improve their skills. Security policies provide the basis for all training.
- Policies provide a basis for counseling security officers on their performance. A security officer's performance can be judged against the policies regarding their training; moral, ethical, and professional behavior; and enforcement of the security policies.

Control Factors

- Business culture must play a major role in the development of security policies. Any security program that does not take an organization's business culture into account is doomed to fail. Users will complain, revolt, and find ways around security policies that do not fit their understanding of the organization's business culture.
- Security policies must balance security control with business productivity. One major cause for the failure of some security policies is that they are conceived in the absence of consideration for business productivity. Users will always find ways to circumvent policies that impede on their ability to do their job or come and go in the performance of their job. All policies should take the possible effects on business operation's effectiveness as one of their first considerations.
- Policies that are too restrictive will be circumvented, thus obviating the intent and effect of the policy. As above, policies that are too restrictive will also undermine the entire security program. When users succeed in circumventing one policy, all other policies suffer. When the security organization fails to enforce one policy, it is easy for users to cite that example as a reason why they should not be compelled to obey other policies. For this reason, it is important to review security policy compliance continuously and make changes to any policies that are so restrictive that they are unenforceable, impede normal business conduct, or defy the organization's business culture. Often, well-intentioned policies turn out to be white elephants that must be modified or shed due to unenforceability.
- Technical controls are not always possible, and therefore, personal intervention must be planned and implemented with effective training. Generally, technical controls are better than controls that rely on security staff for the following reasons:
 - Technical controls cost less to operate, especially when many control points are needed.
 - Technical controls cannot be accused of bias or preference of one user over another.
 - Technical controls are generally well accepted, as users understand that arguing with a card reader, barrier gate, electronic turnstile, or revolving door is fruitless.

Where it is necessary to use security staffing due to the need for directions, a decision process, personal verification, to enroll visitors or to present a "face" to visitors, it is important to plan and implement the control point and train the security staff in their duties well enough to assure the success of the control point.

SUMMARY

The Hierarchy of Security Program Development

These steps virtually guarantee a good security program:

- Perform a competent risk assessment
 - Identify threats
 - Identify vulnerabilities
 - Identify and prioritize risks
- Identify appropriate countermeasures
 - Outline security policies
 - Baseline security program
 - Detailed security policies and procedures
 - All other countermeasures derived from policies and procedures
 - Develop special countermeasures to address unique vulnerabilities
- Apply the countermeasures in conformance with the security policies
- Measure the security program performance against the security policies

Policies, Standards, Guidelines, and Procedures*

A policy is a very brief high-level statement that states the organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. A policy should state a problem or objective and outline a plan of action to mitigate the problem. Policies always state required actions and may include pointers to standards and guidelines. Standards, guidelines, procedures, position papers, and guiding principles all play a role in defining the overall security program.

The Key Role in Policies in the Overall Security Program

Policies define all other countermeasures. A good set of policies will define all security program countermeasures. Under every circumstance, every countermeasure should be supported by an underlying security policy in order to defend against legal challenges and challenges by users. Benefits to having well-defined security policies include:

- Policies dictate a uniform standard of behavior for all, including users and security staff alike.
- Policies provide a basis for enforcement.
- Policies exemplify the organization's commitment to security.
- Policies provide a benchmark for measurement (and a basis for security management metrics).
- Policies help provide consistency across business units and facilities and eliminate variances of interpretation by security staff.

* The introduction section and some other portions are resourced from Sans Institute and Cisco Systems (www.sans.org/resources/policies/policy_primer.pdf).

- Policies give the security staff the backing of management.
- Policies provide a basis for training.
- Policies provide a basis for counseling security officers on their performance.

Control Factors

- Business culture must play a major role in the development of security policies.
- Security policies must balance security control with business productivity.
- Policies that are too restrictive will be circumvented, thus obviating the intent and effect of the policy.
- Technical controls are not always possible, and therefore, personal intervention must be planned and implemented with effective training.

CHAPTER 13

Security Policy and Countermeasure Goals

INTRODUCTION

At the completion of this chapter, you will understand why security programs that are not based on security policies are so likely to fail, the role of policies in the security program, the role of countermeasures in the security program, the types of security countermeasures, why policies should be developed before countermeasures, security policy goals, security countermeasure goals, and a list of key policies that most facilities should include in their security plan.

THEORY

I have seen countless requests for proposals for security systems consulting tasks, for which no risk assessment was performed, nor was one wanted, and for which no security policies were developed by the organization for the facility in question.

I usually turn down such work.

It is not that I do not like the business or enjoy the work, it is for the reason that such projects are almost always doomed to fail, and I do not want my name associated with the failure or to participate in any potential lawsuit resulting from its failure.

There are many security consultants and contractors who will design card readers and cameras into an architectural space without any risk analysis or security policies, based solely on their experience of what previous clients for similar companies have wanted.

This is like asking your neighbor to go to a car dealer and buy a car for your cousin. He might return with a subcompact, or a luxury car, or a sport-utility vehicle (SUV). It might be red or blue or silver. It may have an automatic or manual transmission. All of these might be good choices for your neighbor but may not be what your cousin would like to have. Your cousin, who is an executive, who entertains clients, needs a full-sized four-door car with adequate leg room in the rear seat and good shoulder and head room. The car must be black or dark blue and have an automatic transmission and a comfortable ride. Your neighbor does not know this. Your cousin will not likely get the car he needs in the absence of these specifications being known to the buyer (Figure 13.1).

So it is with security systems designed in the absence of a risk analysis or security policies. The client will not get the system he needs in the absence of the designer knowing the assets, threats, vulnerabilities, and risks. The access cards may be incompatible with



FIGURE 13.1 Buying a Car

other facilities if the designer does not know that to be a criterion. Elevators may not have floor-by-floor control if the client needs such but does not have a policy for it. There may be no card readers on elevator lobby doors if that requirement is not known. There may be no duress alarms at reception desks if that need is not understood.

So, “Design us a security system” truly is equivalent to “Buy my cousin a car.”

Accordingly, the security analyst should address the need for security policy goals before recommending any other countermeasures. All countermeasures should be derived entirely out of the organization’s security policies. If a countermeasure is implemented in the absence of a security policy, it is a waste of money. It is not needed. And it may be counterproductive or even open the organization to unwanted liability. For example, the use of video within a parking structure can actually raise the organization’s liability unless it is properly implemented.

Questions that policies answer (just a few out of many):

- Where should access control technology go, and where should guards be placed in lieu of card readers?
- When are guards better than card readers?
- Where should cameras be used, and what should they view and not be allowed to see?
- Where are alarms needed, and where are they likely to be a problem?
- How could crime prevention through environmental design (CPTED) be used to reduce the need for both security manpower and technology?
- In which situations is security technology not helpful but actually detrimental?
- What type of security credential is necessary?
- How should hi-tech, lo-tech, and no-tech security solutions be mixed to achieve an appropriate balance between best results and best economy?
- How much attention should be paid to perimeter detection?
- Should cameras be used in interior spaces and where?
- How can we achieve effectiveness and still control costs?

And, the list goes on and on.

Policies answer all these questions. Without a risk analysis, policies are not likely to be effective; without policies, countermeasures will almost certainly not be effective.

THE ROLE OF POLICIES IN THE SECURITY PROGRAM

If a risk analysis is the foundation of a good security program, then policies are the structural columns and beams. Everything hangs on policies and will fall if not supported by policies. Policies are the supporting structure that assures that countermeasures will succeed.

Look at the nature of policies. Policies are mandatory and must be followed. There are penalties for not following policies. These penalties apply equally to the lowest position in the office and the highest executive. Policies are universal unless exceptions are expressed in the policy and their application is also universal.

Policies give strength to enforcement. It is common for employees and visitors alike to complain about security procedures: “Hey, I am not a threat! You should not be asking to check my computer bag!”

Policies also set goals to achieve and are a metric against which the security program can be measured. The terrorists who struck hotels in Mumbai in November 2008 avoided hotel security by entering through the kitchen, where there was no useful security presence. A security policy of securing all entrances would have been a measurement metric against which this inadequacy would have been apparent.

Policies act as a road map to success. Security programs that begin without policies develop in a haphazard fashion that often results in a schizophrenic application of disorganized responses. It is common for security programs that are run without policies to be so scattered that a common complaint is that different guards have different interpretations of what their job is. This results in inconsistent applications of what each guard thinks his or her role to be and is assured to generate complaints from employees and guests. It will also result in an ineffective security program.

Security policies are the plan for the security program. If you fail to plan, you are planning to fail. If you have a security program without policies, you are planning to fail. Security policies determine “what” to do.

Security policies create a road map for everything else in the program. Any good security program should include security policies for:

- Crime and Terrorism Prevention Elements
- Access Control to the Campus, Buildings, and Parking
- Asset Protection of Equipment and Documentation
- Individual Responsibilities for Security
- Use of Security Technology
- Emergency Planning
- Recurring Risk Analysis

THE ROLE OF COUNTERMEASURES IN THE SECURITY PROGRAM

There are three main goals for all security countermeasures. These include:

1. Where possible, identify and deny access to potential threat actors.
2. Deny access to weapons, explosives, and dangerous chemicals to the facility (except for legitimate exceptions, which should be well controlled and monitored).

3. Make the environment suitable for appropriate behavior and unsuitable for inappropriate or criminal or terroristic behavior (CPTED program), and to mitigate the actions of both hazards and threats.

If security policies determine “what” to do, then countermeasures get it done. There are three broad types of countermeasures in any good security program:

1. Hi-Tech
2. Lo-Tech
3. No-Tech

Hi-tech countermeasures are the electronic portions of the security program, commonly including:

- Access Control System
- Digital Video System
- Security Alarm System
- Two-Way Voice Communications System
- Information Technology Security (always a subset of the information technology department)

Except for guards, hi-tech elements (Figure 13.2) are the most visible components of the security program. Hi-tech portions of the system can also be a force multiplier when correctly designed. That is, a well-designed security video system can support video surveillance, video guard tours (many more tours of the facility each hour than a walking guard can perform), and video pursuit (following a subject through the building). Access control systems save many tens of thousands of dollars annually in guard costs. And alarm systems provide alerts in many more places than an organization could afford to have eyes.

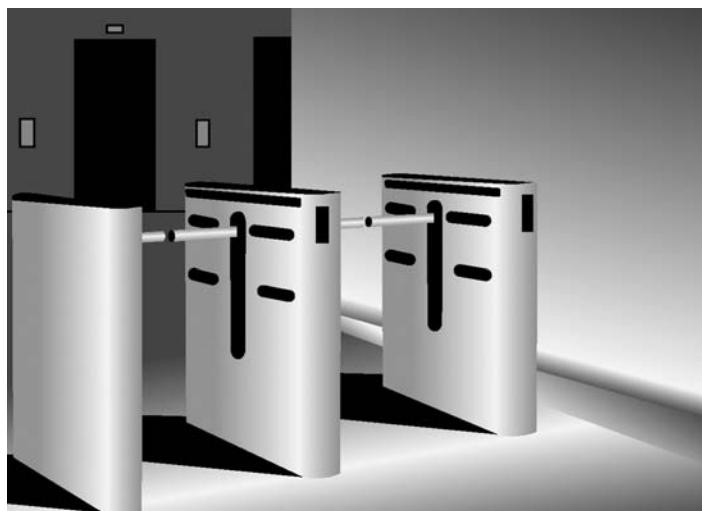


FIGURE 13.2 Hi-Tech Element



FIGURE 13.3 Lo-Tech Element

Lo-tech countermeasures include the physical portions of the security program, commonly including:

- Locks
- Barriers
- Lighting
- Signage
- CPTED elements

Lo-tech elements (Figure 13.3) can be designed to provide an environment that reduces the possibility for criminal behavior and encourages appropriate behavior. Fencing defines boundaries and indicates intent when an intruder breaches a fence. Signage elements help guide visitors to their destination and inform them of the organization's expectations for appropriate behavior. Locks and barriers maintain control over secure spaces, and lighting helps create a safer, more secure environment.

No-tech countermeasures include the operational elements of the security program, commonly including:

- Authorities and Responsibilities
- Reference to Charter for Security Unit
- Statement from the Chief Executive Officer (CEO)/Chairman/President
 - Responsibilities
 - Security unit chief
 - Security supervisors
 - Security officers
 - Security administrative staff
 - Department managers
 - Employees
 - Visitors
 - Maintenance of security policies and procedures

- Protection of Life
 - Weapons and explosives screening program
 - Chemical weapons defense and mitigation measures
 - Special countermeasures for unique vulnerabilities
 - Countersurveillance program
 - All other aspects of baseline security program
- Crime Prevention
 - Security awareness program
 - Post and patrol reports
 - Incident reporting
 - Crime investigations program
 - Law enforcement liaison program
 - Security intelligence program
 - Countersurveillance program
- Access Control Program
 - Identify public, semipublic, controlled, and restricted access spaces
 - Access cards and photo ID badging program
 - Functions, meetings, and events
 - Hours of operations and after-hours access
 - Parking controls for vehicles, motorcycles, and trucks
 - Loading dock and mail room access
 - Control of locks, keys, and access control credentials
- Asset and Property Protection
 - Security of equipment
 - Security hardware
 - Insurance cover
 - Mail recipients and deliveries
 - Headed paper
- Individual Responsibilities for Security
 - In the office
 - Drugs and illegal substances in the workplace
 - Weapons in the workplace
 - Property, lost and found
- Guards
 - Posts
 - Patrols
 - Response
 - Administrative duties
 - Training and career development
 - Random countermeasures
- VIP Protection Program
 - VIP preassessment
 - VIP security team liaison
 - Guard duties
- Emergency Security Plans
 - Weather emergencies
 - Medical emergencies

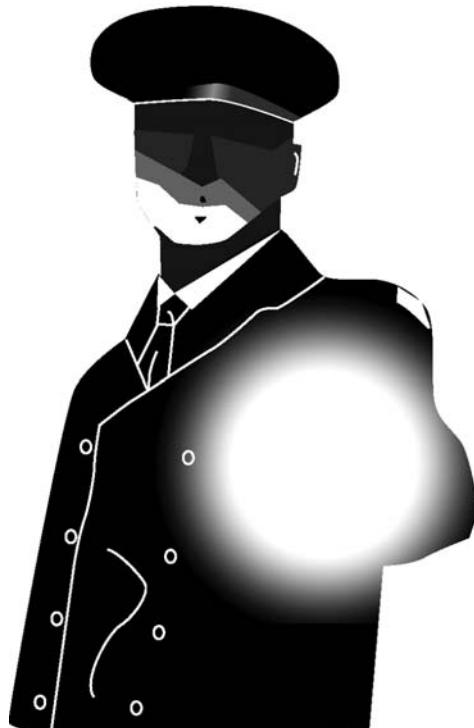


FIGURE 13.4 No-Tech Element

- Civil disorder response
- Disaster recovery plan
- Recurring Risk Analysis

No-tech elements are presented in Figure 13.4.

WHY SHOULD POLICIES PRECEDE COUNTERMEASURES?

Countermeasures that are applied without supporting policies will be necessarily lacking in completeness, organization, and coordination resulting in a haphazard and poorly performing security program.

Security programs deployed without appropriate supporting policies often have very bad results. For example, in one institution, a touchy senior manager was asked to clear through the security checkpoint on a day when he did not wish to do so. An argument ensued that resulted in the officer being accused of inappropriate behavior and the manager demanded disciplinary action (remember, he was the one not following security policy here). In a case of his word versus hers, the manager prevailed, and the banishment of the security officer stuck. This occurred for the following reasons:

- There was no policy in place requiring all employees to follow security policy, and the manager claimed that he was exempt because he was management, not an employee.

- There was no policy or training for officers on how to handle belligerent people, so she was “on her own” to determine how best to respond. (Witnesses claimed she was always polite, and the video showed this.)
- There was no policy in place regarding the treatment of security officers by management, employees, or others (thus no penalty for belligerence).
- There was no audio recording at the security checkpoint, so the manager’s claims as to what was said and by whom went unchallenged, despite the video evidence.
- The security officer suffered because of a lack of policies.

Without appropriate policies, security programs fail.

SECURITY POLICY GOALS

- *Protection of People Is the Key Goal:* Security and protection of employees, contractors, vendors, and visitors is the key goal of the security program. Human rights and dignity must be respected.
- *Security Is an All-Management Responsibility:* Corporate and line management throughout every department must continually be aware of and take responsibility for the security aspects of its business activities. The security unit must reflect this commitment in its organization and resource allocations.
- *Priorities*
 - Focus on prevention. The prevention of security events and emergencies is the first priority.
 - Threat and vulnerability assessment and risk analysis must be carried out on a regular basis, at least annually.
 - Routine facility users should be informed of security policy in a professional manner and made to understand that they are responsible to adhere to corporate security policy while on the premises.
 - Minimize the impact of security on daily operations. All security procedures should be introduced in such a way as to minimize their impact on the normal operations of the organization.
- *Security Countermeasure Hierarchy:* All security policies should be focused on using a combination of hi-tech, lo-tech, and no-tech countermeasures in order to deter, detect, assess, respond, and gather evidence for prosecution.
- *Routine Events Preparedness:* The organization and its security unit must be prepared to handle security events as they emerge daily. The security unit shall develop policies and procedures to handle all routine kinds of security events.
- *Emergency Events Preparedness:* The security unit will develop policies and procedures to handle all kinds of predictable emergencies.
- *Security Program Auditing:* Security measures and procedures should be inspected regularly and verified and validated by independent security specialists.
- *Security Unit Professionalism:* The security unit staff must be held to a high standard of professionalism, knowledge, and integrity and must be exemplary. To that end, the security unit should only hire or contract qualified staff, and appropriate training of security unit management and staff should be continuous, with pay raises and bonuses based upon continuous training and on-the-job performance.

- *Reporting and Follow-Up of Security Events:* All incidents, including security breaches and irregularities, should be reported to the security unit manager and logged into a record of security events. Corrective action should be taken as follow-up to:
 - Determine if the event is routine and requires a routine countermeasure, such as signage to inform users.
 - Determine if the event illuminates a vulnerability that could be exploited by potential threat actors and should be remedied by architectural, technical, or procedural countermeasures.
 - Determine if the event is minor and infrequent in nature and does not represent a significant vulnerability and so requires no mitigating action.
 - Determine if the event requires follow-up, investigation, or prosecution.
- *Security Unit Counseling Role:* The security unit will act as a counselor to each department and will provide periodic security audits of departments to assist management in understanding and improving security within each business unit.
- *Weapons in the Workplace Including Arming of Guards:* Security policy should determine if weapons should be allowed in the workplace and by whom. Policy should also determine if guards should be armed or unarmed, based upon the type of assets protected and the threats faced (including who else is permitted to have weapons in the workplace). If armed, the policy should assure qualifications, training, and practice for armed guards and should lay out clear rules of engagement.

SECURITY COUNTERMEASURE GOALS

The primary goal of every countermeasure is to support one or more specific security policies. The primary goals of all countermeasures are prevention, control, and recovery. These can be broken down into the following functions. All countermeasures are capable of only one or more of the following seven functions:

1. Help control access.
2. Deter a security event.
3. Detect a security event under way.
4. Help a security officer assess a security event.
5. Delay an intruder's progress either in or out of the facility.
6. Help in a response to a security event.
7. Produce evidence of the security event.

Control access: Security is much easier if only you can keep the criminal threat actors and inappropriate users away from your organization's assets. Access control helps assure that only authorized people may access the organization's assets.

Deter a security event: Deterrence is the best result of any security program. All countermeasures should be undertaken with the goal of deterring inappropriate, criminal, or terrorist acts.

Detect a security event under way: When a security incident occurs, it is important to detect it as it is under way wherever possible. Security events that are detected after the fact provide no opportunity for control and often only minimal chances for recovery. Detection may be by alarms, cameras, security staff, or employees.

Help a security officer assess a security event: Once detected, the severity of the incident must be determined in order to mount an effective and appropriate response. The number of threat actors, their dress, weapons, equipment, movements, and aggressiveness, movement toward a goal, entry point and method of entry, preparations for surveillance and detection, and preparations for exit all indicate the measures necessary to counter the threat actors.

Respond to a security event: Depending on the conditions above, a response can be formulated and dispatched. The response should be observed and managed by the console officer and console supervisor via the console and two-way radios.

Produce evidence of the security event: Throughout the security incident, special attention should be taken to record and preserve evidence for investigation and prosecution.

POLICY SUPPORT FOR COUNTERMEASURES

- No countermeasure should exist without a corresponding policy to support it.
- Response may include measures to delay the entry or exit of the subject.
- Each policy should state what countermeasures are needed to support it.

KEY POLICIES

Following is a list of key security policies that any good security program should include. These should be augmented by policies that apply uniquely to the organization's industry, facility type (office, warehouse, factory, marine terminal, etc.), and geographic area.

Authorities and Responsibilities

- *Reference to Charter for Security Unit:* The charter for the security unit is the foundational document upon which the entire security program is grounded. This document lays out the need for security for the organization and lays the groundwork for the formation of a unit to specifically address that issue alone. This document underscores the importance that the organization's management places on security.
- *Statement from the CEO/Chairman/President:* This document, from a recognized voice of authority, declares the organization's emphasis on security and directs all users to observe security policies.
- *Responsibilities:* The responsibilities of each of the organization's personnel responsible for security will be outlined, including:
 - *Security Unit Chief:* Vision, strategy, countermeasure and policy development, unit metric analysis and high-level investigations, training program development, law enforcement liaison, security intelligence program.
 - *Security Managers:* Management of supervisors and staff, training, compilation of logs and reports.
 - *Security Supervisors:* Supervision of officers, logs and reports.

- *Security Officers*: Interfacing with the public, posts and patrols, logs and reports.
- *Security Administrative Staff*: Assistance with record keeping and interfacing security management to its customers.
- *Department Managers*: Responsible for security for their own business unit with guidance and review of the security unit chief.
- *Employees*: Responsible for preserving company property and a safe workplace, also responsible for their own personal security for themselves and their property.
- *Visitors*: Responsible for personal security for themselves and their property.
- *Maintenance of Security Policies and Procedures*: A specific policy will address the maintenance of security policies and procedures, including the process for review of policies, the introduction process for new policies, or change of a policy and the process to submit the change through management channels for approval.

Protection of Life

Protection of life is the key goal of any security program.

- *Weapons and Explosives Screening Program*: The greatest threat to life in any workplace is the presence of weapons, explosives, and chemical weapons in the workplace. A good weapons screening program includes magnetic weapons detectors, X-ray screening, and explosives chemical signature detectors.
- *Chemical Weapons Defense and Mitigation Measures*: Chemical weapons defenses include protecting air intakes and sensing chemicals at air intakes, with automatic shutdown of heating, ventilating, and air-conditioning (HVAC) fans.
- *Special Countermeasures for Unique Vulnerabilities*: Depending on the vulnerability findings, the risk analyst will recommend special countermeasures to address the unique vulnerabilities found in the analysis.
- *Countersurveillance Program*: The best way to prevent a terrorist attack is to identify surveillance attempts that precede any attack.
- *All Other Aspects of a Baseline Security Program*: Taken together, the entire baseline security program forms a deterrent to attacks of all types.

Special Countermeasures Example

Early in my design career, I was confronted with a need for special countermeasures to deal with potential criminal activity. I was designing an extension building next to a banking institution's data center. The property was surrounded by a tall estate fence, but due to zoning restrictions, it was not possible to queue vehicles on the street to enter the property, and the zoning officials had ruled that the fence could not be extended across the driveway, so it remained open, thus allowing pedestrians to enter the property. They had many female employees who worked until late hours who had to walk some distance across the parking area to their cars. Gangs were known to run in the area, and violent crimes had occurred nearby. Management was concerned that some employees might be threatened by intruders through the fence opening.

I developed the following special countermeasures for the organization:

- A system to detect pedestrians entering through the vehicle entrance was necessary. The pedestrian detector included a pair of photo beams placed across the vehicle entry exactly at the fence line, coupled with a vehicle detection loop buried in the pavement exactly below the photo beams. When a vehicle passes through the beams, it is detected by the photo beams and also the vehicle loop detector. Although the photo beams detect the vehicle, the loop also detects it. The loop is programmed to shunt the photo beams so no alarm occurs when a vehicle passes. However, when a pedestrian crosses the photo beams, the vehicle loop does not detect, so an alarm occurs, thus detecting the pedestrian.
- This was coupled with a video/audio system to “escort” late-leaving employees to their cars and to intervene if they encounter any threatening stranger in the parking lot. This system included these elements:
 - A special dedicated card reader at the main lobby for employees to notify security that an escort is needed.
 - A light next to the card reader to notify the person making the request for escort that the request is acknowledged by the console officer so he or she can proceed to the parking lot knowing that he or she is under watch.
 - A low-light pan/tilt/zoom video camera mounted on the corner of the building and equipped with a long-range infrared illuminator and a high-power bullhorn mounted on the pan/tilt mechanism.
- The escort system worked as follows:
 - When an employee was ready to enter the parking lot late at night, she would present her card to the card reader at the reception counter. This would cause an alarm at the security console, notifying the guard that an escort was requested. The guard presses a button causing the light next to the card reader to notify the requestor that the request is acknowledged and an escort is available. The requestor can then leave the building.
 - As the requestor leaves the building, his or her image is displayed on the pan/tilt/zoom camera that has moved to view the front door of the building. The guard then manipulates the pan/tilt/zoom camera to follow the requestor to her car.
 - If a suspicious individual appears, the guard presses the intercom talk button that is already queued to the intercom bullhorn.
 - The guard would warn away the offender and dispatch a guard to intervene, ensure the protection of the requestor, and direct the offender away from the parking lot.

This example illustrates the typical nature of special countermeasures — that is, they typically employ multiple system elements and procedures to accomplish a task of deterrence, detection, and response. Special countermeasures often include elements that form unique responses to unique problems, using combinations of system elements and procedures that you would expect to see in a conventional security program, but which are used in unique ways to address special vulnerabilities.

Crime Prevention

Crime prevention is one of the key goals of any organization's security program. A typical crime prevention strategy includes the following policies:

- *Security Awareness Program:* A security awareness program helps users to understand their responsibilities and their role in crime prevention.
- *Post and Patrol Reports:* Each post and patrol should note any anomalies found during their shift or patrol. These should be assembled and recorded into the following categories:
 - Note of a policy violation
 - Note of a safety concern
 - Note of a condition not covered by policy but suspicious or of concern
 - Note of an unaddressed vulnerability
- *Incident Reporting:*
 - Incidents are any behavioral security policy violation by any user. Incidents can involve employees, managers, visitors, contractors, vendors, or offenders who are otherwise unrelated to the facility.
 - Incidents may be either criminal or policy violations.
 - All incidents should be handled in accordance with security policy and recorded by all security officers involved.
 - Management should review all incidents and categorize them by:
 - Life/safety violations
 - Security policy violations
 - Property violations
 - Proprietary information violations
 - Business reputation violations
 - Any trend in incidents should be analyzed monthly over the last 6 months to 2 years so that additional policy or countermeasures can be developed to prevent such and mitigate any actions related to trending incidents.
- *Crime Investigations Program:* For criminal violation incidents, either an internal or professional law enforcement investigation is appropriate in the event that the incident is unresolved.
- *Law Enforcement Liaison Program:* The security unit chief should formalize a relationship with local law enforcement in order to:
 - Develop, maintain, and test emergency response procedures.
 - Keep law enforcement apprised of security concerns related to their purview (the need for police patrols, etc.).
 - Maintain familiarity and good relations with local law enforcement.
 - Obtain up-to-date information on crime trends, strategies, methods, and tactics.
 - Assist in maintaining the organization's security intelligence program.
- *Security Intelligence Program:* Every organization should maintain a security intelligence program to:
 - Be aware of crime trends, including strategies, methods, and tactics.
 - Be aware of terrorism or regional security activities that could be related to the welfare of the organization (potential for demonstrations, etc.).

- *Countersurveillance Program:* Every organization for which terrorism is a legitimate threat should have a countersurveillance program in order to identify surveillance as a possible precursor to an attack and thus to reduce the probability of a terrorist attack by interrupting the surveillance or providing information to law enforcement for follow-up by their counterterrorism task force.

Access Control Program

The key to crime and terrorism prevention is simple. Keep threat actors out of the facility. Every organization should vet all employees and contractors for criminal background and affiliations with known terrorist organizations. Those persons who do not vet should not be hired. Visitors and employees should be allowed access on a “need-to-access” basis.

- Identify policy for public, semipublic, controlled, and restricted access spaces:
 - *Public Spaces:* Anyone can be allowed access, such as to the main public lobby of a building.
 - *Semipublic Spaces:* Areas available to the public without escort after receiving authorization by the organization’s security unit.
 - *Controlled Spaces:* General “back-of-house” employee spaces, only available to vetted employees and contractors and to vendors and visitors by escort.
 - *Restricted Spaces:* Those spaces that require fully vetted access, only vetted employees, and no visitors and no contractors who are not under escort or fully vetted.
- *Access Cards and Photo ID Badging Program:* Policy for development, use, and control of identification and access control credentials, used by an access control system and using a photo ID credential to make obvious that a person is authorized for an area.
- *Policy for Functions, Meetings, and Events:* Access for functions, meetings, and events should be clearly laid out so that the presence of visitors, especially during other than normal business hours, can be controlled.
- *Hours of Operations and After-Hours Access:* Normal hours of operation should be identified, and access provisions for employees, contractors, and vendors after hours should be established and maintained.
- *Parking Controls for Vehicles, Motorcycles, and Trucks:* Parking is a continuous problem at most facilities. Parking for executives, employees, visitors, and others should be identified by signage and access control measures.
- *Loading Dock and Mail Room Access:* Access to the loading dock should be controlled for antiterrorism and crime prevention reasons. Policy regarding vehicle and driver vetting and access to facilities for drivers should be closely controlled.
- *Control of Locks, Keys, and Access Control Credentials:* Lock and key control is essential to maintaining control over spaces not secured by the access control system. A master-keying system and computerized lock and key control are very helpful. Many organizations maintain their own locksmith facilities. If so, these must also be very closely controlled to assure that unauthorized keys are not made.

Asset and Property Protection

Property control is essential to protecting the organization's property, including fixtures, furnishings, equipment, and proprietary information.

- *Security of Equipment:* Policy regarding equipment marking and bar coding with a property control system. (This function may be under the facilities department.)
- *Security Hardware:* Security hardware should be inventoried and audited regularly for functionality.
- *Insurance Cover:* All property, fixtures, furnishings, and equipment under cover of insurance should be valued and inventoried. (This function may be under the facilities department.)
- *Mail Recipients and Deliveries:* Policy to assure that all mail and deliveries are actually delivered to their intended recipients.
- *Out-Shippments and Shipping Dock Control:* Policy should be coordinated with shipping/receiving to assure that out-shipments are all authorized and that company property not intended for export is not exiting through the shipping department.
- *Headed Paper, Checks, and Purchase Orders:* Policy should be developed to protect all letterhead, headed envelopes, checks, purchase orders, and any other financial instruments or forms indicating that the document carries the authorization of the company.

Individual Responsibilities for Security

Personal security resides with the occupants, not with the security unit. However, policy should be developed to help assure a safe and crime-free workplace, including:

- *In the Office:* Develop policy such that all employees, contractors, vendors, and visitors understand their responsibilities for personal security, security of their own property, and security of others and the property of the company.
- *Drugs and Illegal Substances in the Workplace:* Policy regarding drugs and contraband in the workplace must be clear, unambiguous, and well enforced. Policy may include prohibitions, penalties, and provisions for counseling or rehabilitation.
- *Weapons in the Workplace:* Management must determine their policy regarding weapons in the workplace not only for visitors and employees but also for the security force. This is a matter for individual organization decision in many districts. Increasingly, laws are being put into place to determine who may and may not carry weapons on private property.
- *Property, Lost and Found:* Policy regarding lost and found property and its storage, identification, and return or disposition must be put into place.

Guards

Guards are the “face” of the security unit and present the culture of the organization as it regards its security commitment.

- *Posts:* Dedicated posts, usually for granting of access control, must be established. Security policy will dictate under which conditions a post should be established and when it should be staffed.
- *Patrols:* Security patrols present an indication of a constant security presence and the commitment to watching out for criminal activity and to underscoring the watch for security violations. Policy identifying the purpose and scope of patrols and their frequency should be established.
- *Response:* Policy regarding the nature and methods of response and coordination with emergency responders should be established, along with initial training and scenario testing/continuing training.
- *Administrative Duties:* Policy concerning the administrative duties of the security unit should be established, including telephone answering, log-keeping, record-keeping, and so forth.
- *Training and Career Development:* Policy regarding basic and continuing training should be developed for guards. Guards are responsible for their own career training. Those who underperform should be eliminated.
- *Random Countermeasures:* All security programs should include provisions for random application of procedural countermeasures so that observers planning an attack will never know when a patrol or use of a particular vetting method may occur.

VIP Protection Program

Most organizations have some VIPs either as their own management or as visitors. Policies should be developed to graciously accommodate the special security needs of these special people.

- *VIP Definition:* Policy should determine who is a VIP. An astonishing number of managers, employees, and visitors presume to be treated as such, or press security to have their visitors treated as such. This can overwhelm a security force with frivolous demands.
- *VIP Preassessment:* A true VIP requires preassessment, and their visit will almost always be preannounced. This is one clear definition of a true VIP, the need for special preparation in advance to accommodate his or her presence and also accompaniment by his or her own security team. Pretender VIPs will often arrive unannounced and demand special treatment. True VIPs usually require a preassessment by their own security team. The security unit should have accommodation to deal with such.
- *VIP Security Team Liaison:* Before a VIP arrives and after his or her arrival, the security unit will have to liaise with the VIP's security team. Their team needs to know the following:
 - The layout, access, and egress path of the VIP and the security provisions to be made during transit into and out of the facility and meeting space.
 - Where and with whom the VIP will meet, and the security provisions for that space and the greeting party.
 - Provisions for the VIP's own security escort team (adjacent anteroom, refreshments, etc.).

- Minimization of the presence of those who do not need access to the VIP while they are on the premises.
- Policy regarding access for the VIP and weapons for his or her security unit while at the facility.
- *Guard Duties:* Make the VIP's security liaison familiar with the organization's posts and patrols and any special guards who will be assigned to help protect the VIP while on his or her visit.

Emergency Security Plans

Emergencies will occur. The security unit must have policies in place to accommodate them, or they will bring with them chaos. Policies should be established to deal with the following types of emergencies:

- Weather Emergencies (and Natural Disasters)
- Medical Emergencies
- Power or Communications Outages
- Civil Disorder/Riot Response
- Disaster Recovery Plan

Recurring Risk Analysis: A policy regarding the frequency of risk analyses should be established (annually is suggested). These may be either a self-assessment or by a subject matter expert (SME). SME risk analyses are often well received by senior management, so if significant or costly changes to countermeasures are expected, or if security conditions or business functions or campus construction have changed, an SME analysis is often the best way to go.

SUMMARY

The security analyst should address the need for security policy goals before recommending any other countermeasures in order to answer the following questions:

- Where should access control technology go, and where should guards should be placed in lieu of card readers?
- Where should cameras be used, and what should they view and not be allowed to see?
- Where are alarms needed, and where are they likely to be a problem?
- How could CPTED be used to reduce the need for both security manpower and technology?
- In which situations is security technology not helpful but actually detrimental?
- What type of security credential is necessary?
- How should hi-tech, lo-tech, and no-tech security solutions be mixed to achieve an appropriate balance between best results and best economy?
- When are guards better than card readers?
- How much attention should be paid in the design to perimeter detection?
- Should cameras be used in interior spaces, and where?

And, the list goes on.

The Role of Policies in the Security Program

Policies are the supporting structure that assures that countermeasures will succeed.

Policies are mandatory and must be followed. There are penalties for not following policies. Policies are universal unless exceptions are expressed in the policy, and their application is also universal. Policies give strength to enforcement. Policies also set goals to achieve and are a metric against which the security program can be measured. Security policies are the plan for the security program.

Security policies create a “road map” for everything else in the program. Any good security program should include security policies for the following:

- Crime and terrorism prevention element
- Access control to the campus, buildings, and parking
- Asset protection of equipment and documentation
- Individual responsibilities for security
- Use of security technology
- Emergency planning
- Recurring risk analysis

The Role of Countermeasures in the Security Program

If security policies determine “what” to do, then countermeasures get it done. There are three broad types of countermeasures in any good security program:

1. Hi-Tech
2. Lo-Tech
3. No-Tech

Hi-tech countermeasures are the electronic portions of the security program, commonly including:

- Access control system
- Digital video system
- Security alarm system
- Two-way voice communications system
- Information technology security (always a subset of the information technology department)

A routine security program should include policies for:

- Authorities and Responsibilities
- Reference to Charter for Security Unit
- Statement from the CEO/Chairman/President
- Protection of Life
- Crime Prevention
- Access Control Program
- Asset and Property Protection

- Individual Responsibilities for Security
- Guards
- VIP Protection Program
- Emergency Security Plans
- Recurring Risk Analysis

CHAPTER 14

Developing Effective Security Policies

INTRODUCTION

At the completion of this chapter, you will understand the process for developing and introducing security policies, triggers for policy changes, the need for expertise in periodic policy review, policy requirements, basic security policies, and regulatory- and non-regulatory-driven policies.

PROCESS FOR DEVELOPING AND INTRODUCING SECURITY POLICIES

The process for developing and introducing security policies has several distinct steps:

- Elements that trigger policy changes
- A policy request review
- A policy impact statement
- Subject matter expert review
- Senior management review and approval

Triggers for Policy Changes

In addition to the original development of security policies, there are many reasons why an organization might want to add or change one or more security policies.

- Annual review of security policies vis-à-vis the changing security landscape and revised risk analysis: All security policies should be reviewed annually. Considerations should include:
 - Does this policy serve an important purpose (prevention, control, or recovery)?
 - Is the goal of the policy still valid?
 - Is the policy being observed, or are there active efforts to get around the policy?
 - Is this the most effective way to achieve the goal of the policy?

- Changes in technology that make a policy obsolete or alter its need:
 - Sometimes changes in technology obviate the need for a policy, and sometimes such changes simply change the nature of how a policy might be implemented (e.g., as information technology emerged, all policies relating to proprietary information, which previously had addressed all by reference to paper files). Also, as security technology evolves into a more information technology infrastructure, technical standards need to change.
 - In either case, change in language of a policy might be needed.
- Evidence of a vulnerability that could be exploited which no policy addresses: Sometimes new tactics by criminals and terrorists cause new vulnerabilities to emerge, which were not previously exploited. In such cases, policy should change to accommodate emerging threats.
- Regulatory compliance requirement: As security programs become more regulatory driven, new policies must emerge to address the regulations.
- Client request: Sometimes changes in the organization or in the functions of its business units dictate new needs for policies.
- Policy expiration: Some policies are built with expiration dates. For example, some policies are annual and expire automatically unless renewed. Such cases beg for revision or renewal.
- Position paper compels need for new policy: The security unit chief will issue an annual position paper on emerging issues relating to security. Sometimes these spark discussion regarding a policy to address the issues discussed.
- It is recommended that the security unit should track all client interactions regarding discussions about the need for or insufficiency or inadvisability of any security policy.

Policy Request Review

Any need for a security policy should be submitted by the security unit chief to his or her management, along with a policy impact statement.

Policy Impact Statement

- The policy impact statement should accompany the request for policy or standards changes.
- The policy impact statement should highlight changes and impact (see also Figure 14.1):
 - Description of the new or changed policy
 - Justification or reason for new or updated policy
 - Identification of the risks of not changing the policy
 - Identification of impacted stakeholders
 - Who will be affected if the policy is not implemented
 - Who will be affected if the policy is implemented
 - Identification of the dependencies for implementation of policy changes (that is, regulatory, technology, organization, etc.)



FIGURE 14.1 Policy Impact — Limiting Vulnerability

- Procedures changes do not require policy impact statements but may be changed as needed by the security unit chief to accommodate or improve on implementing security policies.
- Policy changes may be submitted in either of two ways:
 1. Scheduled review once annually
 2. Review to address an emerging or recently identified vulnerability for which no policy is effective to mitigate

Subject Matter Expert and Management Review Process

- A security subject matter expert (SME) should review policy impact statements and the associated proposed policies and either validate the documents or make recommendations for changes in a collaborative way with the security unit chief.
- The SME will return a review report identifying any comments for changes or emphasizing the need for the change or lack of it.
- The security unit chief can either make collaborative changes or make independent changes and submit them to the SME for review and comment. Collaborative changes are best so that it is the most thoughtful process. The SME should send his comments through the security unit chief to help assure full coordination.

- Following the SME review, and any resulting collaborative changes, the security unit chief can submit the changed policy along with the SME report, or may disagree with the SME and submit the policy impact statement and proposed policy without the recommended changes along with the SME's report and the security unit chief's statement supporting the policy in its initial form.
- Security management will then review the policy impact statement and the proposed policies and submit them to senior management for approval or recommend revisions to the security unit chief. If the recommendations do not comply with the SME's recommendations, those will be resubmitted to the SME for further review and comment, and the process will cycle again.
- The proposed policy should also receive review from human resources (HR) (if it affects business operations) and to the legal department prior to receiving review by senior management. Each of those will add comments, and the comments will be relayed back to the SME and security unit chief for further comment, if recommendation is not forthcoming. Let me emphasize that it is not wise to "send the recommendations down the chain" without the security unit chief and SME being allowed to review the HR and legal department's comments. Very often, those departments make a comment without fully understanding the document they are commenting on. This can torpedo a perfectly good document. Most HR and Legal comments can be easily resolved in collaboration, and no HR/legal comment should ever shoot down a recommendation on which the security unit chief and SME have not been permitted a reply comment or collaboration.
- Finally, senior management will review and approve or deny the change to policy and will provide a comment. If denied, the policy may be resubmitted again either annually or as vulnerability needs emerge.

POLICY REQUIREMENTS

Policies must:

- Be implementable and enforceable
- Be concise and easy to understand
- Balance protection with productivity

Policies should:

- State reasons why the policy is needed
- Describe what is covered by the policies
- Define contacts with responsibilities
- Discuss how violations will be handled
- Be reviewed annually and updated if needed

BASIC SECURITY POLICIES

In the process of setting up a new security program, the security unit chief must determine what basic policies are needed. These may include:

- Establish Management Support for Security Policies
- Establish Security Policy Development and Implementation Guidelines (Including a Policy Revision History)

- Establish Access Control
 - Establish area access levels
 - Establish access authorizations for various classes of users
 - Establish access vetting and authorization granting for:
 - Hiring and contracting
 - Management
 - Staff
 - Contractors
 - Vendors
 - Visitors
 - VIPs
 - Public
 - Department visitors
 - Tenant departments
 - Vehicle access to the property
 - Parking by classes of users
- Establish Standards of Behavior for:
 - Use of the facility
 - Use of internal roadways and curbs
 - Courtesy of interactions between staff, visitors, and security officers
 - Respect for the directions of security officers
- Establish Standards for Security Posts and Patrols
 - What is the purpose of posts?
 - What are the purpose and goals of patrols, including routine and investigative?
 - What are the standards for event responders?
- Establish Standards for Use of Security Technology, Including Alarms, Video, Monitoring, Radios, and Coordination with Security Management and Responders
- Establish a Weapons Policy for the Security Unit and Employees and Visitors
- Establish the Criteria for a Public Agency Liaison Program
- Establish the Criteria for a Crisis Management Program
- Establish an Information Technology Security Liaison Policy
- Establish a Department Management Security Liaison Policy
- Establish the Criteria for a Security Investigations Program
- Establish the Criteria for a Security Intelligence Program
- Establish Standards for Training of:
 - Security management
 - Security staff
 - Security contractors
- Establish Security Management Metrics

SECURITY POLICY IMPLEMENTATION GUIDELINES

- Policy Statements
 - Why is a specific policy needed?
 - What behaviors is the policy trying to govern?
 - What conflict or problem does the policy intend to resolve?
 - What is the overall benefit to having the policy?

- Who must observe the policy?
- Who must understand the policy in order to perform his or her job?
- What technologies are used to implement the policy?
- What exceptions are there to the policy?
- References
 - Refer to any government regulations or industry standards.
- Enforcement
 - Define penalties for violating the policy.

REGULATORY-DRIVEN POLICIES

Many security policies are driven by government regulations. Increasingly, regulations are becoming the driving force and requirement behind not only policies, but also entire security programs. Especially in critical infrastructure organizations such as transportation, energy, chemical, and health care institutions, regulations play a key, if not the key, role in determining the nature and extent of security provisions that the organization carries out.

The U.S. Department of Homeland Security (DHS) is the benchmark agency for security regulations, and many nations have copied, adopted, or used the DHS's regulations as models for their own security regulations.

- Significant guidance is provided by the department in the form of:
 - The National Infrastructure Protection Program (NIPP), which can be downloaded at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
 - Components of the NIPP include:
 - U.S. Citizenship and Immigration Services (arguably the worst possible model for border protection)
 - U.S. Coast Guard (USCG)
 - U.S. Customs and Border Protection
 - Federal Emergency Management Agency (FEMA)
 - Immigration and Customs Enforcement (ICE)
 - Transportation Security Administration (TSA)
- Relevant laws and standards include*:
 - Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act).
 - National Environmental Policy Act (NEPA) of 1969.
 - Procedures for Handling Protected Critical Infrastructure Information Act of 2002.
 - The U.S. Department of Health and Human Services enforces Public Law 104-191: Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires significant security measures to protect health care information.
 - The Sarbanes-Oxley (SOX) Act of 2002 was enacted in response to numerous major corporate and accounting scandals including Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom. The legislation

* www.dhs.gov/xabout/laws/.

established standards for all U.S. public company boards, management, and public accounting firms, but it does not apply to privately held companies. The act addresses the management of accounting records and has penalties for noncompliance. As regards security, this could apply to the badging and video databases, e-mails, among others.

- Relevant policies include:
 - DHS Policy for Internal Information Exchange and Sharing
- Additional laws and regulations from the DHS include:
 - Information sharing and analysis*
 - *HSPD-3*: Homeland Security Advisory System (amended by HSPD-5) establishes a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people.
 - *HSPD-7*: Critical infrastructure identification, prioritization, and protection: Establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks.
 - *Final Rule*: Procedures for handling protected critical infrastructure information: These procedures govern the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security.
 - *The Critical Infrastructure Information Act of 2002* (CII Act): The CII Act seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism.
 - Prevention and protection
 - Border security
 - Real ID Final Rule
 - US-VISIT Air and Sea Exit, Notice of Proposed Rulemaking
 - US-VISIT Final Rule: Enrollment of Additional Aliens, Additional Biometric Data, and Expansion to More Land Ports
 - Western Hemisphere Travel Initiative (WHTI)
 - Travel security
 - Changes to Visa Waiver Program to Implement the Electronics System for Travel Authorization (ESTA) Program: Interim Final Rule
 - Advanced Information on Private Aircraft Arriving and Departing the United States: Notice of Proposed Rulemaking
 - Travel procedures
 - Issuance of a Visa and Authorization for Temporary Admission into the United States for Certain Nonimmigrant Aliens Infected with HIV
 - Infrastructure protection
 - Critical Infrastructure Information Act of 2002
 - Final Rule: Procedures for Handling Protected Critical Infrastructure Information
 - Chemical Facility Anti-Terrorism Standards: Interim Final Rule

* www.dhs.gov/xinfoshare/laws/index.shtm.

- Chemical security
 - Chemical Security (Chemical Facility Anti-Terrorism Standard [CFATS])
- Employment issues
 - E-Verify
 - Social Security No-Match: Safe-Harbor Procedures for Employers Who Receive a No-Match Letter
 - Optional Practical Training Interim Final Rule
 - H-2A Temporary Agricultural Worker Program Proposed Changes
- Preparedness and response*
 - *HSPD-5*: Management of domestic incidents: Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
 - *HSPD-8*: National preparedness: Identifies steps for improved coordination in response to incidents. This directive describes the way federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident. This directive is a companion to HSPD-5.
 - *HSPD-8 Annex 1*: Further enhances the preparedness of the United States by formally establishing a standard and comprehensive approach to national planning.

The U.S. Transportation Security Administration (TSA) issues and administers Transportation Security Regulations (TSRs), which are codified in Title 49 of the Code of Federal Regulations (CFRs), Chapter XII, parts 1500 through 1699.[†]

Security Rules for All Modes of Transportation are contained in Subchapter B, CFR 1520. Civil Aviation Security is covered under subchapter C, CFRs 1540, 1542, 1544, 1546, 1548, 1550, 1552, and 1562. CFRs 554 and 1560 are reserved.

Maritime and Land Transportation Security are covered under subchapter D, CFRs 1570 and 1572, with 1580 reserved.

Administrative and Procedural Rules are covered under subchapter A, CFRs 1500, 1502, 1503, 1507, 1510, 1511, and 1515.

NONREGULATORY-DRIVEN POLICIES

Nonregulatory-driven policies include all policies that are not required by law or regulation. However, many of these are required by organization charters.

The key policy development should include policies to:

- Protect People
- Protect Business Operations
- Protect Proprietary Information
- Protect the Organization's Business Reputation
- Protect Property

The goal of every security policy should be to protect one or more of these vital assets.

^{*} www.dhs.gov/xpreprep/laws/index.shtm.

[†] www.tsa.gov/research/laws/regs/editorial_multi_image_with_table_0205.shtm.

The types of policies that accomplish these goals include:

- Policy Basis
 - Establish management support for security policies
 - Establish security policy development and implementation guidelines
 - Establish a facility security plan
 - Establish security management metrics
- Protect People
 - Access control policy
 - Weapons/explosives screening policy
 - Crisis management program policy
 - Security intelligence program policy
 - Standards of behavior policy
 - Security posts and patrol policy
 - Security technology policy
 - Weapons policy
 - Security awareness program policy
 - Security training policy
- Protect Business Operations
 - Access control policy
 - Weapons/explosives screening policy
 - Crisis management policy
 - Disaster recovery policy
 - Security posts and patrol policy
 - Standards of behavior policy
 - Security technology policy
 - Public agency liaison policy
 - Information technology liaison policy
 - Department management liaison policy
 - Security investigations program policy
 - Security intelligence program policy
 - Security training policy
 - Security management metrics policy
- Protect Proprietary Information
 - Access control policy
 - Weapons/explosives screening policy
 - Crisis management policy
 - Disaster recovery policy
 - Security posts and patrol policy
 - Standards of behavior policy
 - Security technology policy
 - Information technology liaison policy
 - Department management liaison policy
- Protect the Organization's Business Reputation
 - Access control policy
 - Weapons/explosives screening policy
 - Crisis management policy
 - Disaster recovery policy
 - Security posts and patrol policy

- Standards of behavior policy
- Security technology policy
- Public agency liaison policy
- Information technology liaison policy
- Department management liaison policy
- Security investigations program policy
- Security intelligence program policy
- Security training policy
- Security management metrics policy
- Protect Property
 - Access control policy
 - Weapons/explosives screening policy
 - Crisis management policy
 - Disaster recovery policy
 - Security posts and patrol policy
 - Standards of behavior policy
 - Security technology policy
 - Public agency liaison policy
 - Information technology liaison policy
 - Department management liaison policy
 - Security investigations program policy
 - Security intelligence program policy
 - Security training policy
 - Security management metrics policy

SUMMARY

Process for Developing and Introducing Security Policies

The process for developing and introducing security policies has several distinct steps, including:

- Elements that trigger policy changes
- A policy request review
- A policy impact statement
- Subject matter expert review
- Senior management review and approval

Policy Requirements

Policies must:

- Be implementable and enforceable
- Be concise and easy to understand
- Balance protection with productivity

Policies should:

- State reasons why the policy is needed
- Describe what is covered by the policies
- Define contacts with responsibilities
- Discuss how violations will be handled
- Be reviewed annually and updated if needed

Basic Security Policies

- Establish management support for security policies
- Establish security policy development and implementation guidelines (including a policy revision history)
- Establish access control
- Establish standards of behavior
- Establish standards for security posts and patrols
- Establish standards for use of security technology, including alarms, video, monitoring, radios, and coordination with security management and responders
- Establish a weapons policy for the security unit and employees and visitors
- Establish the criteria for a public agency liaison program
- Establish the criteria for a crisis management program
- Establish an information technology security liaison policy
- Establish a department management security liaison policy
- Establish the criteria for a security investigations program
- Establish the criteria for a security intelligence program
- Establish standards for training
- Establish security management metrics

Security Policy Implementation Guidelines

- Policy Statements
 - Why is a specific policy needed?
 - What behaviors is the policy trying to govern?
 - What conflict or problem does the policy intend to resolve?
 - What is the overall benefit to having the policy?
 - Who must observe the policy?
 - Who must understand the policy in order to perform his or her job?
 - What technologies are used to implement the policy?
 - What exceptions are there to the policy?
- References
 - Refer to any government regulations or industry standards.
- Enforcement
 - Define penalties for violating the policy.

Policies may be driven by regulations or other needs.

SECTION

III

Countermeasure Selection

CHAPTER 15

Countermeasure Goals and Strategies

INTRODUCTION

At the completion of this chapter, you will understand why security countermeasures are required, and the elements of countermeasure objectives, goals, and strategies.

The term *security countermeasures* implies correctly that they are measures taken to counter a threat action. In an ideal world, security countermeasures would be so effective as to completely eliminate the will of potential threat actors to take action.

Although most people believe that is not possible, in fact it has been done. There are actually numerous examples, but perhaps the best known is the Fort Knox Gold Depository. As one could imagine, there have been many potential threat actors who would be interested in accessing the gold at Fort Knox since it was built. But none have even attempted. Countermeasures including a formidable building and complex, heavily armed guards, layered detection systems, automatic weapons (oh, and do not forget that it sits next to the largest assembly of U.S. Army tanks and tank crews in the world) that are so well developed that no one has ever attempted a robbery there.

Compare that to the average U.S. convenience store, which as a class, these stores have the highest incidence of robberies of any fixed asset, including many fatal violent attacks. It is worthwhile to compare the two in order to develop study models of risk mitigation.

Fort Knox has multiple layers of protection, including heavy arms and multiple layers of detection systems to protect its assets. Its focus is on access control.

Convenience stores have little, if any, protection — often the cash register drawer is directly accessible by reaching across the counter from the public side. Access to the store is free to anyone, good or bad. There are generally no responsive weapons and no detection until a robbery is announced by the threat actor. The greatest protection is usually a video camera system that records the robbery but which cannot intervene. Access control is often limited to a hopeful expectation of politeness.

In one case, access control is heavy. In the other, access control is minimal. The obvious lesson is that keeping bad people out is good for security.

I am not suggesting that all facilities should be equipped like Fort Knox, because most organizations could not function with this level of access control, and the presence of automated .50-caliber weapons and guards on parapets with scoped weapons would be not only a deterrent to crime but also a deterrent to normal business.

Countermeasures should be focused not only on security measures, but also on being balanced with the needs of the organization's daily business needs. Like all other business programs, compromises are necessary. What are the goals of countermeasures, given that compromises are necessary?

COUNTERMEASURE OBJECTIVES, GOALS, AND STRATEGIES

All security countermeasures have the broad goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization.

There are three main goals for all security countermeasures:

1. Where possible, identify and deny access to potential threat actors.
2. Deny access to weapons, explosives, and dangerous chemicals to the facility (except for legitimate exceptions, which should be well controlled and monitored).
3. Make the environment suitable for appropriate behavior, unsuitable for inappropriate or criminal or terroristic behavior, and mitigate the actions of both hazards and threats.

Implementation objectives and strategies include:

- Control access to the target, denying access to possible threat actors.
- Where possible, deter threat actors from acting.
- Detect any threat action.
- Assess what has been detected.
- Delay the progress of any threat actor into or out of the facility.
- Respond to any active threat action.
- Gather evidence for prosecution, investigations, and training.
- Comply with the business culture of the organization.
- Minimize any impediment to normal business operations.
- Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.
- Design programs to mitigate possible harm from hazards and threat actors.

Each aspect of the overall security program has the ability to support one of the three main goals. An incomplete example of how to map these is illustrated in Figure 15.1. You can use this as an example to help build your own list of countermeasures.

ACCESS CONTROL

Goals: Access control should be sufficient to facilitate access by authorized users and to deny access to unauthorized persons to all critical areas.

Unlike Fort Knox, most organizations rely on access by the public to their facilities. However, access should not be universal. All members of the public and all employees do not require full access to all areas of a facility. In the most humble shop, there is a public area and a storeroom/office. In complex facilities, access may be layered so that one needs progressively higher access authorization as one moves deeper into the facility.

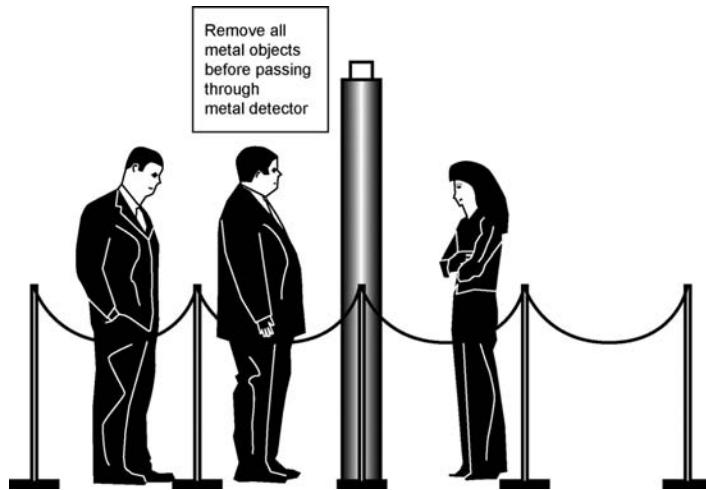


FIGURE 15.1 Security Checkpoint

- *Modes:* Access control has two modes:
 1. Passive — Screening of employees, contractors, and vendors
 2. Active — Screening of entry by employees, contractors, vendors, and visitors
- *Passive Strategies:*
 - Develop an employee/contractor/vendor screening program
 - Screen for criminal background, drug abuse (and financial responsibility where possible)
 - Enforce it strictly
- *Active Strategies:* Access control should be arranged in layers, typically including:
 - Public areas
 - Semipublic areas
 - Controlled areas
 - Restricted areas
 - Public layers will be nearest the main public door, such as a public lobby, customer waiting area, or service desks.
 - Semipublic areas are areas where the general public may not freely go, but where they may be escorted, such as to an interview or triage room or emergency department in a hospital.
 - Controlled areas are for those individuals with authorization, such as non-public office floors, mechanical rooms, auto-mechanic work areas, airport tarmacs, and so forth.
 - Restricted areas are those that require a high degree of vetting and where access is limited to a relatively small number of persons, such as research and development areas, the boardroom, main information technology server room, cash vaults, counting rooms, and so forth.

Access control can be achieved by technology or personnel means. There are two basic types of access control:

1. General Access Control
2. Positive Access Control

General access control assumes that if one in a group has access to a space, anyone he or she is escorting is also permitted. This approach is commonly used in employee work spaces and the like, where an access card reader on a suite door controls access to the space. General access control should not be used where it is important to ensure that each person in a group has access privileges. This is because of the phenomena of an unauthorized person “tailgating” entry behind an authorized person as the door is opened. Although many organizations have tried to encourage employees to vet visitors who try to tailgate, none I know have fully succeeded.

Positive access control uses technology or guards to assure that each person is checked to be sure that they are authorized to enter the space. Examples of positive access control include card-reader-controlled revolving doors and turnstiles, theater or sports event ticket checkers, and airport boarding screening.

DETERRENCE

Goals

Deterrence is the ultimate goal. Deterrence achieves security without intervention against a threat actor. Deterrence builds its own momentum. The longer attacks are deterred, the less likely it is that an attack may take place.

Deterrence occurs when potential threat actors evaluate the risks and rewards of an attack and determine that the risk is not worth the reward.

- For terrorists, this could mean that an attack is not likely to succeed, that their attack would not capture the media’s attention, or that they could be perceived negatively by their own constituency.
- For economic criminals, it could mean that they may not be able to access the desired assets, or to leave with them, or the likelihood of capture after the heist would be high.
- For violent criminals, this could mean that the threat actor could not reach his target, could not succeed in the attack, or might not escape, or might be captured later.
- For subversives, this could mean that they might not succeed in subverting the normal operations of the organization.
- For petty criminals, this could mean that they might not be able to carry out their crime or would likely be captured in the act or later.

Strategies

Deterrence is achieved through making countermeasures visible enough that possible threat actors think twice about their crime. Deterrence countermeasures can include architectural hardness, access control measures, guards, obvious cameras, witnesses, alarms, and alarm signs. To be effective as a deterrent, countermeasures must be visible and must seem to create too much risk to carry out the attack. Ultimately, the entire baseline security program is about deterrence, and it creates the environment for all the other countermeasure functions (Figure 15.2).

There is no such thing as deterrent-specific countermeasures. All visible countermeasures can act as deterrents, but no countermeasures deter alone. Deterrence is a side



FIGURE 15.2 Deterrence

effect of the countermeasure's other (primary) role. Countermeasures deter because the potential threat actor believes that the countermeasure creates risk to him. That risk is the result of the countermeasure serving its primary role of limiting access, detection, assessment, response, or evidence gathering.

DETECTION

Goals

Although at first the reader may be tempted to think that detection means catching the crook in the act, in fact every threat actor must carry out a plan in order to attack a facility. The basic steps in every threat action, whether it is terrorism or vandalism, include:

- Select an appropriate target for an attack.
- Surveil the target to determine the target's vulnerabilities.
- Determine the best way to carry out the attack.
- Plan the attack (the approach, the attack, and the escape).
- Test the target to determine if the vulnerability assessment is correct.
- Execute the attack:
 - Enter
 - Establish and maintain control
 - Establish and maintain countersurveillance
 - Execute the objective
 - Escape

For petty crimes, all these steps may occur in one linear timeline. However, the more valuable the asset, the more important the attack is to the threat actor's strategic goals, the more robust the countermeasures, the more time is required to carry out all these steps. Interviews with highly successful criminals indicate that the planning cycle

for some crimes can take months or even years. This gives the target many opportunities to detect the plan through the detection of surveillance and interception of planning communications.

Strategies

Strategies include surveillance detection and attack detection.

Surveillance Detection

Most people think of detection as occurring during an attack; however, detection can also occur during surveillance. Surveillance is required for virtually every attack in order to:

- Select the target.
- Surveil target vulnerabilities.
- Determine the best way to carry out the attack.
- Test the target to determine if the vulnerability assessment is correct.

Additionally, the longer a criminal spends time with eyes on the target, the more interaction he may have with individuals working in the target space. Each interaction gives the target opportunity to recognize surveillance, attack planning or testing, and interrupt the attack before it occurs.

A good countersurveillance program is highly useful to all organizations where asset values are high, and especially where there is a possibility of violence occurring in the carrying out of a crime. For terrorism, a good countersurveillance program is an absolutely essential component of any workable terrorism countermeasures program.

A good countersurveillance program includes:

- Ample use of video surveillance in exterior and public spaces
- Trained and alert security officers
- Trained and alert console officers
- Loitering detection software on the video system

Attack Detection

Once an attack of any kind is under way, whether it is terrorism, economic crime, violent crime, subversive action, or a petty crime, it is important, where possible, to be able to detect the crime under way.

Detection countermeasures may include:

- Intrusion detection system on property and building perimeters
- Intrusion detection system applied to critical passageways and internal spaces
- Duress alarms at critical counters and desks
- Hold-up alarms

Intrusion detection systems on property and building perimeters may include fence detection systems, microwave and infrared beams, seismic detectors, pneumatic line detectors, video fence-line detection systems, glass break detectors, and door position switches.

Internal space detection systems may include door position switches, area motion detectors, and video motion detectors.

Duress alarms may include hidden finger switches, foot switches, and so forth. Hold-up alarms may include duress alarms and bill traps (last bill removed in a cash drawer triggers a silent alarm).

Alarms may be either silent or audible. It is best to use an audible alarm if the property is vacant, such as at nighttime, and the audible alarm could act as a deterrent, frightening the intruder away. Silent alarms are best where an audible alarm could be false or nuisance and where on-site security staff can respond quickly and where such response would not possibly escalate the crime to violence.

ASSESSMENT

Goals

When an attack is detected, it is then necessary to assess the threat for the following reasons:

- *Is the detection real, false, or a nuisance detection?*
- *If the detection is real, what are the level and nature of the threat actors?*
- *What is their goal?*
- *What weapons are they carrying?*
- *What are their tactics?*
- *Does this appear to be unfolding as a property or violent crime or a property crime with potential for violence?*
- *Are they employing countersurveillance methods?*
- *How are they dressed?* How can law enforcement recognize the threat actors from ordinary employees or customers?
- *What is their apparent exit strategy?*
- *Is the detection real, false, or a nuisance detection?* Many alarms are either false or nuisance alarms. Before responding to any alarm, it is useful to investigate and assess to see if the alarm is real. This can often be done by using a second alarm device as a confirmation, or using a second technology to confirm. For example, on perimeter alarms where nuisance alarms are common, it is useful to have two types of alarm detection technologies, each having different nuisance modes, and both working together. For example, the use of infrared beams and fence line detection, where infrared is subject to nuisance alarms from blowing newspapers or animals, and the fence-line detection is subject to nuisance alarms from nearby trains. If only one alerts, it could be a nuisance alarm, but when both do, it is confirmed. Video cameras can also be used to confirm the alarm when the presence of an intruder can be seen on camera.
- *If the detection is real, what are the level and nature of the threat actors?* Once confirmed, it is important to know the nature of the threat actors. How many threat actors are there? Does their intrusion seem organized or chaotic? Is there an obvious leader? Is the group cohesive and professional, or are they displaying anxiety and fear?
- *What is their goal?* Are they carrying a sign protesting the activities of the organization, or are they carrying automatic weapons? How many threat actors are there? Can their intentions be determined by their actions?
- *What weapons are they carrying?* If the threat actors are carrying weapons, what type are they? Are they knives, handguns, automatic weapons, rocket-propelled

grenades (RPGs), or mortars? Does the use of the weapons indicate a high degree of training, or do they seem amateurish?

- *What are their tactics?* The tactics of an individual or group speak to their capabilities and training and preparation to use force or to counter a security presence. Tactics may indicate that it is appropriate to confront or to stand off.
- *Could their intentions include violence?* Based upon observations such as their interactions with employees and customers, it may be possible to determine their willingness to use violence as a means to control the crime scene or to gain access to specific assets. The willingness to use violence may be important to help dictate your response.
- *Are they employing countersurveillance methods?* The presence of obvious countersurveillance such as a person waiting in a car nearby but not at the door indicates a high level of preparation and planning. This indicates that contingency planning may also be in place to deal with approaching law enforcement or the arrival of external security team members. The presence of countersurveillance will dictate different response strategies.
- *How are they dressed? How can law enforcement recognize the threat actors from ordinary employees or customers?* Whether the response will be by law enforcement or by internal security, it is important for them to know who are the threat actors and who are the victims. Otherwise, all persons will be treated as threat actors. This is especially true where the threat actors are using violence to control the crime scene.
- *What is their apparent exit strategy?* Often overlooked, it is important to determine the probable exit strategies, where possible. These may include:
 - A waiting car, perhaps with a getaway driver (look for a getaway car at all exits)
 - Waiting motorcycles or bicycles
 - The use of weapons to exit the premises
 - The taking of hostages
 - The staging of stolen goods (such as dumping jewelry into a dumpster for later retrieval)

This knowledge can help to cut off the criminals or allow for the interception of the criminals or their stolen goods.

Strategies

Effective assessment countermeasures include video and voice communications systems.

Video cameras should be placed at all facility perimeter areas, facility approaches, and facility entries in order to get a positive identification of any threat actors who enter the facility and to determine what external support they have in terms of lookouts and getaways.

It is very useful to have a video camera viewing every reasonable area where a threat action could occur, including all entry control locations. This allows both detection and assessment of crimes in progress. It is also very useful to have a two-way voice station (intercom station or station without call button) near the camera wherever a threat action could occur. This allows interruption of the threat action by a remote console operator, and for many crimes, this is enough to end the crime.

RESPONSE (INCLUDING DELAY)

Goals

Once a threat action is detected, a response is possible. Responses to threat actions could include:

- Take no direct action to counter the threat actors, instead try to minimize any potential harm to innocent people.
- Gather evidence for an investigation and for a postevent analysis resulting in scenario planning and training later.
- Call others (such as the police) for help.
- Intervene directly against the attack to stop it and capture the threat actors.

Before any response is undertaken, it is necessary to formulate an appropriate response. I propose that the best time to do this is before any attack, when heads are clear and planning time is leisurely. It may be necessary to adjust the plan if an actual attack takes place, but at least there will be a response plan in place.

For example, before September 11, 2001, it was the policy of airlines to cooperate with airplane hijackers and let negotiators arrange for freedom of the hostages once back on the ground. This strategy included allowing hijackers access to the cockpit to avoid casualties on the plane. However, when United Airlines Flight 93 passengers used their cell phones to call loved ones after the plane was hijacked, the passengers learned that another plane had crashed into the World Trade Center, the passengers changed the strategy from one of cooperation to one of counterforce. Although this strategy did not save their own lives, it did save many lives in the ultimate target, in Washington, D.C., and, as such, was certainly an act of heroism.

Strategies

Responses may also include delaying the threat actors, denying them access to the target asset, voice communications for negotiations, and ultimately force on force.

As a design consultant, I am a big believer in using technology to counter threat actors instead of placing lives at risk. The use of reactive electronic automated protection systems (REAPS technologies) may include two-way voice communications, delaying technologies, disruptive technologies, and active force technology for direct use against threat actors. See Chapter 16 for more on REAPS technologies.* Also, REAPS technologies are covered in great detail in my book *Integrated Security Systems Design*.

Intercoms are the forgotten technology of security. Security intercom systems, along with ample use of security video systems, allow for immediate assessment of threat actions without dispatching a guard, which could escalate the crime to violence. One of the most effective tools against convenience store crimes has proven to be a two-way voice

* For even more on REAPS technologies, see the author's book: Thomas L. Norman, *Integrated Security Systems Design — Concepts, Specifications, and Implementation* (Burlington, MA: Butterworth Heinemann, 2007).

communication system that allows console officers in a remote security command center to speak directly to store robbers, alerting them that they are not only being recorded by video cameras, but that their identification is solid and that police have been called and are on the way, and that any escalation to violence will result in more severe charges by law enforcement. This has proven to be effective to get robbers to stop the robbery and leave the premises immediately without further harm to the store employees or customers and in many cases also without completing the robbery.

It is very useful to have a two-way voice station (intercom station or station without call button) near the camera wherever a threat action could occur. This allows interruption of the threat action by a remote console operator, and for many crimes, this is enough to end the crime.

EVIDENCE GATHERING

Goals

The goals of evidence include providing resources for investigations, strategy development, and training. Figure 15.3 presents information on evidence gathering.

Evidence sources may include:

- Video footage
- Audio recordings
- Fingerprints
- Crime scene forensics
- Computer forensics
- Witness statements

Strategies

The security program should be designed to gather evidence from its outset, and personnel should be trained to protect physical evidence.

Camera placement should be useful to identify threat actors as they approach and enter the facility and at the most likely locations where crimes may occur. This requires, during the risk analysis, careful consideration of the types of threat scenarios that are most likely and the locations where such scenarios might occur. All these should be noted in the report.

Audio should be recorded on all outgoing calls to emergency responder phone numbers (911 in the United States and 112 in other countries) and on all active security intercom stations.

Security officers should be trained to secure a crime scene immediately after a crime until law enforcement arrives. Security barrier marker tape (“Crime Scene — Do Not Cross”) should be kept in stock for this use.

Any computers that could have been involved in a crime should be unplugged from the network but left powered on, secured, and sealed for the arrival of a law enforcement or internal computer forensics team.



FIGURE 15.3 Evidence Gathering

COMPLY WITH THE BUSINESS CULTURE OF THE ORGANIZATION

Goal

Every organization has its own unique business culture. It may be formal or relaxed, top-down or lateral, or open for free movement of the public or imposing restricted movements. The security program should be configured to comply with the business culture of the organization. All security measures have some consequence both to normal business operations and to the business culture. Both should be minimized as much as possible.

I have been consulted on many projects to correct failed security programs that, upon review, were basically sound in principle, but which did not take the organization's business culture into account and thus were not accepted by the users. The users are stakeholders in the system. If their point of view and expectations of convenience and perceived intrusion are not taken into account, the security provisions will not be accepted. This is the most important nontechnical element that addresses directly the success or failure of the system.

People will naturally take the path of least resistance. And, if after many years of moving freely, they are suddenly confronted by a queue or a barrier, they will attempt to circumvent it because they are used to being able to move freely through a portal without impediment. If there is a sneak-path, they will use it. If there is a guard, they will argue with him or her. There will be complaints, and pressure will be applied to the security manager to change the procedures or technology. It is important to take traffic flow, throughput, and people's perceptions of how they are being treated by management into account.

Strategies

In the countermeasure planning phase, it is important to understand the organization's business culture as much as possible. This is perhaps the most difficult task that a security practitioner has to do. Business cultures are rarely well documented. Culture by definition is that body of knowledge that is common and allows a common communication based upon shared assumptions of those working together.

For example, in one high-security project, the entire campus could be easily secured by moving all visitor parking to an adjacent parking lot and having all visitors clear through a single visitor center. However, the business culture of that organization required that all visitors be granted access to parking on the campus, thus allowing visitors past the visitor center. Security took second place to business culture.

It should be assumed that the security program should impede as little as possible into the movements of people, and the security program should ensure that everyone is treated with consideration, kindness, and respect.

MINIMIZE IMPEDIMENTS TO NORMAL BUSINESS OPERATIONS

Goals

As with business culture, all security measures have some consequence to normal business operations. The security program should impede as little as possible into the normal business operations.

Strategies

The key impediment to business operations is almost always in the area of access control.

A key strategy of controlling access without creating the sense of an impediment is to rely more on technology than on people for security access control.

It takes more time to clear a staffed checkpoint than to clear through a card reader. And people tend to see technological delays as "part of the environment." However, when the delay is associated with a security guard, they tend to personalize the screening action. (People sometimes presuppose a bias against the person by the screener and infer an intent on the part of the security officer to delay the person.) No such intent can be imposed on a card reader, as technology has no capacity to develop intent or biases or to distinguish any one person from another.

This strategy has other benefits as well. Because technology does not distinguish people, it treats everyone fairly and cannot be compromised by threat, intimidation, or enticement.

All security officers dealing with the public should be trained to be gracious under fire and not to personalize any verbal abuse.

In areas where people are carrying bags or totes, provisions should be made to use as few hand actions as possible. In such cases, the use of photo IDs as an access vetting measure can help speed people along.

SAFE AND SECURE ENVIRONMENTS

Goals

Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.

Strategies

The use of crime prevention through environmental design (CPTED) principles helps to create a safe and secure environment and conveys a feeling of safety and security to all.

Good lighting, gracious guards, well-maintained facilities and security equipment, good way-finding signage, security awareness inserts in the company newsletter — all these things contribute to a feeling of well-being on the part of users.

DESIGN PROGRAMS TO MITIGATE POSSIBLE HARM FROM HAZARDS AND THREAT ACTORS

The security program should include elements to deal with unwanted exceptions, such as:

- Intruders and Offenders
- Disruptive People
- Medical Emergencies
- Natural Disasters
- Civil Disorder and Riot
- Loss of Business Continuity
- Chemical, Biological, Radiological Emergency
- Challenges to the Security Program from Outside and Inside Sources

Countermeasure goals and functions are presented in Figure 15.4.

Countermeasure Goals	Countermeasure Goals and Functions (Examples)						
	Countermeasure Functions						
	Access Control	Deterrence	Detection	Assessment	Delay	Response	Evidence
Identify and Deny Access to Potential Threat Actors	Access Control, Screening Posts, and Employee Screening	Visible Devices, Signage, Guards, and Procedures	Guards, Dogs, and Alarm Devices Including Video Motion	Console, Guards, and Security Awareness Policy	Operable Barriers and Guard Posts	Console, Guards, Operable Barriers and Intercoms	CCTV, Intercoms, and Witness Reports
Deny Access to Weapons, Explosives, and Dangerous Chemicals to the Facility	Screening, Guard Posts, and Procedures	Signage, Guards, and Procedures	Detectors, Dogs, Guards, and Procedures	Screening Posts, Detectors, Dogs, and Patrols	Operable Barriers and Guard Posts	Console, Guards, Operable Barriers and Intercoms	CCTV, Intercoms, and Witness Reports
Make the Environment Suitable for Appropriate Behavior and Unsuitable for Inappropriate for Criminal or Terroristic Behavior, and to Mitigate the Actions of Both Hazards and Threats	CPTED Design, Policies and Procedures, Training Programs, and Security Awareness Programs	CPTED Design, Policies and Procedures, Training Programs, and Security Awareness Programs	Patrols and Reports by Organization Members	Patrols and Reports by Organization Members	See Above	See Above	CCTV, Intercoms, and Witness Reports

FIGURE 15.4 Countermeasure Goals and Functions

SUMMARY

Security countermeasures are measures that are taken to counter a threat action. Ideally, security countermeasures would be so effective as to completely eliminate the will of potential threat actors to take action. Countermeasures should be focused on both security measures but also on being balanced with the needs of the organization's daily business needs. Compromises are always necessary.

All security countermeasures have the broad goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization. This is done in three ways:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terroristic behavior.
2. Detect, assess, and respond to exceptions.
3. Design the program to mitigate any potential harm from hazards and threats.

Implementation strategies include:

- Control access to the target, denying access to possible threat actors.
- Deter any threat action from occurring.
- Detect any threat action.
- Assess what has been detected.
- Respond to any active threat action.
- Gather evidence for prosecution, investigation, and training.
- Comply with the business culture of the organization.
- Minimize any impediment to normal business operations.
- Help to create an environment where people feel safe and secure and can focus on the purpose of the organization.
- Design programs to mitigate possible harm from hazards and threat actors.

CHAPTER 16

Types of Countermeasures

INTRODUCTION

All security countermeasures should have the goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization. This is done in four ways:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terroristic behavior.
2. Control access to critical assets.
3. Detect, assess, and respond to exceptions.
4. Design the program to mitigate any potential harm from hazards and threats.

There are two primary types of countermeasure implementations, each having three elements:

1. The Baseline Security Program (BSP)
2. Special Countermeasures to Address Special Vulnerabilities

Each of these have hi-tech, lo-tech, and no-tech components. Both the BSP and special countermeasures are necessary to cope with all the conditions that an organization may confront. The exact makeup of those programs is the result of recommendations from the risk analysis.

BASELINE SECURITY PROGRAM

The baseline security program is the heart of the countermeasures. The BSP is designed to accommodate normal day-to-day operations and allow for the identification of unwanted exceptions so that they can be handled. The BSP is not designed to cope with highly unusual conditions such as acts of terrorism. The BSP should include all four elements:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terroristic behavior.
2. Control access to critical assets.
3. Detect, assess, and respond to exceptions.
4. Design the program to mitigate any potential harm from hazards and threats.

Typical Baseline Security Program Elements and Implementation

Program Elements

- Hi-Tech Program Elements
 - Alarm/access control system
 - Parking access control system
 - Security video system:
 - Fixed and pan/tilt/zoom (PTZ) exterior cameras
 - Fixed and PTZ interior cameras
 - Video analytics
 - Security communications systems:
 - Digital two-way radio system (part of the telecommunications package)
 - Security intercom system
 - Command/control elements:
 - Lobby consoles
 - Security management console
 - Main and archive servers
 - Situation awareness software
- Lo-Tech Program Elements
 - Perimeter control elements (fencing, etc.)
 - Pedestrian and roadway barriers, such as:
 - Office lobby turnstiles
 - Roadway barriers (lift-arm gates)
 - Automated road blockers
 - Lighting (part of the electrical package)
 - Locks (part of the architectural package)
 - Signage (part of the architectural package)
 - Crime prevention through environmental design (CPTED) elements
 - Security landscaping
 - Security architectural elements
- No-Tech Program Elements
 - Management elements
 - Security program planning
 - Security management acquisition
 - Security policy development
 - Security procedures development
 - Security program metrics development
 - Security guard program
 - Posts (also called a fixed patrol)
 - Patrols
 - Security guard training program
 - VIP handling program
 - Mobile procedures (drop-off areas)
 - Fixed procedures (in-house areas)
 - Liaison with VIP security staff
 - Security awareness program
 - Security communications program

- Security investigations program
- Law enforcement liaison program
- Baseline Security Program Implementation
 - Planning
 - Security supervisor hiring
 - Supervisor training
 - Security officer hiring
 - Security officer training
 - Scenario rehearsals
 - Daily operations training
 - Security program documentation
- Baseline Security Program Phasing
 - Planning
 - Implementation
 - Training
 - Review

Designing Baseline Countermeasures

Follow these steps to design countermeasures for a baseline security program:

- Access Control Program
 - Define access zones, such as:
 - Public zones
 - Semipublic zones
 - Controlled zones
 - Restricted zones
 - Define which assets require what level of zoning, then zone to those requirements.
 - Define control points between zones. These will be the access control locations.
 - Determine what kind of access control is required at each control point (card reader, biometric reader, vehicle lift gate, vehicle sliding gate, etc.).
 - Determine which access control locations need guard assistance (visitor badge issuance, etc.).
 - Determine which access control points need intercom assistance (vehicle parking gates, etc.).
 - Define the access credential program (photo ID badges, etc.).
 - Way-finding signage
- Define the Detection Program
 - Perimeter detection
 - Facility perimeter
 - Building perimeter
 - Interior detection
 - Space detection
 - Duress alarms
- Define the Assessment Program
 - Video assessment
 - Audio assessment
 - Two-factor alarm assessment

- Define the Deterrence Program
 - Patrols
 - Posts
 - Signage
 - Security awareness program
 - Security investigations program
- Define the Response Program
 - Communications
 - Guards
 - Vehicles
 - Armed/unarmed
 - Response training requirements
 - Security-related medical emergencies
- Define the Evidence Gathering Program
 - Video and audio archiving elements
 - Crime scene security principles
 - Evidence preservation
 - Witness statements
 - Follow-up investigations and training

SPECIFIC COUNTERMEASURES

During the course of the risk analysis, you may uncover certain threats that are not day-to-day threats but for which the security program must be prepared to handle. These will require specific countermeasures in addition to the baseline security program. Three common elements of specific countermeasures include:

1. Terrorism and Major Crimes Deterrence Program
 - Terrorism countersurveillance program
 - Security intelligence program
 - Physical hardening of major entries and perimeter boundaries
 - Blast protection and blast mitigation measures
2. Emergency Preparedness Program
 - Medical emergencies
 - States of heightened alert
 - Civil disorder preparedness
 - Fire evacuation and response
 - Earthquake, hurricane, or other natural disaster response
 - Postevent activities
3. Disaster Recovery Program
 - Short-term disaster recovery — security unit coordination
 - Long-term disaster recovery — should be part of the risk manager's mandate, and the security unit will play a part but will not lead that effort

Each of these program elements requires its own unique approach and deserves a book on each subject, but this list covers the most used program elements.

COUNTERMEASURE SELECTION BASICS

Following the guide in baseline security program development above, the analyst, security program manager, and security technology designer should work together to develop a coordinated and effective security program. The basic elements of a well-shaped baseline security program are outlined below, and an appropriate selection of possible countermeasures is listed under each section.

This section also outlines the advantages and disadvantages of various electronic security countermeasures as well as the exploits for them. This is necessary to know in order to use the devices correctly so that they cannot be easily exploited. Note that exploits have not all been verified by the author, and most exploits will result in false alarms with possible detection of the person setting the false alarms.

All detection countermeasures should be used in layers or pairs or with audio or video assessment measures for independent verification of any alarm detection. This effectively counters the exploits of most technologies.

Hi-Tech Elements

Access Control Systems

- Card Technologies
 - General:
 - Access cards are digital credentials that allow authorized users to carry a credential that grants them access through doors and portals, such as revolving doors and turnstiles, that are equipped with access card readers. This helps ensure that only authorized people are permitted into controlled and restricted spaces and achieves this with minimal security force staffing. Access cards may also be configured with the user's photo and other identifying information to identify the user and the areas to which the user has access. The latter is usually shown in card colors where certain colors in certain locations identify the areas for which the user has access. Finally, some access credentials also contain other data, such as biometric information, health records, and financial records.
 - Magnetic Stripe Cards
 - *Description and application:* Magnetic stripe cards are similar to credit cards in form and have a magnetic stripe typically using an American Bankers Association (ABA) stripe with either two or three active stripes. Each stripe holds different information. Stripes may or may not be encrypted to protect the data.
 - *Advantages:* Magnetic stripe cards are very inexpensive and can be used with a photo ID system.
 - *Disadvantages/exploits:* Magnetic stripe cards are easily copied and can be insecure.
 - Wiegand Wire Cards
 - *Description and application:* Wiegand wire cards are credit card shaped, and the card's number is created by laying a series of magnetically encoded wires (Wiegand wires) in an order that represents a distinct binary code, unique to that individual card. The cards are read by swiping them through a Wiegand card reader and can be equipped with photo ID imprints.

- *Advantages:* Wiegand wire cards are permanently magnetized and cannot be modified like magnetic stripe cards. They are also virtually impossible to copy and therefore are much more secure than magnetic stripe cards.
- *Disadvantages:* Wiegand wire cards are more expensive than magnetic stripe cards, and the cards must be swiped through their reader, requiring some precision and contact. These card readers have a limited life, more maintenance, and longer throughput time than proximity cards.
- *Exploits:* Disassemble another card and reconfigure the bitmap to match the card to be copied. This is almost impossible to do correctly, as the spacing as well as the bitmap must be copied exactly in order for the copied card to work properly.
- Proximity Cards and Key Fobs
 - *Description and application:* Proximity cards are credit card shaped and are equipped with a microchip and two antennas. One antenna receives a query from a nearby proximity card reader, and the other transmits the card's unique card number back to the querying reader. Another version of this technology configures the credential as a key fob for convenience.
 - *Advantages:* Proximity cards are relatively inexpensive and can be equipped with photo ID imprints. Proximity cards do not require contact with the reader and thus have a high throughput through an access control portal.
 - *Disadvantages:* There are no disadvantages in practical use.
 - *Exploits:* Proximity cards can be copied by sophisticated technology.
- Active Cards
 - *Description and application:* Active cards are typically used where some distance is required, such as for automotive access. The cards are typically equipped with batteries.
 - *Advantages:* Active cards can be read from long distances, up to 100 feet allowing for very fast throughput, such as automobiles transiting at high speed. Encrypted cards and readers are available.
 - *Disadvantages:* The batteries have a limited life span, and the cards are relatively expensive.
 - *Exploits:* Capture the bitmap with a second reader nearby and create a copy of a valid active card using a sophisticated card programmer. This is virtually impossible for encrypted cards.
- Radio Frequency (RF) Access Devices
 - *Description and application:* RF access devices are similar in form to garage door openers. When a button is pressed, the device transmits a radio frequency code to a receiver. Unlike active cards, the receiver is not transmitting a query code.
 - *Advantages:* These permit long-range use in a convenient and familiar form, such as at the main gate of a housing development, allowing ready access for residents and their vehicles.
 - *Disadvantages:* The codes can be captured and duplicated unless encrypted.
- Bar Code Cards
 - *Description and application:* Cards are typically paper cardstock, and bar codes may be either optically readable or readable by infrared reader.

- *Advantages:* Cards are very inexpensive and are suitable for use for visitors (one-time use).
 - *Disadvantages/exploits:* Optical types can be easily copied on a normal copier.
 - Contactless Smart Cards
 - *Description and application:* Contactless smart cards are access control cards with small integrated circuits embedded.
 - *Advantages:*
 - Contactless smart cards have all of the advantages of proximity cards.
 - They have a higher level of security over proximity cards due to the encryption of data.
 - Cards can carry supplementary data for use as IT access credentials, points of sale, or medical data carriers.
 - Cards can also carry biometric data.
 - Cards can coordinate operation with other systems, including digital cash, health records, time and attendance, guard tour information, and lighting and HVAC control and billing.
 - RF data transmission between cards and readers is encrypted to prevent card “sniffing.”
 - *Disadvantages:* They have a slightly higher cost than the standard proximity card.
 - *Exploits:* There are virtually none if the system is encrypted and configured correctly.
 - Transportation Worker Identification Credential (TWIC) Cards
 - *Description and application:* TWIC cards provide a tamper-resistant biometric credential for maritime workers needing unescorted access to secure areas of port facilities, platforms, and vessels that are under Maritime Transportation Security Act of 2002 (MTSA) regulation. The U.S. Coast Guard administers the program. Persons needing access to the above-mentioned facilities and vessels must submit a photo and biometric sample (such as a fingerprint) and pass a U.S. Coast Guard-administered security check.
 - *Advantages:* TWIC cards provide a high degree of security due to their multiple confirmations that the carrier is the authorized bearer and the security checks. Some facilities use TWIC credentials exclusively, and other facilities use a combination of TWIC and non-TWIC cards, depending on to what part of the facility one needs access.
 - *Disadvantages:* The cost is higher than that for other types of access cards.
 - *Exploits:* There are virtually none.
 - Access Credential Reader Technologies*
 - Three main types of credential readers include:
 1. Readers that let you credential by what you have (cards, fobs, etc.)
 2. Readers that let you credential by what you know (keypads)
 3. Readers that let you credential by who you are (reads a physical attribute — biometric)

* This section lists only card readers that are in common use. For a full list of card readers, refer to the author's book: Thomas L. Norman, *Integrated Security Systems Design — Concepts, Specifications, and Implementation* (Burlington, MA: Butterworth Heinemann, 2007).

- Magnetic Stripe Card Readers
 - *Description and application:* Magnetic stripe card readers come in two types: insertion and swipe. Insertion-type readers are rare and are usually seen only in older installations. Swipe readers are still sold. Each reader reads the magnetic stripe of a magnetic stripe access card.
 - *Advantages:* They are very inexpensive.
 - *Disadvantages:* The card must be swiped. Routine maintenance is required on the reader. Readers may fail to read accurately as they wear and may need to be replaced periodically.
 - *Exploits:* Cards for these readers can be copied easily.
- Wiegand Swipe Readers
 - *Description and application:* Wiegand swipe readers read Wiegand access cards by swiping, inserting, or laying the card against a surface.
 - *Advantages:* Card readers are very secure and reliable. The card cannot be read from nearby devices, as could a proximity card theoretically. Cards are almost impossible to copy.
 - *Disadvantages:* The card must have contact with the card reader, and reader slots may be subject to vandalism.
 - *Exploits:* There are none for the reader. Disassemble another card and reconfigure the bitmap to match the card to be copied. This is almost impossible to do correctly, as the spacing as well as the bitmap must be copied exactly in order for the copied card to work properly.
- Standard Proximity Readers
 - *Description and application:* Proximity readers read cards in near proximity to the card reader.
 - *Advantages:* They are affordable, and no routine maintenance is necessary.
 - *Disadvantages:* Card readers must not be mounted on metal surfaces (such as on the outside of a metal building) in order to work well.
 - *Exploits:* Theoretically, cards could be read from a nearby concealed unauthorized card reader and then cloned allowing an unauthorized user to pose as an authorized cardholder.
- Contactless Smart Card Readers
 - *Description and application:* Contactless smart cards are access control cards with small embedded integrated circuits.
 - *Advantages:*
 - They have all of the advantages of proximity cards.
 - There is a higher level of security over proximity cards due to encryption of data.
 - The card can carry supplementary data for use as an information technology (IT) access credential, point of sale, or medical data carrier.
 - Cards can also carry biometric data.
 - Cards can coordinate operation with other systems, including digital cash, health records, time and attendance, guard tour information, and lighting and HVAC control and billing.
 - *Disadvantages:* They have a slightly higher cost than standard proximity reader and cards.
 - *Exploits:* There are virtually none when encrypted.

- Long-Range Card Readers
 - *Description and application:* Long-range card readers use radio frequency to query and read cards from a distance. Long-range readers come in two types:
 - Those that read conventional access cards (read from 3 to 6 feet)
 - Those that read special access cards (suitable for use in automobiles)
 - *Advantages:*
 - There is no need to remove the card from a wallet or a purse.
 - Conventional-type cards can read conventional cards at vehicle entry points without lowering the driver's window.
 - Cards can be read in automobile windshields.
 - *Disadvantages:* They are more costly than conventional card readers. Those suitable to read automobiles at a distance are comparatively very expensive.
 - *Exploits:* There are virtually none.
- Bar Code Readers
 - *Description and application:* Bar code readers are commonly used to read temporary (visitor) cards.
 - *Advantages:* They can read temporary cards.
 - *Disadvantages:* Most bar code readers have ASCII rather than Wiegand connections, requiring a data protocol converter to be compatible with most access control systems.
 - *Exploits:* Optical bar code cards can be easily copied.
- Keypad Readers
 - *Description and application:* Numeric keypads similar to keypads allow access to doors and portals by entering a code unique to each user, or common to all. These come in two types:
 - Common code: Dry-contact relay interface to door lock or gate
 - Unique user code: Wiegand interface to access control system
 - *Advantages:*
 - They are very inexpensive.
 - There are no cards to carry.
 - *Disadvantages:* Codes can be easily read by a person standing nearby, thus compromising portal security.
 - *Exploits:* Persons with visual access can memorize the access code and then enter it later. This can be easily facilitated by a cell phone video camera allowing the offender to appear to be making a cell phone call while actually recording the keypad entry code.
- Scramble Keypad Readers
 - *Description and application:* These are similar to normal keypad readers, but each number is composed of a seven-segment light-emitting diode (LED) behind a transparent membrane. User first enters "Start" button, which causes numbers to appear in random order, never the same pattern twice in a row. A user entering the same code will virtually always press different buttons each time the reader is used.
 - *Advantages:* They are very secure, as no one nearby can read the number or remember the sequence of the buttons.



FIGURE 16.1 Biometrics

- *Disadvantages:* They are slightly more costly than proximity card reader, provided by only one vendor, and must be used with that manufacturer's access control system, obviating their use on other systems.
- *Exploits:* Extort the code from a valid user.
- Biometric Reader Technologies (see also Figure 16.1)
 - *Description and application:*
 - Biometric readers read a person's physical attributes and validate the person against a card or key code sample or against a database of other biometric samples.
 - Biometric readers may read a variety of biometric attributes, including:
 - Hand geometry
 - Fingerprint
 - Blood vessel patterns in the finger, hand, or eye
 - Iris
 - Retina
 - Voice print
 - Facial characteristics (facial recognition)
 - Handwriting
 - There are two main applications of biometric readers:
 1. *ID Verification:* ID validation of the biometric credential is conducted against another credential (card, keypad code, etc.). This application validates one biometric credential against one other form of credential (dual factor).

2. *True Identification:* Identification of the person directly from the biometric sample is validated against the entire biometric database of all users in the system (single factor).
 - *Advantages:*
 - Biometric credentials provide a more certain assurance that the individual is who he or she claims to be.
 - *Disadvantages:*
 - Biometric readers are more costly than card readers or keypads of all types.
 - Biometric readers are slightly slower to use than card readers or keypads.
 - True Identification readers may operate slowly if the biometric sample database is large.
 - *Exploits:*
 - Hand geometry: None
 - Fingerprints: Fingerprints can be copied using special plasticized coating
 - Blood vessel patterns: None
 - Retina: None
 - Iris: None
 - Voice print: Virtually none
 - Facial: None
 - Handwriting: Virtually none
- Photo ID Systems
 - *Description and application:*
 - Photo ID systems place a photo of the authorized bearer on the access card.
 - The card may also have other identifying information for the individual, the organization, and the area or areas for which the individual has valid authorization.
 - A photo ID system may include:
 - Digital camera(s)
 - Photo ID workstation and software (captures the photo, prints the card, and coordinates those attributes with the access control database)
 - Photo ID card printer
 - Interface to the alarm/access control database
 - *Advantages:*
 - Photo ID systems help assure that the bearer is the authorized cardholder.
 - Photo ID systems help visually identify authorized users from nonauthorized visitors.
 - Photo ID systems simplify enforcement of access card security policy.
 - *Disadvantages:* None.
 - *Exploits:* Numerous exploits have been devised to circumvent photo ID systems, but they remain an effective deterrent against all but the most sophisticated criminals.

Detection Systems

- Property Perimeter Detection Systems
 - Capacitance Detection Systems
 - *Description and application:* Capacitance detection systems can be configured underground or on a fence fabric or fence topper. They detect by sensing changes in a tuned circuit resulting from the introduction of water (in the form of a human) nearby to the antenna of the tuned circuit (the sensing cable). This changes the resonant frequency of the tuned circuit and thus “de-tunes” it. The de-tuning results in a detectable change to the resonance of the tuned circuit which can be measured in mass and location along the sensing cable. Thus, detection software can annunciate the location of a detection along a long line.
 - *Advantages:* Reliable if used correctly. Very little maintenance if installed correctly.
 - *Disadvantages:* Cannot be used underground near pools of water such as puddles.
 - *Exploits:*
 - There are unverified stories of exploits of capacitance systems during very heavy rains.
 - Cutting the line.
 - Fiber-Optic Detection Systems
 - *Description and application:* Long optical fibers attached to fence fabric detect vibrations of a fence climber or an attempt to cut the fence fabric. They detect the location of the forced entry attempt along the sensor line. Some versions also provide audio.
 - *Advantages:* They are highly reliable when installed correctly. Long lines are possible — one manufacturer makes single zones as long as 100 kilometers (60 miles), with sensing accuracy down to ± 1.5 meters, thus suitable for use along a nation’s border.
 - *Disadvantages:* They must be installed correctly, completely along the entire line.
 - *Exploits:* Cutting the line; entry is possible until down-line repairs are made.
 - Seismic Detection Systems
 - *Description and application:* Seismic detection systems are microphones, usually in the form of spikes that are driven into the ground and connected by radio frequency (RF) or cable to a detection circuit.
 - *Advantages:* They detect ground noise for short or long distances, such as footsteps or vehicles nearby.
 - *Disadvantages:*
 - They must be used in the correct type of soil. Loose soil is less effective.
 - They cannot be used in areas with high vehicle traffic (especially large trucks), as the noise of vehicles will drown out any footsteps.
 - *Exploits:* Use of a large vehicle to mask the sound of footsteps (in one case, a jackhammer was used to mask the entry).
 - Monostatic Microwave Detection Systems
 - *Description and application:* Monostatic microwave detectors (transceivers) fill a space with microwave energy and detect the echo of the

microwave energy. When an object such as a person moves within that space, it changes the echo, which is measurable.

- *Advantages:* They are reliable outdoors for short ranges.
- *Disadvantages:*
 - They can sense through walls, causing undesired detections.
 - They cannot be used in close proximity to fluorescent lights, as they will also sense the plasma movement in the lamp.
- *Exploits:* They cause numerous false alarms, resulting in the guard force ignoring later (and real) detections.
- Bistatic Microwave Detection Systems
 - *Description and application:* Bistatic microwave detectors do not work on the echo principle, but rather there are two units (transmitter and receiver). Detection occurs for movement of any object between the units within their field of detection, which is widest at the center point between the detectors.
 - *Advantages:* They are very reliable for detection of any moving object.
 - *Disadvantages:*
 - They must be used with another detector outdoors to confirm as many nuisance detections are possible.
 - The area of detection must be completely free of standing water and small animals — best used inside a confined fence enclosure, such as between two perimeter fences to reduce nuisance alarms
 - The detector will detect any motion, including blowing debris, rain, snow, and blowing dust.
 - *Exploits:* During a rainstorm when there may be many nuisance alarms.
- Pneumatic Underground Detection Systems
 - *Description and application:* Comprising a flexible tube and an atmospheric pressure sensor, these detectors reliably sense pressure on the tube, such as a person stepping on the tube. The tubes are typically buried just beneath the surface of the ground.
 - *Advantages:*
 - Inexpensive compared to some other long-line detectors.
 - Because the tube is buried, its location is difficult for an intruder to detect.
 - *Disadvantages:*
 - Imprecise detection — only the entire zone is detected, not the location along the zone.
 - The line must be pressurized, and pressure must be maintained precisely.
 - Burrowing animals (moles) could gnaw through the tube, thus disabling it. When this occurs, the entire line must be inspected to find the leak.
 - *Exploits:* If the location of the tube could be found, one could create a hole, disabling the entire sensor zone (unverified).
- Infrared and Laser Detection Systems
 - *Description and application:* Infrared and laser detection systems are line detectors that detect a break in the infrared or laser light beam. Laser detectors cover longer distances than infrared beams. As the names of

both types of detectors imply, these are both sensing line-of-sight. Best use is as a set of multiple stacked beams.

- *Advantages:*
 - Very reliable sensing of motion between the beams.
- *Disadvantages:*
 - Senses anything between the beams, including animals, blowing objects, and so forth.
 - Sensors must be “stacked” so that the beam cannot be crawled under or stepped over.
- *Exploits:* Cause so many false alarms that the zone is ignored.
- Leaky Coax Cable
 - *Description and application:* Composed of a coaxial cable in which the grounding braid provides only approximately 50% coverage instead of the usual 100% as used for video and television applications. A tuned circuit is established, using the leaky coax as the antenna of the circuit. The 50% braid allows some of the signal to be “leaked” and creates a capacitive field around the coax wire. The presence of the water in a human body detunes the tuned circuit, causing an alarm.
 - *Advantages:*
 - Leaky coax can be installed below the ground or on a fence.
 - When the coax cable is installed below the ground, the sensor is invisible.
 - *Disadvantages:*
 - Sensitivity on a buried leaky coax is reduced or eliminated by standing water.
 - *Exploits:* Anyone moving less than 1 foot every 10 minutes may not be detected.
- Ground-Based Radar
 - *Description and application:* This is short-range radar that looks for movement of objects (including vehicles, humans, and animals) on the ground.
 - *Advantages:* Very precise detection as to range and direction.
 - *Disadvantages:* Cannot easily be used adjacent to areas of high natural activity, such as a road, as these cause nuisance alarms and reflections into the sensor area.
 - *Exploits:* Confuse the radar with radar noise in the same bandwidth.
- Building Perimeter Detection Systems
 - Door Position Switches
 - *Description and application:* Door position switches sense the door or gate being opened as the magnet (which is on the door) leaves its position next to the switch (which is in the door frame). Better switches utilize multiple magnets to “bias” the switch so that simple exploits actually create an alarm instead of defeating it.
 - *Advantages:* Detects doors opening as little as two inches.
 - *Disadvantages:* Switch and magnet should both be concealed in the door top and frame where the door sits, rather than on the outside of the door.
 - *Exploits:*
 - Early exploits called for the placement of a magnet next to the switch, thus causing the switch to fail to sense that the door had not been opened. Better “balanced bias” switches use multiple magnets to use

this exploit against itself. That is, placing a magnet next to the switch will actually cause an alarm immediately, even with the door closed.

- Saw through the door, leaving it closed in the frame.

- Glass Break Detectors

- *Description and application:* Acoustic- and vibration-based glass break detectors detect the sound of breaking glass.
- *Advantages:* Almost certain detection of window breakage.
- *Disadvantages:* Early acoustic detectors false alarmed on vacuum cleaners and sometimes on keys jangling.
- *Exploits:* Better glass break detectors are nearly invulnerable to outside exploits.

- Photoelectric Beam Detectors

- *Description and application:* Photoelectric beam detectors (usually configured as infrared detectors) sense motion between the detectors.
- *Advantages:* Very reliable detection of any object or person crossing the beams. Infrared beams are invisible.
- *Disadvantages:* In most installations, the location of the beams is obvious, allowing stepping over the beams unless they are used as a stack, which is rare indoors.
- *Exploits:* Leave an object blocking the beams before leaving for the night, thus causing the zone to trip into “trouble” condition.

- Outdoor Passive Infrared Detectors

- *Description and application:* A few companies manufacture passive infrared detectors designed for use outdoors. These have hardened enclosures and specific circuitry to deal with the unique infrared signatures found only outdoors. These include the ability to filter out most infrared noise, such as shadows of leaves, wind-driven temperature changes, and so forth.
- *Advantages:*
 - They are low cost relative to many other outdoor detectors.
 - Detector visibility may act as a deterrent. (Most potential intruders would recognize it as a security device but would not understand its workings and thus be fearful of being caught.)
- *Disadvantages:*
 - Higher false alarms than some other outdoor systems.
 - Does not work well in high-temperature environments or extremely low-temperature environments.
- *Exploits:*
 - Very, very slow movement.

- Interior Space Detection Systems

- Microwave Detection Systems

- *Description and application:* Microwave detectors (transceivers) fill a space with microwave energy and detect the echo of the microwave energy. When an object such as a person moves within that space, it changes the echo, which is measurable. Microwave detectors use the Doppler effect to detect. Accordingly, microwave detectors are most sensitive to objects moving toward and away from the detectors.
- *Advantages:* Reliable indoors in confined areas as long as the energy does not penetrate an adjacent room, where it could also be measured.

- *Disadvantages:*
 - Can sense through walls, causing undesired detections.
 - Cannot be used in close proximity to fluorescent lights, as it will also sense the plasma movement in the lamp.
- *Exploits:*
 - Very, very slow movement directly across the field of the motion detector.
 - Cause numerous false alarms, resulting in the guard force ignoring later (and real) detections.
- Infrared Detection Sensors
 - *Description and application:* Infrared motion detectors are wall-mounted units usually mounted near the ceiling and viewing an entire room or corridor. Some types are configured as a “curtain” sensing motion moving through the curtain. In all types, the sensor is configured to view a number of zones (also called fingers), and the sensor detects differences in heat signature between the fingers. Thus, persons moving across the fingers are most readily detected.
 - *Advantages:* Reliable detection within normal temperature zones of any motion across the fingers.
 - *Disadvantages:*
 - Heat sources such as heating vents can cause false alarms.
 - Detector is least sensitive for persons moving toward the detector.
 - Detectors are useless as the ambient temperature approaches ambient body temperature.
 - *Exploits:*
 - Covering the intruder with a very heavy blanket that blocks the detection of infrared energy and moving slowly may cause the detector to fail to detect intrusion.
 - Moving directly toward the detector.
- Dual-Technology Sensors
 - *Description and application:* Designed to address both the weaknesses and strengths of microwave and infrared detectors, dual-technology detectors use both technologies in one package. In order for detection to occur, both detectors must sense motion.
 - *Advantages:* These detectors are sensitive to motion both across and toward the detector, thus confirming detection internally and obviating the failure modes of both detection technologies.
 - *Disadvantages:* None.
 - *Exploits:* Virtually none.
- Ultrasonic Sensors
 - *Description and application:* Ultrasonic detectors have fallen into disuse due to numerous false alarms and occasional failures to sense real security events. Two types exist (active and passive). Active detectors emit an ultrasonic frequency and listen for disruptions in its reflection. Passive systems listen for sounds in the ultrasonic range.
 - *Advantages:* None.
 - *Disadvantages:* Failure modes include keys jangling, vacuum cleaners, insects, other noises, nearby airports, and construction zones.
 - *Exploits:* Many.

- Thermal Imaging Sensors
 - *Description and application:* Thermal imaging sensors detect the heat from bodies against the background.
 - *Advantages:* Very good detection, including imaging of the intruder.
 - *Disadvantages:* Very expensive.
 - *Exploits:* High-ambient temperature and cannot penetrate glass.
- Point Detection Systems
 - Duress Alarms
 - *Description and application:* Unlike all other alarms above, which are unintentionally triggered by suspicious persons, duress alarms are switches that are intentionally triggered by authorized persons when they believe they need help. Most duress alarms are configured to be triggered discretely, though there is also a class of duress alarms that are positioned for anyone to trigger, such as a call-security button by a security intercom on a train platform.
 - *Two-finger switches:* This type requires that two fingers press two adjacent pushbuttons to assure that no accidental duress alarm is sent.
 - *Shroud switches:* This type has a single pushbutton contained within a shroud to prevent false alarms.
 - *Pull switches:* This type requires the user to pull on a knob, usually contained within a shroud.
 - *Foot switches:* This type requires the user to place his or her foot under a bar and lift to trigger the alarm.
 - *Bill traps:* When the last bill in a cash drawer is removed, the alarm is automatically triggered.
 - *Audio/video verification:* All duress alarms should be used with both audio and video verification wherever possible.
 - *Advantages:* These alarms provide the user with the ability to call for help.
 - *Disadvantages:* Some types can be triggered accidentally or intentionally, creating false alarms.
 - *Exploits:* The person confronting the duress alarm user will convince the user not to trigger the alarm, usually by threat of force. Defeat the alarm communication media (telephone, etc.) so that even though the alarm has been triggered, it will not be reported to anyone who could respond.
 - Explosive Detection Systems
 - *Description and application:* Various types of explosives detection systems exist, including:
 - X-ray
 - Millimeter wave scanner
 - Chemical residue detection systems
 - Dogs
 - Electronics
 - Visual inspection systems
 - Hand inspection
 - Undervehicle mirrors
 - Undervehicle video detection systems
 - *Advantages:*
 - *X-ray:* Available in two types — transmission and backscatter X-ray systems. Can image the interior of packages and cargo, including

vehicles, trailers, and containers. Backscatter X-ray can scan individuals and identify objects concealed under clothing.

- *Millimeter wave scanner:* Similar to backscatter X-ray in effect, the technology can scan persons from a distance and provides a visual image of the person scanned sans clothing, but displaying any objects concealed under the clothing. These are used with software that blurs the face and private areas; however, there is much discussion about whether they breach privacy expectations.
- *Dogs:* Very efficient when properly trained and used, also they make good company, and in most parts of the world, people find the search of their articles and person by a dog to be unobtrusive and often welcome the interaction with the dog. This is not the case for persons carrying explosives.
- *Electronics:* Electronic detection methods use mass spectrometry or other means to “sniff” explosives residues. These do so with varying degrees of efficiency and efficacy. The best of these can detect minute traces of explosives on vehicle door handles, trunk latches, steering wheels, and radio knobs.
- *Visual Inspection Systems*
 - *Hand inspection:* Hand inspection is inexpensive and can be very thorough when X-ray machines are not available or for infrequent occasions
 - *Undervehicle mirrors:* These can detect unusual objects placed under vehicles that could be a threat to the vehicle occupants and anyone standing nearby. Note that packages under vehicles rarely contain enough explosives to be a danger to buildings, only the vehicle occupants and persons nearby. Bombs under cars are usually placed there to assassinate the anticipated occupant.
 - *Undervehicle video detection systems:* These systems can provide a complete undervehicle view better than and in less time than the use of a mirror.
- *Disadvantages:*
 - *X-ray:*
 - Transmission X-ray machines can miss some organic substances, and the technician must be trained to properly read the images presented.
 - Backscatter X-ray machines do not penetrate objects as far as transmission X-ray systems do and illustrate only one side of the object. The best backscatter systems can penetrate only up to 30 cm (~12") of solid steel. Backscatter X-ray used on individuals creates an image of the person without clothing, creating privacy concerns. Steps have been taken to blur private areas and to move the screener away from the person being screened to enhance privacy. However, privacy concerns remain unabated, especially in Arab and South Asian countries.
 - *Millimeter wave scanner:* Similar concerns regarding privacy to backscatter X-ray, also millimeter wave scanners become inefficient as the

ambient temperature rises to near body temperature and when clothes are wet as when entering from a rainstorm.

- **Dogs:** Dogs are unacceptable in some Muslim countries due to religious beliefs. Dogs require frequent breaks; thus, many more dogs than one might imagine are required for a single checkpoint. When used at many checkpoints, the quantity of dogs can become unmanageable. Trained dogs are costly and also require dedicated, trained handlers and frequent scenario training to keep the dog's skills honed.
- **Electronics:** Many mass spectrometers require expensive supplies and must be constantly cleaned, thus reducing their effectiveness. The better systems are self-cleaning and require few supplies, but these are very costly compared to the less-capable types.
- **Visual inspection systems**
 - *Hand inspection:* Exposes the inspector to possible bomb triggering.
 - *A word about undervehicle inspection:* I am fascinated at the amount of effort put into undervehicle inspection as a means of protecting facilities. There is no record of any bomb placed under a vehicle that has ever damaged any building's structure, nor is it ever likely to happen. Undervehicle bombs are almost always placed for detonation to kill or maim the occupant(s) of the vehicle and not to damage property or kill large numbers of people. The use of undervehicle inspection at a facility entry checkpoint is an indication of an ignorant security analyst and planner. This is yet another example of the placebo effect — that is, the attempt to appear to protect the public, while doing little to actually do so. These systems are most often used in an ineffective manner, thus compounding the problem by advertising to real threat actors that security measures are not only ill-conceived but also ineffective.
 - *Undervehicle mirrors:* Often, inspections using undervehicle mirrors are cursory and ineffective, usually inspecting only the front or one side of a car. Very effective with training.
 - *Undervehicle video detection systems:* This is an expensive solution in search of a problem. I have seen many of these in practice, and in no cases could the operator identify any object that was not original to the car.
- **Exploits:**
 - *X-ray:* Placing objects in a manner to obscure their nature or function. For example, placing a gun against the side of a suitcase instead of placing it flat where its outline could be easily seen.
 - *Millimeter wave scanner:* Using rain, hot weather, or a heavy coat to render the system ineffective.
 - *Dogs:* Dogs are very hard to beat — maybe by offering the dog a steak, but then the handler might notice that.
 - *Electronics:* Also very hard to beat when used properly — these are a very potent deterrent.
 - *Visual inspection systems*

- *Hand inspection of packages:* Using accomplices to create a distraction.
 - *Undervehicle mirrors and undervehicle video detection systems:* Generally pointless if their intended purpose is to protect the facility — that is, unless it is you getting into the car.
- Video Detection Systems
 - Visible Light Cameras

Visible light cameras are the most common type, converting visible light into a lens and onto an imager into analog or digital signals that can be recorded and viewed on recorders, digital archivers, and video monitors.

 - Fixed Video Cameras (Figure 16.2)
 - *Description and application:*
 - These cameras have a constant unchanging field of view that is dependent upon the lens focal length.
 - Most cameras today also have automatic backlight compensation to prevent silhouetting, automatic gain control, automatic shutter speed or automatic iris to adjust for light levels, and digital image processing to help assure the best possible image under all light conditions.
 - Fixed cameras come either as an exposed camera on its own mount (often with an enclosure) or concealed within a dome for aesthetics and to conceal the direction that the camera may be viewing.
 - A third type is pinhole video cameras, which are discussed separately below.
 - Cameras are available in a broad variety of qualities.
 - *Advantages:* Least costly.
 - *Disadvantages:* Require multiple cameras for multiple views.



FIGURE 16.2 Video Cameras

- *Exploits:*
 - Conduct crime outside the field of view of the fixed camera, which is more difficult with dome cameras as they often conceal which direction the camera is viewing.
 - Aim a laser at the imager to blind it.
 - Spray paint over the lens or enclosure glass.
- Pan/Tilt/Zoom Video Cameras
 - *Description and application:* Pan/tilt/zoom (PTZ) cameras allow the viewing of multiple angles and zoom ratios, thus permitting a very versatile point of view for the camera. Most PTZ cameras are enclosed in domes and may be used indoors or outdoors. Multiple mounts are available depending on the configuration needed.
 - *Advantages:*
 - Multiple views and zoom ratios are available.
 - Dome PTZ cameras conceal the direction of the camera view.
 - *Disadvantages:*
 - Camera can only view one thing at a time. Other areas within its total hemisphere of view will not be seen.
 - Nondome PTZ cameras are obvious as to their direction of view.
 - *Exploits:*
 - Create a diversion to attract the attention of the guard viewing the camera, who will point the camera to the diversion, allowing crime to be committed outside the field of view of the PTZ camera.
- Pinhole Video Cameras
 - *Description and application:* Pinhole cameras are conventional cameras fitted with a pinhole lens that is virtually impossible to detect. When mounted properly, only the tiny lens opening (2 mm) is exposed, thus appearing only as a fleck of dust on the wall.
 - *Advantages:*
 - Aesthetics are high, the camera does not intrude into the visual environment.
 - The camera is discreet.
 - Threat actors would not know they are within a camera's field of view.
 - Pinhole cameras may provide a view inside hostage situations after all other cameras in the area have been disabled, allowing authorities to coordinate a response with the fewest possible casualties. As hostage terrorist attacks increase, this becomes an increasingly valid countermeasure.
 - *Disadvantages:*
 - Concealed cameras may not be acceptable in some areas due to policy or cultural reasons.
 - A camera lens provides limited light, so bright light must be available within the scene view. Supplemental light can be provided by infrared illuminators configured as other normal types of fixtures.
 - *Exploits:* None.

- Day/Night Imagers
 - *Description and application:* Some cameras are available with day/night imagers that allow the camera to convert from color (day) to black/white (night) operation when light levels fall.
 - *Advantages:* Better sensitivity with black/white imager at night.
 - *Disadvantages:* Unless light is very low, the image may be more readable in color, even in low light.
 - *Exploits:* Same as other cameras.
- Analog Cameras
 - *Description and application:* Analog cameras provide National Television Standards Committee (NTSC) or Phase Alternating Line (PAL) images compatible with older television standards.
 - *Advantages:*
 - Comparatively inexpensive.
 - Single standard, easily converted to any digital standard.
 - Especially well suited to very small installations where inexpensive digital video recorder with analog inputs is used to record and view cameras.
 - Analog cameras do not allow hacking into the security system network when used outdoors, as might digital cameras. This can be an important feature when using digital systems and there are outdoor cameras to monitor and record.
 - Analog cameras arguably provide more reliable operation outdoors than digital cameras to date.
 - *Disadvantages:* Most analog cameras will have to be converted to digital before 2015. This can be done with the addition of a digital codec.
 - *Exploits:* Same as other cameras.
- Digital Cameras
 - *Description and application:* Digital cameras provide Transmission Control Protocol/Internet Protocol (TCP/IP) images in a variety of digital compression formats, including JPEG, Motion JPEG, MPEG1, 2 and 4, Wavelet, and H.264.
 - *Advantages:*
 - Inherently digital signal so that camera can easily be scaled into an Enterprise System Framework of long-distance archiving and monitoring of hundreds to thousands of cameras.
 - Images can be processed for intelligent video algorithms.
 - Images can be enhanced.
 - Redundant archiving is possible.
 - Viewing across many sites and long distances is possible.
 - Megapixel digital cameras provide extreme detail.
 - *Disadvantages:*
 - For storage, large data files require large storage systems.
 - Multicast digital systems are required when camera count exceeds 50.
 - *Exploits:* Same as other cameras.
- Digital Fish-Eye PTZ Cameras
 - *Description and application:* Digital fish-eye PTZ cameras are actually fixed megapixel cameras fitted with a 180-degree fish-eye lens.

This allows the camera to view and record an entire hemisphere, such as a ceiling-mounted camera viewing downward.

- *Advantages:*

- Cameras allow multiple PTZ views simultaneously.
- Cameras allow PTZ viewing within archive video, which is impossible with analog PTZ cameras.

- *Disadvantages:*

- Special software is required to view as a normal image.
- Megapixel cameras create very large digital files and thus require very large and expensive storage solutions.

- *Exploits:* Virtually none.

- Thermal Imaging and Short-Wave Infrared Cameras

- *Description and application:* Thermal imaging cameras view heat signatures rather than visible light. They are especially useful for viewing at night under very limited light and through smoke or fog (smoke and fog diminish performance).

- *Advantages:* Can view in total darkness, especially well over long distances with cooled thermal cameras, less range with uncooled cameras. Short-wave infrared cameras can also view in virtual total darkness.

- *Disadvantages:*

- Cost is high.
- Extreme fog or fog over long distances can diminish the performance of the camera.
- Maritime fog affects performance more than ground fog because maritime aerosols have, on average, greater particle radii than rural and urban aerosols.*

- *Exploits:*

- Carry out attack in very foggy conditions and far from an infrared (IR) camera.

- Video Analytics (Intelligent Video Software)

- *Description and application:* Video analytics software processes digital video images to help find useful information that implies possible unauthorized or criminal behavior. System alerts console operator to view camera to confirm unwanted behavior. Many algorithms exist, including:

- Line of crossing
- Left article
- Removed article
- Unusual crowd behavior
- Loitering
- Unauthorized direction of movement
- Behavior recognition
- And many others

- *Advantages:* Allow unintended operation of hundreds to thousands of cameras without missing relevant and important alerts to possible improper behavior.

- *Disadvantages:* Expensive, but truly empowers large video systems.

* FLIR® Technical Note, “Seeing through fog and rain with a thermal imaging camera,” FLIR Commercial Vision Systems, B.V. Netherlands (www.flir.com).

- *Exploits:* None, as no offender could know that there is analytic software operating, and criminals have been known to exploit the fact that most large video systems (such as transit systems) are not well watched.

Consoles and Management Offices

- Security Command, Control, and Communications (C³) Consoles
 - C³ Consoles allow the viewing of multiple systems across campuses and great distances, including across state and national boundaries. This allows significant supervision over security monitoring and access control functions for an enterprise organization. C³ Consoles also help organizations uniformly apply corporate security, safety, and operations policies throughout the entire enterprise. C³ Consoles include two or more monitoring stations that monitor video, alarm/access control, and security voice communications throughout the enterprise. They are sometimes integrated with building engineering monitoring functions to provide a complete facility-wide view of a campus for security, fire, HVAC (heating, ventilating, and air-conditioning), safety and elevators from a single location, thus enhancing the cost-effectiveness and coordination of operations across security and building engineering functions.
- Lobby Consoles
 - Lobby consoles are the “face” of security to many public users. These consoles enable console offers to service its public by providing information on access credentials and authorizations for employees and visitors. The consoles often also provide a secondary alarm and video station for off-peak hours use. (Lobby consoles should not be used for monitoring video or access control assistance during peak business hours.)
- Photo ID Badging Stations
 - Photo ID badging stations include:
 - Cameras
 - Backdrop
 - Lighting
 - Mirror for readying photo session
 - Badging workstation with photo ID software
 - Badge printers
- Security Management Offices
 - Security management offices should include:
 - Office for the manager and lead supervisor
 - Receptionist
 - Photo ID badging station
 - Interview room (for subjects of interest)
 - Toilets
 - Break room
 - Mustering room
 - Training center (often combined with mustering room)

Security System Archiving Technologies

- *Description and application:* There are two basic types of security archiving technologies: analog and digital.



FIGURE 16.3 Digital Video Servers

- *Analog:* Analog technologies use videotape to record analog video. These are rapidly falling into disuse and are being replaced by digital storage technologies.
- *Digital:* There are two main types of digital storage technologies:
 - *Digital video recorders (DVRs):* DVRs are purpose-built computers that store video for a small number of cameras. Some of these can be networked together, however none provide the flexibility of server-based archivers. These are most appropriate for small systems with limited budgets that will never see extensive system growth or other than very basic operational functionality. (See also Figure 16.3.)
 - *Server-based archivers:* Server-based archivers utilize the following types of devices to manage and store video:
 - *Directory server:* Manages where live images are directed (which cameras to which workstations).
 - *Archive servers:* Manage the recording of between 32 and 70 cameras depending on the resolution and frame rate. A few systems can record more.
 - *Storage media:*
 - *Fiber channel disks:* Very high throughput systems (most expensive).
 - *SCSI-disk systems:* Medium high throughput.
 - *SATA-disk systems:* Lower throughput.
 - *Tape storage:* Long-term storage on the shelf or in an automatic tape carousel.
 - *DVD storage:* Long-term storage on the shelf or in an automatic DVD carousel.
 - *Solid-state disk storage:* A large-capacity memory chip solution that is an emerging technology intended to replace disk types above.
 - *Storage systems:* All of the above can be configured into any of the following:
 - *Internal storage:* Storage within the archive server, local to the operating system.

- *Network attached storage (NAS)*: A box of disks, DVDs, or tape storage designed to be attached to the server network. Files appear to be on the network, not attached directly to the operating system.
- *Storage area network (SAN)*: A network of storage boxes to which the server network attaches in a way in which the storage devices appear as though they are locally attached to the operating system.
- Digital Storage Solutions Advantages and Disadvantages:
 - Digital video recorders (DVRs) are cost-effective for very small applications but do not provide the flexibility to manage large systems for other than the most basic functions.
 - Internal storage is very inexpensive, but lacks large capacity.
 - NAS (network attached storage) offers higher capacity, but slower throughput.
 - SANs (storage area networks) offer the highest and most effective use of video digital data. Some SANs use creative file management to employ low-cost SATA drives for virtual very high throughput otherwise not possible without fiber channel connections.
 - Fiber channel offers very high throughput but is most costly.
 - SCSI (Small Computer Systems Interface) and iSCSI offer medium throughput but are most well suited to small applications or as extended short-term storage (from 2 to 30 days).
 - SATA offers lowest cost but also lowest throughput. Some SANs use creative file management to make SATAs “appear” to have high throughput by spreading files across multiple disks for simultaneous recording of segments rather than recording entire files onto a single disk. The SAN then pieces the file segments back together for viewing.

Security System Archiving Schemes

- Immediate and Long-Term Archiving
 - *Fiber channel*: Fiber channel offers *immediate* access to very large amounts of video data. It is best used for large systems (over 70 cameras) with centralized storage for immediate access (up to 2 days). Its cost generally prohibits its use for longer-term storage.
 - *SCSI*: SCSI disks offer immediate access to small systems and short-delay access (a few seconds to a minute delay) to larger systems.
 - *SATA*: SATA disks offer reasonable delay for their minimal cost on larger systems (several seconds to a minute depending on the system software).
 - *Tape/DVD*: Tape and DVD storage offer lower-cost long-term retrieval of video archives without the cost of many multiple disk drives. Excess tapes or DVDs are stored on the shelf or cassette for retrieval when required. This retrieval process inserts a noticeable delay of up to several minutes while the system database locates and then retrieves and loads the video data for viewing.
 - *Solid-state storage*: Solid-state storage has great promise but is limited to experimental versions as of the date of this book.

- *Description and application:*
 - *Small systems*
 - DVR
 - One archive server with internal disks and one tape drive
 - *Medium systems*
 - A few archive servers and a small NAS or small SAN system
 - Long-term storage with one or more tape drives or a small tape carousel retrieval system
 - *Large systems*
 - Many archive servers and a large SAN system using three types of data storage:
 - Very short-term storage: Fiber channel disks on SAN switch and server (instant retrieval up to 2 days)
 - Short-term storage: SCSI or SATA SAN (near instant retrieval up to 2 weeks/1 month)
 - Long-term storage: Tape or DVD carousel on SAN
- *Redundant archiving schemes:* For business continuity, redundant archiving is recommended (to handle routine and emergency maintenance and loss of archives due to accident, natural disaster, or intentional harm).
 - *Basic redundancy:* One spare archive server on location to handle emergencies or maintenance.
 - *More adequate redundancy:* Two spare archive servers to handle emergency while maintenance is being conducted.
 - *Full redundancy:* Full replacement set of all primary archive servers and short-term and long-term storage off-site connected by multigigabit fiber connection.
 - All these systems typically use RAID5 or RAID6 arrays.
- *Advantages and disadvantages:*
 - *Basic redundancy:* Least expensive option, very limited redundancy, better than none at all.
 - *More adequate redundancy:* Provides for on-site redundancy of up to two archive servers, reasonable cost.
 - *Full redundancy:* Most preferred operationally, most expensive.

Security System Infrastructures

- General
 - Prior to 2003, security systems used three common types of infrastructures:
 1. Video: Coax or analog fiber.
 2. Intercom: Two- or four-wire analog audio plus call/control.
 3. Alarm/access control: RS-485 and minimal use of TCP/IP for interconnecting systems between buildings.

There were rare exceptions to these, but the three types above were the most common. This all changed beginning in 2000, and by 2003 there was a substantial movement toward a total digital infrastructure for all but the smallest systems.

- Security System Digital Infrastructures: The security industry's move to digital infrastructure provided for the implementation of many functions not possible with analog and proprietary infrastructures. These included:

- The ability to develop truly enterprise systems, operating as one across many cities and states and nations
- Truly scalable systems
- Centralized and remote redundant monitoring of many video, alarm/access control, and intercom systems
- Video analytics

Security digital infrastructures can take forms of wired, fiber, and wireless.

- Wired
 - Wired infrastructures utilize CAT-5 or CAT-6 cable and digital switches and routers in a variety of configurations. The most common of these include
 - *Small systems*: Simple switch architecture, connected by a gigabit backbone. A tree architecture is common, though sometimes ring architectures are used. This will be a total CAT 5/6 network.
 - *Medium systems*: Hierarchical switch architecture, with branches segmented by Virtual Local Area Networks (VLANs). Either a tree or ring architecture may be used. Fiber switch backbone may be used. The network will include core and edge switches, where core switches connect together and also connect to servers, SANs, and routers. Edge switches connect to edge devices (cameras, access control controllers, intercoms, etc.) and to core switches. Workstations may reside on either core or edge switches, depending on preference.
 - *Large systems*: Redundant hierarchical switch architecture, using edge (access layer) switches to connect field devices, core switches to connect to servers and SANs, and may use distribution layer switches as the system becomes larger. All switches may be partially or fully redundant. All switches will connect by fiber using ever-increasing capacity as one nears the core layer. For example:
 - 100 MB edge device
 - 1 GB edge switch to distribution layer switch
 - 10 GB distribution layer to core switch
 - 10 GB+ core layer
- Fiber-Optic Cable
 - *When to use fiber optic cable*: Fiber should be used whenever distances exceed ratings of CAT5 or CAT6 cables (90 meters/270 feet),^{*} or when capacities exceed the ratings of the CAT5 (100 MB)[†] or CAT6 (1 GB). For any speed above 1 GB or distance over 90 meters, fiber should be used.
 - *Types of fiber*: There are two types of fiber: single mode and multimode. Multimode fiber is the least expensive (usually plastic), and the transmitters and receivers are usually LED sources rather than lasers. Maximum distances vary, up to several miles. Single-mode fibers use glass cores instead of plastic, and their transmitters and receivers use lasers instead of LEDs. Single-mode fiber and its transmitters/receivers are thus more expensive and provide higher capacity and distance.

^{*} Note that the actual maximum engineered CAT 5/6 distances are 100 meters or 300 feet, but it is best to provide some engineering factor for safety with digital video signals.

[†] Note that CAT5 and CAT5e cables can run gigabit speeds but are not certified for such.

- Wireless
 - General
 - All wireless options are less reliable and secure than wired or fiber optic options regardless of any implications to the opposite by anyone.
 - Anyone thinking to use a wireless option should conduct a field radio frequency survey to assure that the desired frequency is free and available and that the environment will support the operation of the system on the desired frequency.
 - Licensed versus Unlicensed Options
 - Wireless solutions come in two broad variants: licensed and unlicensed options. The specific frequencies requiring licensing vary from country to country, so this book cannot provide uniform worldwide guidance on this topic. The designer should confirm that the solution selected is licensed if required.
 - Benefits of each:
 - Licensed options could provide more security in that fewer people are permitted to operate on the designated frequency. Licensed options ensure that no one else will operate on the assigned frequency.
 - Unlicensed options do not have the cost or formalities burden of licensed options but provide no guarantee of continued clear operations, as anyone else could also begin using the same unlicensed frequency in the same space, thus diminishing its capacity in that environment. That is to say that one could set up an unlicensed wireless system only to discover that months later it will not support its desired operations due to the installation of a nearby wireless system on the same frequency.
- 2.4 GHz
 - The most common unlicensed frequency worldwide is 2.4 GHz, which supports 802.11 b/g/n operations. This frequency can support up to three simultaneous video channels in the same airspace. This frequency has the most amateur and commercial users, and thus, the highest probability of interruption by adjacent users.
- 5.8 GHz
 - 5.8 GHz supports 802.11a operations which can support up to ten simultaneous video channels in the same airspace. This frequency also has far fewer users, and thus, less likelihood of interruption by other users. 5.8 GHz may be licensed or unlicensed depending on the locale.
- 900 MHz
 - 900 MHz is the forgotten frequency, very seldom used. It supports short distances but can pass through trees, leaves, and so forth, better than the two frequencies above. 900 MHz may be licensed or unlicensed depending on the locale.
- WiMax
 - WiMax is an emerging technology that should support more reliable operations. WiMax is typically licensed depending on the locale.
- Wireless Mesh Networks
 - Wireless mesh networks create a fully redundant network in which there are multiple lines of communications possible, thus making a more robust and redundant network.

- Microwave
 - Microwave communications are licensed in most areas and provide secure communications line of sight up to several miles depending on the equipment and frequency.
- Laser
 - Laser communications provide very secure transmissions over line of sight up to several miles.
- Antennas: Two types of antennas are available: *directional* and *omnidirectional*. Omnidirectional antennae should be used whenever signals from several cameras are being gathered together at a single access point. The omnidirectional antenna should only be used on the access point. For all outdoor remote cameras, directional antennae are best, and whenever possible, it is also best to use directional antennae at the access points as well, only unless multiple cameras signals are collected from several directions. For a complete discussion on antennae, see *Integrated Security Systems Design*.*

Lo-Tech Elements

Locks

- Electrified Mortise Locks
 - Electrified mortise locks are made from standard mortise locks that are fitted with a solenoid (to unlock the door) and can also be fitted with a request to exit switch on the handle (so that the request to exit is sent when the handle is turned, thus bypassing the normal door alarm), and they can also be fitted with a door closed switch or door locked switch. Electrified mortise locks are very secure and require no special knowledge to use and comply with all known codes for nonfire-egress doors.
- Electrified Panic Hardware
 - Electrified panic hardware (EPH) are standard mechanical panic hardware (crash bars) that are fitted with a solenoid (to unlock the door) and can also be fitted with a request to exit switch in the push bar. EPH are available in mortise, rim, and concealed and exposed vertical rods. EPH fulfill requirements for all known codes.
- Magnetic Locks
 - Magnetic locks are fitted at the top of the door and supplement other door hardware with centrally controlled locks. Magnetic locks are often fitted to existing doors with existing locks to simplify the lock installation. Egress is from an infrared request to exit motion sensor above the door, by a switch in a panic bar, by a labeled pushbutton beside the door, by central command from the console, by a fire alarm interface, or by a special emergency unlock pull station (similar to a fire alarm pull station). Magnetic locks must receive code approval in most jurisdictions on a case-by-case basis, and special attention should be paid to the fire alarm interface and other safety measures to

* Thomas L. Norman, *Integrated Security Systems Design — Concepts, Specifications, and Implementation* (Burlington, MA: Butterworth Heinemann, 2007).

help assure that persons are not accidentally locked into the space as has occurred many times due to bad design.

- Delayed Egress Hardware
 - Delayed egress hardware couples a magnetic lock with a crash bar, a countdown timer, and a local alarm. Signage advises the user to push and hold the push bar for a certain number of seconds (usually 15 to 30) after which the door will open. During that time, a countdown timer displays the count down to zero and an alarm is sounded to discourage casual use. Delayed egress hardware provides for high-security openings and a certain way of exiting no matter what.
- High-Security Electric Locks
 - A few companies manufacture high-security hardware, including:
 - Four- and six-point electrified deadbolts (for single or double doors)
 - Detention and Housing Authority quality door hardware are made to stand up to very heavy intentional abuse that would cause the immediate failure of normal locks.
 - Note that four- and six-point electrified deadbolts on robust doors are virtually impossible to breach with conventional tools, excluding only industrial diamond saws and certain very robust frame spreaders.
- Drop-Bolt Locks
 - Drop bolts are out of favor due to door alignment problems, which cause lock jamming. However, they can be used on storeroom doors. They should never be used on occupied rooms. Generally, these have been replaced by magnetic locks. I do not recommend the use of drop bolt locks on any door.
- Electrified Cylinder Locks
 - Very insecure conversions of mechanical cylinder locks. Avoid these always.
 - Lock Power/Fire Alarm Supervision
 - Lock power should be centralized and backed up by a generator and uninterrupted power supply. The final power feed to the lock power supply should be serviced/interrupted by a relay that is supervised by the fire alarm system, thus assuring that all magnetic locks will permit passage during a fire alarm. The circuit should be equipped with a test switch that also sends an alarm to the alarm/access control system to log the test event.

Revolving Doors

Revolving doors and full height mechanical turnstiles provide positive access control — that is, one card, one entry. This prohibits tailgating of unauthorized persons behind authorized users. When used at egress points, the revolving doors and turnstiles should be coupled with a conventional leaf door with a delayed egress hardware system.

Mechanical and Electronic Turnstiles

- Mechanical (sports venue type) turnstiles and electronic turnstiles are becoming more well used due to the focus on assuring clearance of persons entering buildings. The user is granted access through the turnstile, usually through a visitor card. Employee cards are also valid at the turnstiles. Turnstile configurations include:

- Tripod (sports venue type)
- Glass wing
- Drop paddles
- Swing-away paddles
- No paddles (alarm only on violation) — these have fallen into disfavor
- Electronic turnstiles help ensure positive access control in a very aesthetic fashion. Throughput varies from one person per second up to one person every 2 to 3 seconds.

Vehicle Gates

Vehicle gates can be configured as lift-arm, swing fabric gates and sliding fabric gates. Lift-arm gates provide the least security but deploy quickly. These should be used wherever the arm is manned and where security is lax, such as to a parking lot. Sliding and swing fabric gates (imagine chain-link or estate fence) provide security also against pedestrians (which lift-arm gates do not) but deploy more slowly.

Deployable Barriers

- Vehicle Barriers
 - Deployable vehicle barriers come in two types; high-security and low-security.
 - High-security barriers are capable of stopping vehicles traveling at speed with a payload in a very short distance, usually about 1 meter of overtravel. On most high-security barriers, destruction of the vehicle and death or serious injury to its occupants is a probability if the vehicle is traveling at speed and may occur even if the barrier deploys under a standing vehicle. Configuration of these types generally includes:
 - Deployable bollards
 - Phalanx (rising wedge) barriers
 - Cable-beam barriers
 - Certain newer barriers can deploy without causing serious damage or injury by stopping the vehicle in a controlled fashion. Some of these also serve as mildly effective pedestrian barriers. Configuration of these is typically as a rising web of aircraft-landing capture cables and nylon webbed fabric.
 - Low-security barriers are usually configured as rising arms (parking control arms). These can also be configured with antipedestrian barriers.
- Pedestrian Barriers
 - I have for many years advocated the use of deployable barriers inside public buildings to disrupt terrorist takeover attacks, such as occurred in the November 26, 2008, attack on hotels in Mumbai, India. The use of motorized operable walls, roll-down grilles, and deployable doors has the potential to save many lives when a hostage-oriented paramilitary attack occurs. These are appropriate for any public or commercial building where an attack by armed militants is a possibility. The use of deployable barriers requires close coordination with fire department authorities. Barriers should be placed mid-point between fire stairwell locations and where no sneak-paths are available. They are especially effective against “moving shooter” attacks such as in the Mumbai attack as they contain the shooter to a small segment of the building while allowing victims to exit nearby to safety. The shooter will not use the exit, as he will be captured by armed police response forces. These should

be used in cases where two exits are possible in each segment. My recommendation of these was long considered radical until their merits recently became obvious.

Lighting

Lighting can be used in four ways: Lighting can improve the safety of legitimate users, indicate occupancy when buildings are occupied and imply occupancy when buildings are unoccupied, increase the risk of discovery upon entry, and disrupt a security event.

1. *To improve the safety of legitimate users:* Lighting should be used on all natural vehicle and pedestrian pathways along with clear sight-lines to help assure that offenders cannot easily approach legitimate users unsuspected.
2. *Lighting to indicate occupancy:* Lighting can be used to imply that a facility is occupied. For burglaries, indications of occupancy are the number one prevention technique. Studies have shown that burglars will nearly always avoid residential and commercial buildings they believe to be occupied.* Lighting should be scheduled and used with other indicators such as parked cars or sounds (radio station, etc.).
3. *Lighting to increase the risk of discovery upon entry or exit:* For parking lots, lighting can be used to make the movements of burglars more obvious, especially around logical points of entry and the approaches to those areas.
4. *Lighting to disrupt a security event:* Once a presence is detected, lighting can be used to disorient and disrupt the offender. The turning on of lights in response to motion sensed, especially inside the structure, makes the offender believe he or she has been detected and may cause the offender to abandon the attack. For very sensitive facilities, turning off lighting in an unoccupied building can help to disorient the attacker and allow the response force to follow the subject, especially where infrared enabled cameras are used indoors.

Signage

Two types of signage assist in the security program: *way-finding signage* and *security warning signage*.

- Way-finding signage assists legitimate users in finding their way through a facility to their intended destination by “pointing the way.” Well-designed way-finding signage has two distinct advantages: (1) assisting users and (2) reducing the time spent informing users of directions. The second of these helps improve the overall security program by allowing security personnel to focus on exceptions rather than on normal behavior. This is an elemental principle of security operations — that security personnel should focus on exceptions to the extent possible and that all matters related to normal behavior should not require the intervention or interruption of security personnel from their normal duties. Good way-finding signage actually begins with good architectural and departmental planning. From the time a visitor or new employee enters the building, their attention is on finding their way to their intended destination. Especially, first-time visitors are

* Paul Cromwell and James N. Olson, *Breaking and Entering* (Florence, KY: Wadsworth, 2003): “90 percent of burglars we interviewed stated that they would not knowingly enter a residence where they knew someone was at home.”

generally unaware of any rules for visitors, such as signing in. Prominent signage guiding visitors to the reception desk is important. From there, either signage or map handouts are an effective way to guide visitors to their destination. For larger facilities, way-finding signage helps keep visitors on track. Sign colors can also help keep visitors guided more intuitively than language signs alone. Way-finding signs should be hierarchical in nature — that is, the signs will provide more detail as one progresses through the facility. For example, in the lobby, signage may indicate what floors certain departments are on, and room number ranges should be displayed just off elevator lobbies so that visitors are not wandering down the wrong halls looking for suites. Way-finding signage should also indicate where assistance and key services such as toilets are available. All signage should be readable from the distance intended. For example, at 1,500 feet, letters must be 2 feet high, however in an elevator lobby, 1-inch-high letters are sufficient. Signage must also take into account the speed with which the reader may be traveling. For example, letters must be larger the faster a reader is traveling in order to facilitate time to read and the distance that will take.*

- Security warning signage helps guide employees and visitors to the correct behavior by informing them of what is and is not considered acceptable. For example, at a LNG terminal, signage in large letters may warn watercraft not to approach closer than 1,500 feet of a vessel and cite the federal regulation requiring that distance. Signage may also state possible penalties. For example, it is common to see signs at airports declaring what items may not be taken in carry-on baggage and warn of possible arrest for violation. Security warning signage both guides correct behavior and removes the excuse of ignorance. All security warning signage should be based on laws or documented policies and procedures and should be stated simply and clearly and in a professional manner. Signage that is too wordy often does not get read and so fails in its intended purpose.

No-Tech Elements

Define the Deterrence Program

In general, the primary goal of any security program is deterrence. If the program is successful in that goal, then it is completely successful. If it is unsuccessful in that goal, then it is very costly and dangerous to remedy that shortcoming. Remember, a good security program has two primary elements:

- A baseline security program
- Specific countermeasures to address specific vulnerabilities

The baseline security program is composed of countermeasures that guide users to appropriate behavior through deterrence tactics and also help to detect, assess, respond, and gather evidence of any inappropriate criminal behavior. No baseline security program is effective as anything other than a mild deterrent against terrorist behavior.

The specific countermeasures to address specific vulnerabilities are intended to act as deterrents against terrorist behavior and unique opportunities for criminal behavior.

* Airmaster Letter Height Visibility Charts, 20 mph/2 kph, 4 inches/9 cm at 147 feet/45 meters, 65 mph/105 kph, 12 inches/30 cm at 477 feet/145 meters (www.airmastersales.com/hivisibility.html).

For the baseline security program, the deterrence package includes security patrols and posts, CPTED elements, a security awareness program, access control elements including both electronic and staffed, and a security investigations and intelligence program. The no-tech elements of these include patrols and posts, security awareness program, and the security investigations and a security intelligence program.

- *Security Posts:* The presence of security posts (also called fixed patrols) at property perimeter entries and exits and at building entries is a constant reminder that the organization is vigilant about security. The effectiveness of security posts is entirely based upon the professionalism of the officers and equipment at the post. This is especially true for antiterrorism checkpoints (bomb and weapons detection). It is at this point that professional offenders will judge whether the organization's security program is all for show or if it is a serious challenge to their criminal intentions.

Remember, appropriate users see a security post and immediately think that the facility is secure, but professional offenders see every vulnerability and imagine quickly how to exploit the holes in the procedures. Thus, effective policies and procedures coupled with effective training and random scenario testing help ensure an effective deterrent.

- *Patrols:* Security patrols are one of the most effective deterrents because anyone on the premises with criminal intent is aware that they are at risk of being caught by a roving guard at any time. Patrols should not be predictable. That is, each time a guard patrols, he or she should vary the route and time so that the route is not predictable. This may include returning shortly to patrol checkpoints that were just visited minutes or even seconds ago. This kind of unpredictability helps assure that no one with criminal intent will feel safe from observation by a patrol officer.
- *Responses:* Professional offenders will often "test" the organization's response to a security event. Thus, responses to "nonevents" are as important as responses to actual security events. The timing, manner, and actions of the responding officers indicate to the offender how much of a challenge the security program will be to overcome. An effective response to a nonevent will nearly always deter an attack, according to interviews with known terrorists and criminals.
- *Security Awareness Program:* Security awareness programs have two objectives: (1) to help the organization's employees, contractors, and vendors to understand the organization's security policies as they relate to their own behavior and activities; and (2) to help create a safe and secure work environment by helping those constituents understand what behaviors are expected by the organization. Elements of a security awareness program often include the following:
 - *Security and way-finding signage:* These help the public and visitors find their way and help assure that unauthorized people do not go into areas where they should not be.
 - *Handouts:*
 - *Security rules:* These help visitors, contractors, vendors, and new employees understand their behavioral obligations while on the property or while working on the organization's projects.
 - *Security and safety guidances:* These help the organization's constituents understand concerns and issues that could affect their security and safety and how to take steps to assure their own security and safety while on the organization's property and in their daily lives. These can also include

such things as warnings about security and credit card scams that could affect the organization's constituents. Security and safety guidances are generally viewed as an added value to working with the organization by its employees.

- Verbal Guidance
 - Security personnel should be trained to provide verbal guidance to persons having questions (way-finding, security questions, etc.).
 - Security personnel should be trained to defer verbal guidance on subjects for which they are not qualified and direct the questioner to a better source (always to a manager).
 - Security personnel should always carry a pocket guide for security policies to aid in answering any questions.
 - Security personnel should be trained to escalate problems to supervisors or managers when they are confronted with a belligerent person.
 - Security personnel who have contact with the public should be trained in basic conflict resolution.
- Newsletters, E-mails, etc.
 - A security program periodical is a good way to transmit and focus the recipients on the organization's security mission.
- Security Investigations Program
 - There are security problems in every organization. These problems can be internal, external, or external with internal collusion. Security problems can be either immediate or chronic. Security offense perpetrators may be obvious or concealed.
 - Security investigations programs help uncover the concealed offenders and assemble the evidence necessary to prosecute the offender and to put an end to the offenses, if chronic.
 - Immediate offenses leave evidence of the offense which can be used to determine the methods and tactics of the offense, the asset used, taken, or destroyed, and the characteristics of the offender (time, method of entry and exit, concealment during the offense, etc.).
 - Chronic offenses also leave evidence (shortages, etc.). However, it may be difficult to tell when such shortages occurred and, thus, who suspects might be. Especially when organized crime is involved and when employees have been turned to be participants in or facilitators of the crime, investigations play a vital role in solving the problem.
- Security Intelligence Program
 - Intelligence is information that is relevant to the protection of the organization from possible harm. Intelligence allows management to position the organization to avoid harm.
 - Both security and related risk management should receive intelligence reports.
 - Reports should be analyzed for urgency and importance upon receipt. Urgent and important intelligence requires immediate action. Important but not urgent intelligence requires planning and coordination rather than immediate action.
 - Common organization formal intelligence programs include:
 - Contacts with law enforcement
 - Commercial security intelligence service

- Selected news feeds
 - Security blogs
- A word about commercial security intelligence services. I recommend that you subscribe to at least one good commercial security intelligence service in order to keep up with intelligence agendas. However, do not place complete faith in these to keep you informed. I will cite an example. One of the sources that I use is a very comprehensive service. However, I was amazed to note that as I was writing this book, in its weekly intelligence guidance for February 8, it had only one line February 12 on Lebanon. This was amazing to me because February 12, 2009, is the 1-year anniversary of the assignation of Imad Mugniyah (the military strategist for Hezbollah), whose assassination was blamed on Israel by Hezbollah. Even though tensions were high between the two countries and Israel conducted mock air raids over Lebanon in the days before the anniversary, this service made only an anniversary mention of this event and ignored that it had the potential to spawn a war between these two countries, indeed that Israel expected an attack and threatened war in response, all of which was published in its public press. At one time, this service had spot on guidance on the region, but things can change as quality sources move into and out of regions. Missing an event such as this in intelligence guidance is very concerning and shows a lack of analysis expertise on a critical region.
- How to develop intelligence sources:
 - Commercial risk analysts only have open-source information sources available to them. The challenge is to gather together as many sources as possible and filter them for relevance.
 - One good way to do this is to begin with Google Alerts. Set a Google Alert on one or more key words that are relevant to your needs. These may include the names of countries, industries, and security or terrorism. Google Alerts will feed relevant and irrelevant information to your mailbox daily. As you click on interesting articles, you can bookmark these sources, and you will begin to build a wealth of credible open-source news sources. To filter these, you can also subscribe to Usenet groups. For example, you can subscribe to Google Groups (one of the best) such as alt.security.terrorism and put in a keyword filter such as "Lebanon." This will return on a typical day over 4,000 relevant articles from all points of view.
- A few of the many other good sources include:
 - The NEFA Foundation (www.nefafoundation.org)
 - The Investigative Project on Terrorism (Steve Emerson — www.investigativeproject.org)
 - Jane's World Insurgency and Terrorism Portal (http://catalog.janes.com/catalog/public/index.cfm?fuseaction=home.ProductInfoBrief&Product_id=98796) — a subscription source
 - www.PlanetData.net/sites/Intelligence/
 - www.Businessmonitor.com
 - www.defensereview.com
 - www.asisonline.org
 - South Asia Terrorism Portal (www.satp.org)
 - You will soon develop many others

- News connections
 - One of the best is the World News Connection (WNC), which is a consolidation of up-to-date news from local news sources all over the world, all translated into English. The WNC is a commercial (for fee) subscription service of the U.S. Government National Technical Information Service (NTIS) by the Open Source Center (OSC) and is a service of the Commerce Department. Though some consider it too expensive, I believe that WNC may be the most comprehensive open-source information source in the world.
- Emergency Services Liaison Program
 - An emergency services liaison program is essential to assure that when an emergency occurs, security personnel manage the scene to facilitate rapid and uninhibited response to emergency personnel and to manage curiosity seekers.
 - The program should be planned in coordination with fire, paramedic, and police personnel and should include the following essential elements:
 - Triage the scene to determine if emergency services are needed, and which agency should be called.
 - Notify emergency responders and notify management of the call to emergency responders.
 - Manage the scene, including taking actions to protect anyone injured or ill including life-preserving measures.
 - Secure the scene to protect the victims' privacy from curious onlookers and to protect evidence.
 - Mitigate any further damages, such as from fire, to the extent possible.
 - Facilitate emergency responders to rapidly locate the scene of the emergency.

Define the Response Program

- Communications: The most important element of any response is communications. Communications include:
 - Communications between the console officer and responding patrol officers, providing them with information about the security situation, the event, and the suspects.
 - Communications between the console officer and security management or supervisors.
 - Communications between the console officer and any offenders within view of a video camera.
 - Communications between the console officer and anyone seeking assistance at an assistance phone or intercom.
 - Communications between security personnel and responding law enforcement.
 - Communication tools include security intercoms, telephones including mobile phones, and two-way radios.
- Guards:
 - Guards or security officers are the security program's enforcement staff.
 - Guards should be well versed in all of the organization's security policies. No statement should be made by any guard regarding any security matter that is not founded from security policy.

- Guards have several basic duties, including posts, patrols, and office duties, including reports, training, and photo ID badging.
- Guards may be in-house or contracted. Advantages of contracting guards include:
 - Scalable staff, meaning increased and decreased staffing on demand.
 - Guards work for the guard company, not directly for the organization, so any improper guard action is mitigated to varying extent by the guard company and their insurance. The primary role of a guard company is to provide trained and qualified guards. Any failure in that is the responsibility of the guard company.
 - Advantages of in-house guards include greater control over training. Some organizations utilize a mixture of contracted and in-house guards, with key staff in house and line staff contracted.
- Vehicles: Vehicles may include automobiles, trucks, motorcycles, bicycles, and golf carts, depending on the needs of the patrol. A vehicle's primary roles include patrols and response.
- Armed/Unarmed: Guards may be armed or unarmed. Armed guards are appropriate only with excellent firearms training and especially training as to rules of engagement. Organizations should keep in mind that any accidental or improper shooting is on the organization's shoulders, with some mitigation by the guard company, if contracted.
- Response Training Requirements:
 - Security staff must be trained to respond properly to a variety of security and safety events. Training should include:
 - Security and safety policies
 - Security laws, especially concerning laws regarding citizen's arrest
 - Security event identification, verification, and assessment including what kind of response is most appropriate
 - Security staff position awareness (where are all staff at all times)
 - Response team selection and dispatching
 - Security event management including observation and directions using closed-circuit television (CCTV) and intercoms/radios
 - Suspect apprehension and citizen's arrest
 - Suspect holding for law enforcement
 - Evidence gathering and incident report generation including note taking and report generation
 - Handing over suspect, evidence, and incident report to law enforcement
 - Testifying in court
- Security-Related Medical Emergencies:
 - Security staff is often the first responder to any emergency. Security staff should be trained in the types of emergencies and how to mitigate injuries or medical conditions, control the scene, and obtain help from emergency responders.
 - Security staff should be versed in all common types of medical emergencies, including:
 - Common injuries
 - Heart attack and stroke
 - Heimlich maneuver
 - Rendering cardiopulmonary resuscitation (CPR)

- An automatic electronic defibrillator should be kept within minutes from every location on the facility, and all security staff should be trained in its use.
- Scenario training is important as it points out how the security staff will interact with everyone in an emergency, including rendering aid, controlling the scene, and obtaining help from civic emergency responders.

Define the Evidence-Gathering Program

- General: Every security event leaves its evidence which could include witness statements and video or forensic evidence. All evidence must be protected, noted, and preserved for law enforcement. Any activities by anyone including security staff could disturb evidence and reduce or eliminate its value. All security organizations should also maintain a supply of crime scene tape to protect evidence prior to the arrival of police investigators.
- Video and Audio Archiving Elements:
 - All video and audio channels should be recorded and archived for a suitable period to determine if a security event has occurred. For most events, this may be 2 weeks to 1 month. For some types of events, longer periods may be required.
 - Only archiving methods that are court acceptable should be used.
- Crime Scene Security Principles and Evidence Preservation:
 - Security staff should be trained in crime scene security principles including how to secure a crime scene for law enforcement.
 - All possible evidence must be preserved.
- Witness Statements:
 - All security staff should be trained in taking witness statements. This includes:
 - Identifying possible witnesses
 - Separating witnesses from each other so that stories do not get mixed
 - Interviewing witnesses by asking nonleading questions which should include:
 - What did you see?
 - How did the event unfold?
 - Identification of suspects
 - Witness contact information
 - Witness statement reports: From the witness statement notes, develop reports that are unbiased, accurate (including any discrepancies in statements), and clearly written. The reports should agree completely with witness statement notes. Notes should be preserved.
- Follow-Up Investigations and Training: For any security event that is not immediately handed over to law enforcement, a follow-up investigation will occur. Investigations should only be handled by qualified investigators.

SUMMARY

All security countermeasures have the goal of adjusting the behavior of potential threat actors so that they do not pose a threat to the organization. This is done in three ways:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terroristic behavior.
2. Detect, assess, and respond to exceptions.
3. Design the program to mitigate any potential harm from hazards and threats.

There are two primary types of countermeasure implementations, each having three elements:

1. The Baseline Security Program (BSP)
2. Special Countermeasures to Address Special Vulnerabilities

Each of these have hi-tech, lo-tech, and no-tech components. Both the BSP and special countermeasures are necessary to cope with all the conditions that an organization may confront. The exact makeup of those programs is the result of recommendations from the risk analysis.

Baseline Security Program

The BSP should accommodate normal day-to-day operations and identify unwanted exceptions so that they can be handled. The BSP is not designed to cope with highly unusual conditions such as acts of terrorism. The BSP should include all three elements:

1. Design an environment that encourages appropriate behavior and discourages inappropriate, criminal, or terroristic behavior.
2. Detect, assess, and respond to exceptions.
3. Design the program to mitigate any potential harm from hazards and threats.

Specific Countermeasures

The risk analysis may uncover certain threats that are not day-to-day threats but for which the security program must be prepared to handle. These will require specific countermeasures in addition to the baseline security program. Three common elements of specific countermeasures include:

- Terrorism and Major Crimes Deterrence Program
- Emergency Preparedness Program
- Disaster Recovery Program

Countermeasure Selection Basics

Both the baseline security program and special countermeasures utilize hi-tech, lo-tech, and no-tech elements.

Countermeasure Selection and Budgeting Tools

INTRODUCTION

At the completion of this chapter, you will understand what makes a security countermeasure effective or not effective, the functions of security countermeasures, infiltration and attack scenarios, attack objectives, criminal offender types, criminal offender countermeasures, how to develop countermeasure effectiveness metrics, and how to develop a Decision Matrix to help decision makers reach consensus on a specific countermeasure when there are many points of view to consider.

THE CHALLENGE

Security organizations have historically been astoundingly poor at measuring their cost-effectiveness and, for that matter, even their effectiveness at securing the organization.

Management is about metrics. The age-old management adage is “If you can’t measure it, you can’t manage it!”* But the security industry has been woefully inadequate not only in measuring its success in the execution of its program, but also of the recommendation of countermeasures.

With the exception of national laboratories such as Sandia, most risk analysts have paid little interest to any measure of the effectiveness of their countermeasure recommendations. At best, risk analysts would scale their program recommendations with “good, better, best,” or some such qualitative estimate on which no calculations whatsoever had been conducted.

This is most unfortunate, as clients deserve to know how well the money being budgeted for security programs is likely to succeed in its mission. I think that most analysts have not addressed effectiveness and cost-effectiveness for two reasons. The first is that most major risk analysis methodologies have no countermeasure effectiveness metric (with the notable exception of the Sandia model, which has these functions). The second is that the metrics that do exist require exceptional depth of analysis, time, and money to carry out, beyond the budget and capabilities of most analysts and arguably of most commercial organizations.

But, like anything else, if you can conceptualize the problem, you can create a solution.

* Credited to W. Edwards Deming, Peter Drucker, Robert Kaplan, and others variously from different sources.

COUNTERMEASURE EFFECTIVENESS

First, in order to measure countermeasure effectiveness, we have to ask: “Effective against what?” — “Against what threat?” “Against what purpose?” “Using what formula?”

FUNCTIONS OF COUNTERMEASURES

We begin by examining the functions of security countermeasures. There are only seven things that any security countermeasure can ever hope to do:

1. Control access
2. Deter an attack
3. Detect an attack
4. Help the security force assess the attack
5. Delay the attack
6. Respond to the attack
7. Collect evidence of the attack

Various countermeasures do one or more of these things, more or less well, at greater or less cost. Some countermeasures are effective against some threat actions and not against others. We now have four dimensions of comparison for countermeasures:

1. How many functions does the countermeasure fill?
2. How well does the countermeasure perform each function?
3. What threat actions is this countermeasure useful against?
4. How much does the countermeasure cost?

Examples

Figures 17.1 and 17.2 illustrate why the function of a specific countermeasure’s effectiveness can only be measured based upon the threat it is against. In the simplistic examples below, no scale is given as to effectiveness (it is shown as binary effective/not effective), because specific countermeasures are not under review, just the category of countermeasures against generic criminal or terrorist threats.

Figure 17.2 illustrates that countermeasures that are effective against criminal threats may be of little use against a terrorist threat.

The more specific the threat, the more specific the countermeasure can be estimated. For example, glazing with blast film may reduce smash-and-grab crimes and reduce the loss of life in a minor explosion but is of no use if the bomb in question is a truck bomb at the curb of the building.

Also, specific countermeasures in specific locations have varying degrees of effectiveness. A normal-resolution closed-circuit television (CCTV) camera with a wide-angle lens on a camera pole can help describe the subject in question in terms of height, weight, build, sex, clothing, armament, and actions, but it should not be considered capable of identifying the specific individual by facial recognition.

Criminal Threat Countermeasure Functions								
Security Function	Alarm	Access Control	CCTV	Intercom	Barriers	Locks	Lighting	Landscaping
Access Control		X			X	X		X
Deterrence	X	X	X		X	X	X	X
Detection	X	X	X					
Assessment		X	X	X			X	
Delay		X			X	X		X
Response		X	X	X			X	
Evidence	X	X	X					
Functions:	3	6	5	2	2	2	3	2

FIGURE 17.1 Criminal Threat Countermeasure Functions

Terrorist Threat Countermeasure Functions								
Security Function	Alarm	Access Control	CCTV	Intercom	Barriers	Locks	Lighting	Landscaping
Access Control					X			X
Deterrence					X			X
Detection	X		X					
Assessment			X	X			X	
Delay		X			X	X		X
Response			X				X	
Evidence	X	X	X					
Functions:	2	2	4	1	2	1	2	2

FIGURE 17.2 Terrorist Threat Countermeasure Functions

Let me pause here to state one of the most important principles of security that any risk analyst must understand — *except for identifying persons carrying weapons or explosives, for terrorist threats on commercial, government, and critical infrastructure facilities, the only effective countermeasures are physical countermeasures.* I will say that again. Forget alarms, forget access control systems, forget CCTV systems, and

certainly forget intercom systems. Forget the security guard force. In most cases they will just become additional victims, typically among the first.

Electronics has little, if any, function except to identify weapons on pedestrians and vehicles and give eyes to Special Forces if the system is designed properly (that is, deny the system to the terrorists and give it solely to Special Forces). Nothing but physical barriers and deployable barriers matter for terrorism. That means for terrorist considerations, any system that can deny access to the site, such as deployable vehicle barriers and security landscaping and any system that can protect glass from shrapnel effects or structural elements from structural collapse, is effective against terrorism.

If the Taj Hotel in Mumbai had available bulkhead operable walls to segment the hotel, the moving shooters would have been contained, the number of casualties would have been dramatically reduced, and the siege would have been shortened to hours instead of days. Physical barriers — Understand them. Get them in your head. For antiterrorism, it is mostly about physical barriers.

In order to understand how to protect facilities, one must understand how facilities are attacked. Once an attack begins, it is too late to consider countersurveillance, intelligence, or any other method that would have been useful before that moment. Now, it is all up to the physical protective systems to protect lives. First, look at infiltration scenarios and then consider attack scenarios.

Infiltration Scenarios

- Insider Infiltration
 - False identity
 - Clean operative
- Special Mission Tactics and Techniques
 - Foot infiltration
 - Air infiltration
 - Vehicle infiltration
 - Sea infiltration
- Authorized Access with Valid Identification
- Illegal Access
 - Calm infiltration
 - Gate crash
 - Air infiltration
 - Vehicle infiltration
- Infiltration of Marine Facilities
 - Infiltration by sea
 - Infiltration by land
 - Infiltration by scuba diver or swimmer

Attack Scenarios

- *Moving Shooter:* One of the best examples of a moving shooter attack was the November 2008 attacks on hotels in Mumbai, India. In a moving shooter attack, shooters are moving through a space shooting while aggressing and degressing as well as doing lateral movements. Being a successful moving shooter requires much skill and rehearsal. Moving shooters must scan, scan, and scan for hidden adversaries lurking in the background. Moving shooters are much more difficult to counter than stationary shooters. In the Mumbai attacks, the shooters moved around each floor and from floor to floor. The forces deployed to find them did

not know where they were or where they would be next. Moving shooters have the advantage of surprise and endurance, as outside forces cannot easily contain them to a siege area.

- *Countermeasure:* Denial of access and containment.
- *Stationary Shooter:* Stationary shooters take a position and fire on moving or stationary targets. Stationary shooters have advantages on anyone within their line of sight. A good stationary shooter can usually land his first shot every time. Stationary shooters are often vulnerable to snipers, excellent targeting, and overwhelming force.
 - *Countermeasure:* Denial of access and overwhelming force.
- *Sniper:* Snipers are stationary shooters that shoot from a distance under cover. Snipers are deadly. Although sniper attacks from terrorists are rare in civilian settings, logic indicates that tactic will be used again.
 - *Countermeasure:* Cover and concealment, safe exit for noncombatants under cover, and countersnipers. Countersnipers are awesomely deadly to snipers.
- *Standoff Weapons:* Standoff weapons include Stinger missiles, rocket-propelled grenades (RPGs), and the like. These are rocket-powered, shoulder-launched grenades. Standoff weapons are typically used against vehicles and structures, particularly armored vehicles and reinforced structures. Though they are devastating against conventional vehicles and structures, they can also be fitted with fragmentation warheads for use against personnel.
 - *Countermeasure:* For conventional vehicles, none. Buildings and structures can be fitted with a decorative screen covering that detonates the RPG before it reaches the structure. The covering should be at least 1 meter distance from the structure.
- *Improvised Explosive Devices (IEDs):* IEDs are package bombs that are left in a location for detonation when the target arrives or after the bomber has left the area. IEDs may be left by the roadside (roadside bomb) or left in an airport or other public location or at a place of work (as with the Unabomber).
 - *Countermeasure:* Weapons detection and explosives detection systems including dogs, millimeter wave technology, X-ray, electromagnetic imaging in the infrared, terahertz, or microwave spectral range systems.
- *VBIEDs (Vehicle-Borne Improvised Explosives Devices):* The VBIED is the preferred method by terrorists around the world for delivering large explosive charges to damage or destroy buildings and structures. VBIEDs have been creatively constructed to deliver incendiaries, such as the Marriott hotel blast in Islamabad in 2008. That building was massively damaged more by the incendiaries than by the blast. VBIEDs do not need to get next to a building, though closer is better for the terrorist.
 - *Countermeasure:* Standoff. Create standoff by creating a security checkpoint at least 100 meters (300 feet) from the building. An absolute minimum of 30 meters (100 feet) is required. The checkpoint and the surrounding perimeter should be capable of stopping a large truck at speed. This can be accomplished with deployable barriers (crash barriers) and security landscaping.
- *Suicide Bomber:* A suicide bomber is a human IED delivery vehicle. Suicide bombers can get close to crowds of pedestrians and place bombs in precise locations for maximum casualties. Suicide bombers can deliver bombs inside buildings where a wedding or meeting of leaders is taking place, inside buses, to gatherings of people or any other precise location.

- *Countermeasures:* Weapons detectors including dogs, millimeter wave technology, video (human gait analysis), X-ray, electromagnetic imaging in the infrared, or terahertz or microwave spectral range systems. Pity the security officer they pick to intercept the person detected. Many heroes have died in this essential but dangerous role.
- *Hijacking:* Hijacking is the act of seizing control of a vehicle, whether it is an aircraft, truck, car, bus, or ship for the purpose of carrying out a terrorist attack. The attack may use the commandeered vehicle either as a delivery mechanism or as a bomb or incendiary device, as was the case in the World Trade Center and Pentagon attacks of September 11, 2001.
 - *Countermeasures:* Weapons detectors. Do not let terrorists board a vehicle or vessel. Detect the weapons they would use to hijack the vehicle.
- *Hostages:* The taking of hostages is important to terrorists because of the empathy that the victims' community feels for the event and the compounding of the tragedy beyond mere structural damage. The longer that terrorists can hold hostages attended by high levels of media coverage, the better for the terrorists.
- *Aircraft:* Aircraft have been used on several occasions as bombs. Plans to continue to do so have been found in terrorist safe houses repeatedly before and after September 11, 2001. Some of those plans include using rented planes to strike buildings, thus obviating the need to hijack a plane. Others include the use of chartered planes that often do not require passengers to be security screened.
 - *Countermeasure:* There is no suitable countermeasure that any specific facility can take to counter this threat.
- *Vehicles:* Vehicles have been used to deliver bombs (VBIEDs), to deliver terrorists, and as weapons.
 - *Countermeasure:* Deployable barriers and screening checkpoint.
- *Watercraft:* Watercraft have been used to deliver terrorists (Taj Hotel, Mumbai) and bombs (*USS Cole*) and have been hijacked by terrorists (Achille Lauro, 1985).
 - *Countermeasures for waterfront facilities:* Waterfront barriers, short-range radar, active use of CCTV, response team.
- *Grenades:* Grenades are used by terrorists for distraction, for offense, and for defense. Grenades can create significant casualties among unprotected civilians as part of a complete suite of a single terrorist's weaponry, such as in Mumbai in 2008.
 - *Countermeasures:* Weapons screening checkpoint and preattack intelligence. Subsequently, Special Forces including snipers.
- *Incendiaries:* Incendiaries are used to burn structures and may be configured as Molotov cocktails to VBIEDs configured as an incendiary.
 - *Countermeasures:* Standoff, deployable barriers, security landscaping, and security checkpoints.
- *Small Bombs under/in Vehicles:* These are low-impact terrorism tools and are also used for assassinations. Contrary to popular opinion, a bomb under a vehicle is not likely to damage a structure, only the people inside the vehicle and persons standing nearby. Some may be injured by broken glass. The use of undervehicle screening at a security checkpoint is usually cosmetic rather than meaningful because the threat is not to the structure but to the people in the car. Most of these systems are also staffed by personnel who are not trained to recognize an explosive if one is placed under the car, as tests have shown.
 - *Countermeasure:* Check under vehicle with mirror by skilled observer.

Attack Objective Parameters

General Objectives of Terrorism: Each terror strike has its own objectives, though common objectives exist. Common objectives include:

- *Change of Government Policy*: Terrorist attacks aim to draw attention to a cause by creating suffering among the “silent majority” of public. Formerly, terrorists made direct demands to release hostages. That is uncommon today. The current trend is to claim the act in the name of the terrorist organization and its cause.
- *Demoralize the Public*: Destroy the feeling of security and make the public fear future terrorist acts.
- *Reduce Faith in Government*: Terrorists aim to reduce the faith of the public in their government.
- *Change of Government*: One primary aim is to cause public pressure to change the government either to one more friendly to the terrorist’s cause (effectively done in the Madrid train bombings, 2004), or to a government that is more likely to get on the course of war with its neighbors (India, 2008).
- *Cause Economic Chaos*: One of the stated goals of Al Qaeda is to cause economic chaos in Western countries. This is primarily due to increased spending for security in the public and private sectors to defend against terrorism.

Specific Targeting Objectives: Each attack has its own targeting objectives, some of which are as follows:

- *Terror*: Simply to sow terror among the populace.
- *Mass Casualties*: Low-intensity terrorist attacks involve only a small number of casualties, but spectacular attacks strive to obtain large numbers.
- *Destruction of Iconic Structures*: High-intensity terrorism is almost always focused on an icon of the community’s economic or cultural self-image.
- *Media Coverage*: All terrorists crave media coverage. Any target that can be ideal for video coverage is also ideal for a terrorist attack.
- *Time*: Terrorists want the attack to last as long as possible, either the attack (as in Mumbai in 2008) or the response (as in the Islamabad Marriott fire of 2008) or the repercussions (as in the still reverberating September 11, 2001, attacks).
- *Assassination*: Many terrorist attacks are targeted against strategic individuals (January 2, 2009, suicide bomber killed 24 Iraqi tribal leaders at house of Sunni sheik discussing national reconciliation). Many car bombs were detonated in Lebanon following the assassination of former Prime Minister Rafic al Hariri in 2005. Those bombs uniquely targeted outspoken critics of Syria.

Criminal Violent Offender Types

Criminal violent offenders fall into two main groups — those who are mentally unstable, and those who use violence as a means to an end or as an end itself.

- Mentally unstable offenders often appear unexpectedly and behave erratically. They may or may not have any connection to the organization and may or may

not range from highly agitated to completely irrational, having no sense of reality whatsoever. Countermeasure: Depending on the extent of the mental instability, the weapons and the offender's ability and intent to harm others, countermeasures may range from talking the subject down to a swarming attack to disarm the offender.

- Focused criminals who use violence intentionally fall into two groups. Those who use violence to an end, and those who use violence for its own purpose. Criminal violence objectives include:
 - Intimidation to establish and maintain control: Criminals often use violence as a means to establish and maintain control over their crime victims. Intimidation may include:
 - Brandishing a weapon
 - Using a weapon against property
 - Using a weapon against a person or persons to intimidate that person or others
 - Rape to intimidate that person or others
 - Murder to intimidate others
 - Assault, rape, or murder:
 - Criminals may use assault to target a specific individual with violence against that person the objective of the attack and not a means to an end.
 - Criminals may also rape or murder a victim with no other crime in mind.

Economic Criminal Types

Economic criminals fall into two main groups — *internal* and *external*:

- Internal criminals have much greater access to the organization's assets, resources, proprietary information, and in particular, the full nature of the organization's security measures. For the well-prepared criminal, internal access is golden. With time to surveil, plan, test, and then execute, internal criminals can be very difficult to counter. Internal criminals can "come to the well" again and again and can even place clues to implicate other employees, contractors, or even outsiders.
- External criminals do not have the access of insiders, but they do have surprise and anonymity. Most external economic criminals execute their crimes once, not repeatedly. Most do not know their victims.

Most economic criminals of both types prefer to remain completely anonymous and escape undetected.

Economic Criminal Objectives

- *Embezzlement:* Internal theft, usually by those with access to cash or cash-like instruments (checks, purchase orders, etc.). Most embezzlement is conducted by a single "trusted" person in a relatively small business and almost always where there are poor accounting controls (only one person controlling

expenses and income reports). Countermeasure: Accounting controls by two or more people.

- *Robbery*: Robbery is a direct “in your face” crime, usually involving intimidation and force. Robbery is common in convenience stores and other small establishments. Most robbers escape with only a few dollars. Some victims do not escape with their lives. Invasion robberies happen more commonly at homes than at convenience stores or banks. These can be quite violent. Countermeasures: Physical protection for employees such as bullet-resistant glass cash enclosures and multiple employees in the store at all times. Few robbers want to try to control multiple employees. An exception to this is bank robbers who are willing to take on an entire bank full of employees and customers, where physical protection for the cashiers is usually an effective method. This reduces the likelihood of success of the robbery and thus serves as a strong deterrent.
- *Burglary*: Burglary is a faceless crime where the criminal makes entry, usually through breaking and entering, for the purpose of removing assets. Countermeasures: Robust physical security on the property and interesting assets, alarm system, CCTV system, dogs, and patrols.
- *Theft of Information*: Most theft of information today is via networks and the Internet. However, information is sometimes also taken via audio interception (phone, microphone, or acoustic). Document theft is also a concern. Countermeasures: Information technology countermeasures, office technical countermeasures (bug) sweeps, clean desk policies, secure file management, and a security awareness program focused on creating understanding about eavesdropping in public places.
- *Shrinkage*: Shrinkage is reduction in retail inventory caused by shoplifting and internal theft. Countermeasures: For shoplifting, vigilant employees, shop layout to deter shoplifting and active watched CCTV. For internal theft, internal investigators, secret shoppers, and internal controls.
- *Diversion*: Diversion of assets is often by collusion between internal and external criminals. This often takes place in the shipping/receiving departments. Countermeasures: CCTV, internal investigations, document controls, law enforcement liaison.

Criminal Offender Countermeasures

For all the criminal offender objectives stated above, a baseline security program is essential. The purpose of the baseline security program is to address through a uniform and comprehensive approach a whole range of statistically anticipated criminal behaviors and policy violations. Without treating the protective systems in a systematic comprehensive way, offenders can and will find the weaknesses in individual countermeasures which can be exploited for their own purposes. The basic elements of a baseline security program are shown below. The countermeasures listed below are discussed in detail in Chapter 16.

- Baseline Security Program
 - Security policies and procedures
 - Use of space definitions and alarm/access control systems
 - Define access levels
 - Control access to the access levels

- Physical barriers
- Authorization granting
- Access portals
- Perimeter and access-level penetration detection
- Use of video
 - Perimeter video
 - Entry point video
 - Circulation node video
 - Surveillance
 - Video patrol
 - Video pursuit
 - Video archiving
- Use of voice communications
- Use of guards
 - Posts
 - Patrols
 - Random applications of countermeasures
- Security awareness program
- Security training program
- Emergency services liaison program
- Security investigations program
- Special Countermeasures to Address Unique Vulnerabilities

COUNTERMEASURE EFFECTIVENESS METRICS

Functional Effectiveness

The first measure of effectiveness of a countermeasure is its functional effectiveness. As each countermeasure has one or more functions as outlined below, one can estimate its ability to perform each function on a scale of 0 to 10, with 10 being absolute and 0 being no function.

The functions again include:

- Access Control
- Deterrence
- Detection
- Assessment
- Delay
- Response
- Evidence

Take the list of vulnerabilities that you created from the vulnerability assessment and create a spreadsheet with those vulnerabilities listed as rows on the left and possible countermeasures listed in columns above. Array the vulnerabilities, grouped by asset classifications (that is, people, property [subcategorized], information, and reputation), and array the countermeasures by functions (access control, detection, assessment, delay, response, and evidence measures).

For example, under the property category, I may have the perimeter with subcategories of north, east, south, and west perimeters, then the main building (subcategories of entrances (also sub each entrance), then ground floor (sub lobby, etc.), and so forth.

For countermeasures, the categories are access control, detection, assessment, delay, response, and evidence gathering with subcategories of hi-tech, lo-tech, and no-tech countermeasures, each itemized under the category above. We might see evidence sub-categories video, patrols, witness statements, sniffer dogs, and so forth.

If multiple countermeasures apply to a particular vulnerability, duplicate those rows so that only one countermeasure is assessed for each row. Thus, we might have four rows for the same countermeasure, with two rows considering existing countermeasures, and two rows considering new countermeasures.

For each countermeasure related to each vulnerability, estimate its ability to deter, detect, assess, delay, and assist in a response or gather evidence. Estimate each from 0 to 1, with 1 being complete and 0 being none. This process identifies the effectiveness of each countermeasure for its purpose.

HELPING DECISION MAKERS REACH A CONSENSUS ON COUNTERMEASURE ALTERNATIVES

Sometimes when you present several alternative solutions to a committee, you will find that the committee cannot reach a consensus. Each stakeholder has a different agenda or takes a position and people become entrenched. Some people want the lowest cost, and others want the most effective countermeasure, and still others want the solution that is the most convenient to use or the most aesthetic. For such cases, I help the committee reach consensus by using a Decision Matrix. This is a simple spreadsheet tool that helps decision makers reach consensus by laying out the goals, risks, costs, and other factors, and scores each countermeasure by its ability to achieve the goals, mitigate the threats, and considers other factors including costs. Just as importantly, the Decision Matrix shows what risks the organization is accepting if a given countermeasure is selected. Whenever I have used the Decision Matrix, after reviewing the matrix, the committee's decision has often been unanimous in favor of a single countermeasure, which is often not the least costly. An example of a Decision Matrix is shown in Figure 17.3.

The Decision Matrix begins by listing the goals of the countermeasure, numbered 1 through N. This is followed by a listing of the possible risks for the countermeasure to mitigate, lettered A through X. The matrix follows which lists the countermeasure methods in rows and then has sections for goals achieved, risks mitigated, score, rank, risks accepted, estimated cost, effectiveness, and convenience. This is followed by notes that help the reader understand the matrix.

Our Lady of Perpetual Funding — Medical Center Security Landscaping and Fencing Decision Matrix												
Goals Description		Risks Mitigated					Risks Accepted					
Goals	Description	1	2	3	4	5	6	A	B	C	D	E
Fence Entire Property with Gates at Major Road Entrances Only *	A Harmless Unvetted Visitor — No criminal intent	1	1	1	1	1	1	1	1	1	1	1
Fence Parking Lots and Garage Only **	B Unauthorized Visitor Having No Business with BMC — Possible criminal actor based on crimes of opportunity											
Use Landscaping Only to Create a Barrier to Unwanted Visitors	C Property Criminal — Nonviolent criminal intent directed at property crimes only							1	1	1	1	1
Use Landscaping and Fencing to Enclose Property and Deny Access Except at Major Road Entrances Only*	D Personal or Sexual Attack Criminal — Nonvictim-specific violent crime with intent to compel property or induce victim to comply with sexual demands							1	1	1	1	1
	E Workplace Violence Visitor — Victim-specific violent crime which sometimes escalates to include violent attacks against innocent coworkers and law enforcement ***							1	1	1	1	1

Methods

Methods	Goals Achieved	Risks Mitigated	Score	Rank	A	B	C	D	E	Estimated Cost	Effectiveness	Convenience
Fence Entire Property with Gates at Major Road Entrances Only *	1 2 3 4 5 6	1 1 1 1 1 1	7	2						\$400,000	High	High
Fence Parking Lots and Garage Only **	1 1 1 1 1 1		4	3	•	•	•	•	•	\$150,000	Low	High
Use Landscaping Only to Create a Barrier to Unwanted Visitors	1 1 1 1 1 1		3	4	•	•	•	•	•	\$400,000	Low	High
Use Landscaping and Fencing to Enclose Property and Deny Access Except at Major Road Entrances Only*	1 1 1 1 1 1	1 1 1 1 1 1	10	1						\$500,000	High	High

Notes:

- Score is based on highest number of goals achieved and threats mitigated or eliminated
- Rank is based on highest score
- Final estimated cost numbers may be lower than estimates on Revolving Doors
- * Assumes Guard House at Major Road Entrances
- ** Assumes no Guard Houses at any entrance
- *** Workplace Violence Threat Actors cannot be easily identified at the perimeter. None of these options is an effective deterrent.

(D Decision Matrix is a PPI Best Practices Tool)

FIGURE 17.3 Decision Matrix

SUMMARY

Security organizations have historically been poor at measuring their cost-effectiveness or even their effectiveness at securing the organization. Management can only be efficient when results can be measured and compared to goals (metrics), and security management is no exception.

First, in order to measure countermeasure effectiveness, we have to ask: “Effective against what?” — “Against what threat?” “Against what purpose?” “Using what formula?”

There are only six things that any security countermeasure can ever hope to do:

1. Control access
2. Deter an attack
3. Detect an attack
4. Help the security force assess the attack
5. Delay the attack
6. Respond to the attack

Various countermeasures do one or more of these things, more or less well, at greater or less cost. Except for identifying persons carrying weapons or explosives, for terrorist threats on commercial, government, and critical infrastructure facilities, the only effective countermeasures are physical countermeasures. Operation elements use physical countermeasures and electronics to contain inappropriate behavior, but physical security is the primary container. Security attacks involve two protective considerations: *infiltration* and *attack*.

Criminal violent offenders include those who are mentally unstable and those who use violence as a means to an end or as an end itself. Rational criminals who use violence intentionally include those who use violence to an end, and those who use violence for its own purpose. Criminal violence objectives include:

- Intimidation to establish and maintain control
- Assault, rape, or murder

Economic criminals include both internal and external criminals. Economic criminal objectives include:

- Embezzlement
- Robbery
- Burglary
- Theft of information
- Shrinkage
- Diversion

A baseline security program is essential to deterring and dealing with all criminal offenders. The purpose of the baseline security program is to address, through a uniform and comprehensive approach, a whole range of statistically anticipated criminal behaviors and policy violations. Without treating the protective systems in a systematic

comprehensive way, offenders can and will find the weaknesses in individual countermeasures which can be exploited for their own purposes.

The primary measure of effectiveness of a countermeasure is its functional effectiveness.

When a committee cannot reach a consensus, the Decision Matrix is a valuable tool to help decision makers find a common ground.

CHAPTER 18

Security Effectiveness Metrics

INTRODUCTION

At the completion of this chapter, you will understand the elements of security effectiveness and learn how to develop a useful security effectiveness model suitable for every project not involving extremely high national security.

THEORY

One of the most difficult challenges of security management is the challenge of estimating the effectiveness of security countermeasures in their role of preventing crime and terrorism. By its very nature, crime and terrorism that has been deterred cannot easily be measured.

However, as we have seen from previous chapters, many things about security can be measured or estimated with a reasonable degree of accuracy, as can the effectiveness of countermeasures to detect, assess, delay, assist in a response and to capture evidence. All these can assist in deterrence. Although deterrence cannot be accurately assessed, all other factors can, and these all contribute to enhancing the difficulty of a successful attack, or looking at it another way, reducing the probability of success of an attack. Then a reasonable person would assume that as the difficulty level increases, deterrence does also. Difficulty could be construed as a surrogate for deterrence for most crimes and also for terrorism.

Security effectiveness is also a primary contributor to cost-effectiveness. The basic goal of cost-effectiveness is lower cost and more effectiveness. First, we must measure or estimate effectiveness in order to determine cost-effectiveness (Chapter 19).

SANDIA MODEL

Absolutely the best metrics for countermeasure effectiveness are contained within the Sandia Vulnerability Assessment Model. The Sandia model was developed to address mission-critical military and nuclear facilities (and other highly critical facilities for which security is a core mission). Weapons storage facilities, nuclear power plants, storage facilities, and such are all proper for application of the Sandia model, and most of these mandate the use of the Sandia model. The Sandia model measures the performance of each aspect of the security countermeasures program with great precision through firm scientific process.

I strongly recommend that all readers of this book also obtain a copy of Mary Lynn Garcia's book titled *Vulnerability Assessment of Physical Protection Systems* (Burlington, MA: Butterworth Heinemann, 2006). No better book has ever been written on vulnerability assessment. The Sandia model applies great precision to measuring every aspect of both vulnerability and the effectiveness of existing and proposed protective systems.

However, the Sandia model is so intricate and precise that the cost to fully apply it puts it beyond the reach of many organizations' security budgets. Commercial enterprises, many second- and third-tier critical infrastructure facilities can be estimated with less costly tools. In recognition of this fact, the U.S. Department of Homeland Security does not require this level of precision for most critical infrastructure facilities.

Quoting from Mary Lynn Garcia's book: "The Sandia Model expresses system effectiveness as a probability, P_E . P_E is determined using two terms: the probability of interruption (P_I) and the probability of neutralization (P_N). Performance-based analysis techniques use adversary paths, which assume that a sequence of adversary actions is required to complete an attack on an asset. ... It is important to note that P_E varies with the threat. As the threat capability increases, performance of individual security elements or the system as a whole can decrease."* The two types of analysis are compliance-based and performance-based analysis. Compliance-based analysis compares the system to specified mandates (codes, regulations, policies, and procedures) and assures that required elements are in place. Conformance-based analysis evaluates how the various components of the protection systems might perform against estimated threat scenarios. Each individual element can be analyzed or estimated against threat scenarios and determined what it contributes to overall system effectiveness.

The Sandia model utilizes six steps:

1. **ASD:** Create an adversary sequence diagram (ASD) for each asset location.
2. P_I : Conduct a path analysis. This provides P_I . Interruption is the arrival of responders to interrupt adversary progress.
3. **SA:** Perform a scenario analysis.
4. P_N : Complete a neutralization analysis where appropriate. This provides P_N . Neutralization is the defeat of the adversaries by direct engagement.
5. P_E : Determine system effectiveness, P_E .
6. **RMU:** Risk mitigation upgrade: If system effectiveness (or risk) is not acceptable, develop and analyze proposed upgrades.

For the Sandia model, $P_E = P_I * P_N$. Factors to consider are as follows:

- For adversaries that are likely to give up when confronted by a responder, P_N is not a factor.
- If no immediate response is possible, P_N is not a factor. In such cases, $P_E = P_I$.
- For the system to be considered effective, it must detect an attack while there is time to respond (before the critical detection point [CPD]).
- Provide a rapid assessment of alarms so that only valid alarms yield a response.
- Communicate the detection to an adequate response force in a timely manner.
- Collect evidence.

* Mary Lynn Garcia, *Vulnerability Assessment of Physical Protection Systems* (Burlington, MA: Butterworth Heinemann, 2006), 255.

- Ensure that detection occurs before delay, and delay the adversary long enough to process the detection, perform assessment, and communicate to a response force and get that force to the delay point (succeed at interruption).
- Use protection in depth (multiple layers) to assure that there are multiple opportunities to detect and delay an offender.
- Balance protection — that is, assure that all paths to assets have roughly the same probability of interruption (P_I).
- Engage and neutralize the offender with adequate and appropriate force.
- Conduct a full analysis of adversary paths, with system effectiveness (interruption and neutralization) as the overall performance metric. Analysis must occur along all credible paths.

The Sandia model is the pinnacle of vulnerability and risk analysis. The security industry high-security facilities throughout the world owe a debt of gratitude to Mary Lynn Garcia and the entire Sandia team for their excellent work.

Although the Sandia model is undoubtedly the best model in terms of quantifying every aspect of protection system effectiveness, it achieves this result at great cost in terms of the number of hours of research and computation. Accordingly, the full Sandia model is almost totally unused for commercial facilities. The Sandia model should always be used for such projects as nuclear power plants, weapons storage facilities, military bases, hydroelectric dams, and other projects where the loss of the asset would represent completely unacceptable consequences.

However, for most commercial projects, save only a few, the cost of the Sandia model has historically made any deep analysis of system effectiveness less likely to occur. Over the years, several other approaches have been developed by various individuals to provide some metrics to system effectiveness without the cost of the Sandia model. Many of these have been less than helpful with respect to determining actual effectiveness of security programs, systems, and system elements.

What has been needed is a method that is both easy enough for a single qualified analyst to use and which results in metrics that are meaningful in terms of helping budget decision makers to decide on which portions of a security program to fund in which order. What follows is just such a model.

A USEFUL COMMERCIAL MODEL

Before we look at the model, we will review the needs. Security program effectiveness metrics are needed by two classes of users:

1. Security Program Managers
2. Security Budget Decision Makers

Each user needs the following:

- Security program managers need to know which program portions are the most critical and effective and which portions need improvement and the priority in which they should be improved — cost to render effective and the importance of that program element in the overall security program (priority).

- Security budget decision makers need to know which portions of the program are most critical and effective and, based upon available budget, which elements can be funded.
- Both users need to know the impact on security effectiveness of unfunded portions — that is, what assets are left exposed by unmitigated vulnerabilities and what consequences could result if those vulnerabilities are exploited.
- Both users need to know what risks they are accepting by not mitigating remaining vulnerabilities.

To achieve the above results, the model needs to:

- For new projects: Identify what types of countermeasures could be effective to mitigate each listed vulnerability.
- For existing programs: Identify which existing countermeasures are effective to mitigate each listed vulnerability.
- Identify the effectiveness of each countermeasure in terms of:
 - Entry control
 - Intrusion detection
 - Assessment
 - Delay
 - Response
 - Evidence gathering

It is a common mistake to try to evaluate security programs in terms of “intrusion events interrupted or defeated.” There is a very small category of facilities for which this criterion is the chief criteria for consideration, and even in those, it would be a mistake to use it as a key or chief criteria. But virtually every metric ever developed focuses on detecting and interrupting intrusions (including the Sandia model).

One must consider what kind of security events one wants to control. Look at the universe of offenders again:

- Terrorists
- Economic Criminals
- Violent Criminals
- Subversives
- Petty Criminals

Any effectiveness metric that evaluates only one factor (intrusion) in my opinion completely misses the point. What is the range of offenses?

- Intrusions by unauthorized persons
- Destruction/damage/theft of assets (including people/property and intellectual assets)
- Subversion of the business environment to fulfill personal agendas
- Damage to business reputation arising from one of the above

Look at a few classic cases and what the victim organizations could have done to prevent the attacks:

- Terrorism
 - 9/11 — Absolutely nothing that the Port Authority of New York and New Jersey could have done could have prevented these attacks. The attacks were carried out by subverting the business processes of airports and airlines to carry out the agendas of the attackers. Once the terrorists got past the airport security checkpoints and into the cockpits, the World Trade Center towers and everyone on the upper floors were doomed.
 - Marriott Hotel, Islamabad, Pakistan, September 22, 2008 — Suicide truck bomb attack — A large truck rams the crash-resistant gate to the hotel, then a small explosion occurs in the truck, followed by a massive explosion. A massive fire erupted fed by a gas line that was ruptured when the powerful explosion blew off the front of the building.*† This set off fires on the fourth and fifth floors fueled by the gas line, and reaching temperatures of 400°C, according to the *Guardian*, overwhelming the sprinkler system and fire services. The fire was further fueled by the addition of aluminum powder‡ to the bomb which adhered to everything it struck, maintained a flame, and caused the adhered surface to burn. Aluminum powder is a component in thermobaric bombs including the 15,000-pound BLU-82 (Daisy Cutter) and the 21,000-pound MOAB (mother of all bombs). In both cases, aluminum powder is used to increase their destructive force.§ Aluminum powder creates a longer blast pulse that is far more damaging to buildings. This also extends the “reach” of the blast, damaging structures farther away than a conventional explosive and creating more destruction to the façade and structure. It is not a good idea to have gas lines that do not shut off automatically when ruptured. It would have been better if the checkpoint was more than 60 feet (20 meters) from the front door. Otherwise it was a good checkpoint design, having a sharp turn with no direct line of approach. A more thorough approach to risk analysis including utilities studies would have uncovered the gas line vulnerability before the bomb did. Moving the checkpoint out to 30 meters (100 feet) would have reduced damage from both the bomb blast and the flaming aluminum powder and might well have prevented the attack altogether.
- Economic Criminals
 - *Burglaries*: Burglaries come in two types: sophisticated and unsophisticated.
 - Unsophisticated burglars can be easily deterred, detected, and denied by conventional security programs with good response characteristics.
 - Sophisticated burglars are the economic equivalent of terrorists in that they spend considerable time selecting targets, planning, and testing before carrying out an attack. Such burglars often bypass alarm and closed-circuit television (CCTV) systems. Sophisticated burglars target extreme valuables (jewels, etc.), large vaults of cash (\$100,000-plus) and proprietary information. Professional burglars spend considerable time planning their burglaries. Countersurveillance programs are most helpful as most professional burglars will abandon an attack if they are intercepted during the target selection, planning, and testing phases.

* <http://lessakele.over-blog.fr/article-22995764.html>.

† <http://terrorwonk.blogspot.com/2008/09/islamabad-bombing-i-brute-force-tactics.html>.

‡ <http://terrorwonk.blogspot.com/2008/09/islamabad-bombing-i-brute-force-tactics.html>.

§ www.nationalterroralert.com/updates/2008/09/29/thermobaric-bombs-al-qaedas-new-weapon-of-terror/.

- *Insider crimes:* Insiders have time, access, and special knowledge of the facility and its assets working for them. Most insiders, however, do not have the skill and patience to leverage these advantages. Often insider crimes require investigations more than conventional security systems, which many insiders figure out how to circumvent or simply conduct their crime while at work when such systems are off or in areas where cameras do not monitor.
- Violent Criminals in the Workplace
 - *Outsiders:* Outsider violent crimes are of two main types:
 - Economic crimes using violence to control the victims. Most outsider violent crimes occur as opportunistic crimes (such as convenience store robberies), though some are planned (such as bank robberies).
 - Or they may be outsiders who may be related to workers or the organization in some way (spouse/lover/ex-worker). Ex-employees who continue to contact other employees or management with grievances or harassment should be taken as a sign of possible future violence.
 - *Insiders:* Workers being disciplined are the most common form of insider violent crime. Workplace violence can be minimized by proper human resources policy and a coordinated security program of workplace violence prevention. Other insider violent crimes include mentally-ill students of high schools and universities. Such crimes should be acted upon with great immediacy, as time delays may ensure more victims. Programs to identify possible students at risk of severe mental defect may also be helpful.
- Subversives (Types)
 - *Outsiders:* Activist groups are the most common types of subversives that organizations have to deal with. These typically involve intrusions and harassment actions. Security elements that detect, assess, respond, and collect solid identification evidence are most helpful in deterring such crimes.
 - *Insiders:* Insider subversives include chronic rule breakers and those who misuse the organization's assets for their own use. Improper Internet use, persistent rule-breaking, agitators, and sexual harassment all can affect the productivity and profitability of an organization. Insider subversive actions should be defined in employee policy manuals.
 - *Subversives and saboteurs:*
 - *Cause-oriented subversives:* Cause-oriented subversives may include activist groups with an agenda opposed to a government, religion, cause, or industry. This can include such groups as the Animal Liberation Front (ALF), the Environmental Liberation Front (ELF), and others.
 - *Nonaligned subversives:* Other subversive acts can include civil disorder events that are related to protests or civil riots. For example, the city of Los Angeles, California, was gripped by civil disorder and riots in 1992 following a trial of Rodney King, a black motorist who was beaten by Los Angeles Police Department (LAPD) officers. The beating was caught on camera and played on local television news stations.* Many businesses were damaged in the riots that followed.

* Lou Cannon, *Official Negligence: How Rodney King and the Riots Changed Los Angeles and the LAPD* (Boulder, CO: Westview Press, 1999).

- *Political and industrial spies:* Increasingly, organizations are being targeted by political and industrial spies. One article noted that industrial spies play a very big role behind the scenes at World Trade Organization talks.* There have been many cases of industrial and political spies prying into the secrets of large and small organizations alike.
- *Hackers:* Hackers may deface Web sites, damage networks, or act as spies to extract important information. In one recent case, hackers stole highly sensitive data on the U.S. Pentagon's newest fighter jet, the Joint Strike Fighter from military contractor's computers that were connected to the Internet.
- *Invasion of privacy threat actors:* Paparazzi and celebrity stalkers are the bane of celebrities for their invasion of privacy. Businesses that cater to the wealthy and celebrities are often confronted with aggressive celebrity seekers, photographers, and autograph seekers who interrupt the private moments of their clientele and subvert the purpose of a commercial enterprise for their own purposes.
- *Persistent rule violators:* These are individuals who frequent the organization's facilities either as employees or as visitors and who act as though the organization's assets are their own to use or abuse as they wish. Though warned of rules of conduct, they persist in violating the rules. Such individuals create problems for the organization in several ways:
 - They set a bad example for behavior for others.
 - They often require special attention to accommodate their demands or actions.
 - They often create safety or code of conduct preconditions that could lead to either injuries or to conduct problems on a larger scale (when one person acts out, it is common to see others follow that example).
 - They are disruptive of a normally orderly environment.
 - Their behavior may be illegal or affect the good business reputation of the organization, in some cases putting the organization at risk of prosecution for not abating the behavior, such as in racial or sexual misconduct cases, for example, where a manager is abusing his or her power over an employee.
 - Persons who abuse parking privileges, cut in line, demand special treatment, or act abusively toward employees are subversive influences.
- *Petty Criminals:* Petty crimes are offenses that are less than felonies and are usually punishable by a fine, a penalty, forfeiture of property, or imprisonment in a jail facility rather than in a penitentiary (misdemeanors).

* Les Blumenthal and Michael Doyle, "Spies bring trade secrets to the table at WTO talks," *Star Tribune* (Minneapolis, MN), November 27, 1999.

- *Vandals:* Vandals destroy property's value by defacing it. Vandals have caused millions of dollars in damage to property and have damaged the business opportunities of entire communities.*
- *Pickpockets:* Pickpockets ply their trade in many public places, including in hotels, restaurants, retail malls, parking lots and parking structures, elevator lobbies, literally anywhere two or more people come into contact, and especially where one of those people may be distracted. Businesses that provide such environments can be harmed by the damage to their reputation as a safe environment to frequent.
- *Prostitutes, pimps, and panderers:* Prostitution can affect hotels, retail malls, and other public spaces and can damage the reputation of the business.
- Other petty crimes include disturbing the peace, public nuisance, and public drunkenness.
- Business Reputation Crimes
 - *Outsiders:* In 1982, an unknown criminal laced Tylenol capsules with cyanide and placed the contaminated packages back onto store shelves where they were sold and taken by unsuspecting consumers. Johnson & Johnson, whose market share dropped from 35% to 8% after the incident, responded with very aggressive action including removing the product entirely from the marketplace, developing triple seals, and enacting aggressive product pricing. Within a year, Tylenol had recaptured its place in the market.
 - *Insiders:* Enron lost its entire business as a result of the improper accounting actions of some of its key management. Organizations should focus on their mission. Periodic oversight by shareholders or owners should audit the organization's actions against its mission, lawful actions, codes, and regulations.

The above information is not meant to discourage analysts from metrics-based effectiveness studies, but rather to indicate that there is a limit to what they can achieve. Much of security has to do with human resources policy development and enforcement and management ethics enforcement.

More importantly, this is to point out that intrusion-based metrics will not result in a valuable tool to reduce security incidents, as many security incidents do not involve intrusions.

Having said all that, it is better to evaluate security programs on the basis of being able to identify and respond to all types of security incidents, not simply security intrusions.

WHAT KIND OF INFORMATION DO WE NEED TO EVALUATE TO DETERMINE SECURITY PROGRAM EFFECTIVENESS?

Security managers need to know:

- Asset Locations
 - People
 - Property
 - Proprietary information

* Joseph Rivera, *Vandal Squad: Inside the New York City Transit Police Department* (Brooklyn, NY: Powerhouse, 2008).

- Vulnerabilities
 - Intrusions
 - Where intrusions are possible
 - Where intruders are likely to travel where they can be delayed or interrupted
 - Where intruders can be detected along the way to valuable assets
 - Direct attacks
 - Where direct attacks from the perimeter can be conducted
 - Removals/misappropriations
 - Where assets are readily available that can be stolen or misused
- Countermeasures
 - Locations and types of countermeasures
 - Entry control points
 - Detection systems
 - Assessment systems
 - Delaying systems
 - Response systems
 - Technologies
 - Communications systems
 - Guards
 - Transportation
 - Weapons
 - Tactics
 - Functions
 - Detect intrusion
 - Verify intrusion
 - Assess intentions
 - Delay intrusion
 - Intervene
 - Defeat aggression
 - Identify intruder
 - Evidence-gathering systems
 - Vulnerabilities they can address (a matrix of vulnerabilities and countermeasures)
 - Probable effectiveness of countermeasures in addressing the type of vulnerability
 - Detection
 - Assessment
 - Delaying
 - Responding
 - Deterrence (e.g., patrols and intercom response)
 - Denial (delaying systems and respond and defeat force)
 - Containment (prevent the adversary from leaving with the asset)
 - Recovery (after the loss of the asset)
 - Observe and report
 - Respond and defeat
 - Evidence gathering
 - Remaining Vulnerabilities
 - Remaining percentage of vulnerabilities addressed inadequately by existing countermeasures

WHAT KIND OF METRICS CAN HELP US ANALYZE SECURITY PROGRAM EFFECTIVENESS?

There are several possible metrics to use. Each metric evaluates a different factor in security program effectiveness. These can be used in combination to achieve a complete picture of overall system effectiveness. Some metrics are useful for both new and existing security facilities, and others are only applicable to existing facilities.

- Metrics usable for proposed security programs include:
 - Vulnerability/Countermeasure Matrix
 - Adversary Sequence Diagrams
- Metrics usable for existing security programs include:
 - Adversary Sequence Diagrams
 - Vulnerability/Countermeasure Matrix
 - Security events logs
 - Patrol logs (vulnerabilities spotting/violations spotting)
 - Annual risk analysis

Each of these are explained below.

Adversary Sequence Diagrams

Adversary Sequence Diagrams relate to a specific type of threat actor — those who use intrusion to gain access to their target asset. The most valuable assets of organizations are not located at their front gate at street side. In order for an intruder to get to the target, the intruder must make his or her way from outside the property through various gates, doors, corridors, and then finally to the target. This is true whether the attacker is a terrorist, criminally violent threat actor, or economic or intellectual property criminal. It is true for all burglars, attackers using force or subversives. Whether the threat actor is breaking in, breaking down doors, or secretly making his or her way to an office during working hours to steal money or information, there is a common factor. Each attacker must make entry, make his or her way through passages and barriers, and arrive at the target. For most attackers, the plan is also to make their way back out again, without detection, if possible.

Intrusion attackers come in three types:

1. Those using overwhelming force to make entry.
2. Those using stealth to make entry.
3. Those using the organization's normal business operations to make entry.

Obviously, each of these types presents different requirements for detection, assessment, and response. These three types also present themselves as two main types when encountering a response force:

- Those who will surrender peacefully or try to flee (mostly economic criminals, petty criminals, and some violent criminals).

- Those who will resist:
 - Those who will resist with moderate force (any threat actor except terrorists).
 - Those who will resist with overwhelming force (all terrorists and some violent criminals — only a few economic or petty criminals).

Intrusion threat actors can be further categorized into two broad groups:

1. Sophisticated criminals following an organized plan.
2. Opportunistic criminals mostly following their instincts (spontaneous planning).

Sophisticated criminals present special challenges for the following reasons:

- Intrusions are generally well planned.
- Sophisticated criminals know their target (its value, its location, the paths to the target, protective measures they will encounter on their way in and out).
- Sophisticated criminals know your facility, including its daily operations.
- They know your detection capabilities.
- They know your security force quality, quantity, training, force capabilities, and weaknesses.
- They can generally predict what your security response will be.
- Except for terrorism, from an evidence standpoint, sophisticated criminals usually leave little evidence.

Unsophisticated criminals also present special challenges:

- Unsophisticated criminals exhibit little or no preplanning, usually responding to opportunities without knowing much about their target, its detection capabilities, occupants, or its response capabilities.
- Poor planning means they may not act predictably either in terms of what direction they go and in how they will respond when encountered by a response officer.
- Unsophisticated criminals rarely make a prolonged entry for fear of detection and response.
- From an evidence standpoint, unsophisticated criminals often leave a chaotic crime scene.

The key to dealing with intrusion threat actors is to detect them as early as possible and intercept them with a superior response before they can make their way to their intended target. Failing that, you can detect them and present a superior response on their exit.

This is where the design basis threat becomes relevant again. The quality of detection, assessment, and response should be proportionate to the level of threat actor and their worst-case scenario. Countermeasure selection must be appropriate to the sophistication and force of the design basis threat.

The Adversary Sequence Diagram (Figure 18.1) is used to evaluate the possible points of entry and the paths that a threat actor could take to his or her target, and then to the exit. This, of course, will result in multiple Adversary Sequence Diagrams, one for each entry/target combination.

The next type of metric is the Vulnerability/Countermeasure Matrix.

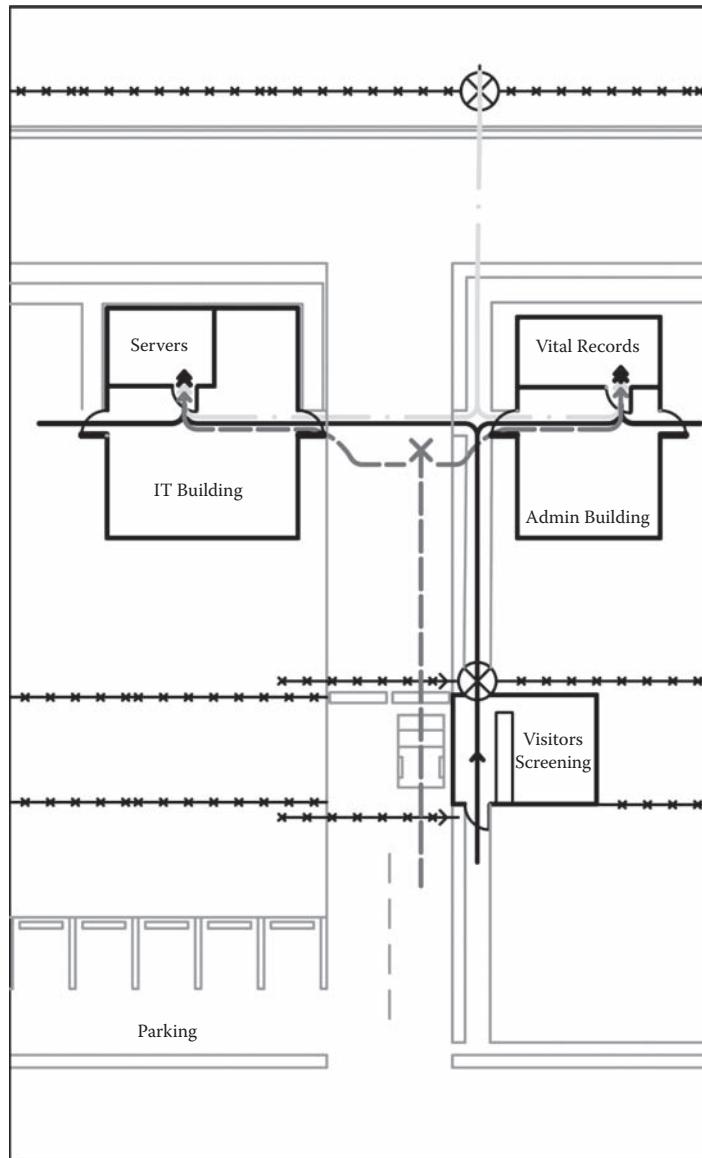


FIGURE 18.1 Adversary Sequence Diagram

Vulnerability / Countermeasure Matrix

The Vulnerability/Countermeasure Matrix is a spreadsheet of vulnerabilities (rows) and various types of countermeasures (columns). Ideally, every vulnerability identified should be listed on its own row. The vulnerabilities can be categorized by major asset groups, buildings, areas, and so forth. At intersection points between vulnerabilities and countermeasures, place a percentage of probable mitigation (1 being 100%).

For example, for detection systems, if detection of an exploiter of this vulnerability is assured, that gets a 1. For assessment, if there is a camera that can verify the alarm, that gets a 1.

For response, if a response can be mounted that can intervene before the subject reaches his target, that gets a 1. This could, for example, be a security intercom that allows the console officer to intervene and interrogate the subject remotely, while a patrol officer is being sent. The subject's response will dictate further action. If the subject continues after being intercepted by an intercom call, that defines intent. Then three other options exist. These include denial, containment, and recovery.

For facilities where the acquisition of the asset could cause unacceptable consequences, such as chemical plants and nuclear power plants, denial is required. This requires a robust security force with excellent training.

For facilities where the mere acquisition of the asset is not a consequence, only its loss would be, containment is a possibility. This allows the security force time to plan a response, including staging a recovery on the aggressor's exit.

For sites where a robust response force is not financially feasible, recovery may be a legitimate option. For this, excellent evidence is required, including vehicle ID including license plate and a clear photo of intruders (face and clothes, height, weight, gender, etc.) and evidence of the crime and evidence of the removal and getaway. Few commercial security systems can accomplish this, though all should.

For evidence, if there is a camera that can get a good identification, that would receive a 1. For a camera that can read gender, clothing description, and other details but not facial identification, that might be a 0.5, and for a camera that can see form and movement but could not identify gender, that might be a 0.2.

It may be useful to assemble columns in the spreadsheet into groups. I have done this two ways but finally settled on the second. The first grouping included hi-tech, lo-tech, and no-tech countermeasures. The second grouping included access control, detection, assessment, delay, response, and evidence. I now use the second group because it explains the function of each countermeasure more clearly. Some countermeasures can serve multiple functions, which is not evident in the first categorization. For example, a video camera can detect and assess. Arguably it could even be considered a response if a pan/tilt camera is seen to move from one position to follow a subject. This would be observable by the subject and thus constitute a response that could be a deterrent.

You will notice that there is no category for deterrence, because deterrence cannot be easily measured or estimated. Deterrence is purely a subjective phenomenon completely reliant on the subject in question. Factors involved in deterrence include:

- The subject's motivation.
- The subject's determination.
- The subject's concern for detection and capture (this is a key reason why terrorism is so difficult, because many terrorists do not care if they die in the attack, so they certainly expect to be detected and responded to). Thus, none of the usual factors comprise deterrence for a terrorist, except any response factors that could compromise the fulfillment of their mission.

Thus, if a subject wishes to elude detection, the deterrence value of alarms, dogs, cameras, lights, and so forth may be high. But if a subject has little concern for detection or response (terrorists, workplace violence threats, mental health threats, activist action groups, etc.), deterrent value of the same countermeasures may be low. One cannot estimate deterrence from the existence of countermeasures, and I do not recommend that you even consider it as a factor.

This principle should guide the design of response countermeasures. The degree of response should be directly correlated to the consequences of a threat action. If the consequences of a threat action are acceptable and can be mitigated after the loss, then the response can be unarmed and muted, such as in a normal office or commercial environment. However, if the consequences of the loss are wholly intolerable, such as at a nuclear power plant, nuclear weapons storage facility, or Phosgene (CG) chemical production plant, then the response capability should be superior to the severest possible threat action.

For any very severe consequence that could affect community welfare (chemical plant, etc.), I recommend the Sandia Risk Assessment Model and very robust countermeasures. Sadly, this is most often not the case for facilities in the commercial sector which are not subject to strict government security regulations. In my opinion, the government should mandate stricter risk assessment and countermeasure programs at many more types of facilities than they do now, because many facilities with relatively relaxed risk assessment and countermeasure requirements constitute a grave risk to society.

By categorizing countermeasures by their functions, one can get a picture of the overall effectiveness of the countermeasures that relate to a specific vulnerability. Within the categories of entry control, you might include access control reader, vehicle checkpoint, and so forth. For detection, you might have DPS (door position switch) motion detector, motion video detector, fence line detector, buried perimeter detector, left-behind article detection, patrol detection, and dog. For assessment you might include video camera, intercom, and patrol officer. For delay you might include deployable barriers and burglar bars. For response you might include patrols, dispatch, and intercom. For evidence you might include video archiving, audio intercom archiving, telephone, and 911 logging recorder. For a given security program, there may be dozens of types of countermeasures.

Different countermeasures will be applicable to different types of vulnerabilities (e.g., a glass façade is vulnerable to blast and intrusion). Countermeasures could include glass break detectors, blast film CCTV cameras, crime prevention through environmental design (CPTED) measures providing blast standoff and so forth. Because certain vulnerabilities may apply to multiple threat actions, the range of possible countermeasures is not universally applicable. However, each countermeasure has an effectiveness factor against each threat. Glass break detectors are of no help to a blast threat, but they are helpful against burglary. It is appropriate to list all possible countermeasures and rate them each for effectiveness against the types of threats that they can mitigate. This provides an overall view of effectiveness. It may also be useful for high-consequence vulnerabilities to add a remarks field to the right of all columns to note the highest consequence, as this may be taken into consideration when preparing the qualitative report. Apply an effectiveness estimate to every applicable countermeasure. The value of layering countermeasures will begin to display itself as the value of each of the countermeasures begins to add to a value of 1.

Do this for every vulnerability listed in the vulnerability analysis until all applicable countermeasures for all vulnerabilities have been estimated. You will note that certain countermeasures are capable of mitigating multiple vulnerabilities, and most vulnerabilities require multiple countermeasures to fully mitigate. Also keep in mind the design basis threat. If the design basis threat is violent crime, countermeasures that will mitigate violence may be of little use to economic threats. For economic crime, countermeasures that could mitigate terrorism may be of little use. For complex projects, I have actually developed Vulnerability/Countermeasure Matrices for several types of threat actions. This is

not usually done for every vulnerability in the facility, but for key assets (for violence, you may do this for people, but not for office equipment vulnerabilities).

The Vulnerability/Countermeasure Matrix should be prepared after the Adversary Sequence Diagrams, which will help to point out vulnerabilities that cannot be noticed without performing them.

Having explained this process to classes and individual consultants, it requires a step-by-step explanation to fully understand:

- *Step 1* — Create a spreadsheet of every vulnerability in the project. This spreadsheet will also serve as the basis for the risk register, if the project requires it (see Chapter 10). For the purposes of illustration, we will look at 2. Each vulnerability will reside on its own row, separated by asset class or area of facility.
- *Step 2* — Add columns for risk number, probability score, vulnerability score, consequences score, and risk score $R = (P + V + C)/3$. Add a column for recommended countermeasure and estimated cost.
- *Step 3* — Create columns for each type of countermeasure, grouped by functions. Function classes include:
 - Entry control
 - Detection
 - Assessment
 - Delay
 - Response
 - Evidence

To the left of each function, include a column marked Countermeasure Effectiveness Estimate (or CEE). To the right of all columns, add an additional column titled Total Mitigation Estimate (or TME) (Figure 18.2).

The screenshot shows a Microsoft Excel spreadsheet titled "Countermeasures.xls (Compatibility Mode - Microsoft Excel)". The spreadsheet contains data for a Countermeasures Effectiveness Matrix (CEM). The columns represent different types of countermeasures and their effectiveness scores. The rows represent various vulnerabilities. A "Baseline Security Program" section is present, followed by sections for different asset classes like Casino, Main Office, and Anti-Terrorism Measures. The data includes columns for Risk, Countermeasure, Access, Deterrent, Detection, Assess, Delay, Response, Evidence, Total, and Consequences (Critical and Medium). The "Total" column represents the Total Mitigation Estimate (TME), and the "Consequences" columns represent the Countermeasure Effectiveness Estimate (CEE).

Vulnerability	Risk	Countermeasure	Mitigation Value						Consequences	
			Access	Deterrent	Detection	Assess	Delay	Response	Evidence	Total
20 Unrelated Events	Critical	Develop New Post Opening	14%	14%	14%	14%	14%	14%	80%	1
21 Gamma Dawn/Evening Methods	Critical	Review Dawn/Evening Procedures	14%	14%	14%	14%	14%	14%	98%	1
22 Access Control on Policies	Critical	Limit Access of Critical Policies	14%	14%					29%	1
23 Security force is inadequate	Critical	Review competency of all officers for possible reassignment	20%						20%	1
24 Posts & Patrols may be inappropriate	Critical	Audit Posts and Patrol Positions	20%						20%	1
25 Security force is inadequate	Critical	Reassign poorly performing officer	20%						20%	1
26 Unable to hire new security staff	Critical	Provide Financial Contract Staff	20%						20%	1
27 Grouped Staff	Critical	Periodic Functional Audits/Undercover Investigations	20%	20%			20%	20%	80%	1
28 Unvetted Visitors	Critical	Institute full security checks on non-VIPs	10%	10%	10%	10%	10%	10%	70%	1
29 No ID Badges for Employees	Critical	Implement Photo ID Badges	10%	10%	14%	7%	5%	40%	1	
30 No BOH Visitor Badges	Critical	Implement BOH Visitor Badges	20%	20%					40%	1
31 Unvetted Guests	Critical	Education/Training in Civil Disorder Events	30%						30%	1
32 Civil Disorder Events	Critical	Develop Riot Recovery Plan	30%				30%		60%	1
33 No Business Recovery Plan	Critical	Develop Business Recovery Program							0%	1
34 Current CCTV Room inadequate	Medium	Establish a proper security CCTV Room							0%	1
35 No radio coordination with ISF	Critical	Radio Link to ISF					14%	14%	14%	1
36 Fire Exit & Pedestrian Safety	Medium	Speed bumps at Hailper Turn	7%	14%	4%	7%	14%	14%	46%	1
37 Fire Exit & Pedestrian Safety	Critical	Consider installing Strobe Door/Monitor within	14%	14%	14%	14%	14%	14%	84%	1
38 Weapons/Explosives Screening	Critical	Consider an Architectural Study for Security Area							0%	1
39 Package Bombs	Critical	X-Ray Machine for Package Screening	14%	14%	14%	14%	14%	14%	64%	1
40 Package Bombs	Critical	Consider screening packages off-site or move room					14%	14%	0%	1
41 Package Bombs	Critical	Negative pressure HVAC in Main Room					14%	14%	14%	1
42 Moneylenders in Casino	Critical	Cameras at Upper Main Road-Facial Recognition	7%	14%	14%	7%	14%	14%	70%	1
43 Moneylenders in Casino	Critical	Cameras at Upper Main Road-Facial Recognition	7%	14%	14%	7%	14%	14%	70%	1
44 Moneylenders in Casino	Critical	Cameras outside each Toilet-Facial Recognition	7%	14%	14%	7%	14%	14%	70%	1
45 Main Doors subject to confusion	Medium	RH Doors In/LH Doors Out	14%	7%	14%	7%	14%	14%	84%	1
46 All exterior openings no alarm	Medium	Alarm on all exterior openings	14%	14%	14%	14%	14%	14%	56%	1
47 Many exterior doors left open	Medium	Access Control on most exterior doors	14%	14%	14%	14%	14%	14%	98%	1
48 Banned Persons hard to recognize	Medium	Facial Recognition Software	7%	14%	14%	7%	14%	14%	70%	1
49		Anti-Terrorism Measures								
51 In the Dark about Developing Problems	Critical	Subscribe to Intelligence Briefing					12%		12%	1
52 Vulnerable to Vehicle Intrusion	Critical	Upper Drive In/Lower Drive Out (2 Lanes In Upper Drive)	14%	14%	14%	14%	14%	14%	70%	1
53 Forced Vehicle Entry	Critical	Reinforce Main Gates (2 m)	14%	14%	14%	14%	14%	14%	70%	1
54 Explosives in Vehicle	Critical	Utilize highly effective explosives detector	14%	14%	14%	14%	14%	14%	64%	1
55	Critical	Countermeasures Against Environmental Threats	14%	14%	14%	14%	14%	14%	64%	1

FIGURE 18.2 Countermeasure Effectiveness Matrix

- *Step 4* — For each vulnerability place an “X” under each countermeasure that applies. Then, for each function, place an estimate from 0 to 1 where 1 is total mitigation for that function and 0 is no mitigation for that function.

For example, for detection, countermeasures might include door position switch, glass break detector, guard dog, and patrol. For each of these that are applicable for this vulnerability, place an X under the countermeasure. Then estimate the total mitigation for that vulnerability for the detection function. If detection is assured, place a 1 in the Estimate column. If detection is not likely to occur, place a 0 in the column. If detection is nearly always likely, place a number lower than 1 and more than 0.5 in the column. Do this for each vulnerability and for each functional group. This provides the mitigation score for each function for each vulnerability.

Then place a weighting on the functional estimates. Since we have 6 functions, a balanced weighting would be 16.6% for each function.

The formula for total mitigation is simple and straightforward. Total Mitigation = (Entry Control * Weighted Score {WS} Entry Control) + (Detection * WS Detection) + (Assessment * WS Assessment) + (Delay * WS Delay) + (Response * WS Response) + (Evidence * WS Evidence).

Security Event Logs

Security event logs are also a very good way to determine overall security program effectiveness. Across a year’s time, security logs will display trends and identify unresolved vulnerabilities. We are interested in both, but especially the unresolved vulnerabilities.

It is unlikely that every last vulnerability will be identified in any risk assessment, but you can be certain that offenders will notice any unresolved vulnerabilities and try to exploit them. These will often be found by minor offenders or the guard staff. These minor exploits will show up as security events in the logs and are a valuable source for tightening up those unresolved vulnerabilities that would otherwise go unnoticed.

I recommend that whatever logging method you use to keep track of security events should have a column to track whether each security event was related to an unresolved vulnerability. An additional column could identify the unresolved vulnerability. This allows the security director to relate security events either to misbehavior that was handled in accordance with policy or was an event that should spark reconsideration of security countermeasures.

Over the course of a year, any unresolved vulnerabilities that develop into security events will draw management’s attention to the needs for those vulnerabilities to be mitigated with appropriate countermeasures. Adding the column to identify the security event as related to an unresolved vulnerability and describing that vulnerability allows the security director to quickly identify any unresolved vulnerabilities and also note which vulnerabilities are related to recurring security events.

The goal of ongoing risk assessments is to continuously uncover unresolved vulnerabilities and emerging threats and to make accommodations for them. Security event logs are one of the very best tools an analyst can use to achieve this goal.

In the event that there is no column to identify if each security event is related to an unresolved vulnerability, all is not lost. An analyst can import the logs to a spreadsheet

program and add the columns. If the analyst is familiar with the facility, he or she will likely think of the vulnerabilities that could relate to the security event. If not, he or she can assemble the related security events and then discuss these events with staff to uncover any unresolved vulnerabilities.

The spreadsheet acts as a metric, listing both incidents related to vulnerabilities and those that are not. The percentage of incidents related to vulnerabilities is a useful metric to determine that the security program is minimizing risk.

Patrol Logs (Vulnerabilities Spotting / Violations Spotting)

In the same manner that security incident reports can uncover unresolved vulnerabilities, so too can patrol logs. Quality security program directors train their patrol officers to understand vulnerabilities and to spot them when they see them. I always find it interesting when performing risk analysis surveys that interviews with both post and patrol officers always and without exception uncover unresolved vulnerabilities.

There is a wealth of information among the officers “on the ground” about the weaknesses in security countermeasures. It is very common after a major security incident to hear one or many officers say “Yeah, I knew that was going to happen someday.” So why did they not report it? Usually it is because management does not emphasize focusing on vulnerabilities and reporting them to management.

By training security officers to observe, and not just to see, management can find those vulnerabilities that are missed by risk analysts and management due to their lack of intimate familiarity with the facility and its operations. Security officers, who spend hours every day interacting with the business operations and every corner of the facility, know every vulnerability well. But in most cases, they are not trained to see them as vulnerabilities that should be addressed and reported to management.

The patrol logs spreadsheet acts as a metric, listing both patrol notes that are related to vulnerabilities and those that are not. The percentage of patrol notes related to vulnerabilities is a useful metric to determine that the security program is minimizing risk.

Annual Risk Analysis

Finally, the risk analysis should be updated annually. This presents an opportunity once each year to compare overall risk progression year over year. The delta between this year and previous years serves as a useful metric to determine risk progression.

SUMMARY

One of the most difficult challenges of security management is the challenge of estimating the effectiveness of security countermeasures in their role of preventing crime and terrorism. By its very nature, crime and terrorism deterred cannot be measured.

However, many things about security can be measured or estimated with a reasonable degree of accuracy. So too, can the effectiveness of countermeasures to detect, assess, delay, assist in a response, and capture evidence. Deterrence is the combination of the

effectiveness of these factors combined with the motivation, capabilities, and determination of the threat actor.

Security effectiveness is also a primary contributor to cost-effectiveness. The basic goal of cost-effectiveness is lower cost and more effectiveness. First, we must measure or estimate effectiveness in order to determine cost-effectiveness.

The Sandia model measures the performance of each aspect of the security countermeasures program with great precision through firm scientific process. However, the Sandia model is so intricate and precise that the cost to fully apply it puts it beyond the reach of many organizations' security budgets. Commercial enterprises and many second- and third-tier critical infrastructure facilities can be estimated with less costly tools. In recognition of this fact, the U.S. Department of Homeland Security does not require this level of precision for most critical infrastructure facilities.

A Useful Commercial Model

Before we look at the model, we will review the needs. Security program effectiveness metrics are needed by two classes of users:

1. Security Program Managers
2. Security Budget Decision Makers

For new projects, identify what types of countermeasures could be effective to mitigate each listed vulnerability; for existing programs, identify which existing countermeasures are effective to mitigate each listed vulnerability; and identify the effectiveness of each countermeasure in terms of the following:

- Entry control
- Intrusion detection
- Assessment
- Delay
- Response
- Evidence gathering

It is a common mistake to try to evaluate security programs in terms of intrusion events interrupted or defeated. There is a very small category of facilities for which this criterion is the chief criterion for consideration, and even in those, it would be a mistake to use it as a key or chief criteria. But virtually every metric ever developed focuses on detecting and interrupting intrusions.

The range of offenses includes:

- Intrusions by unauthorized persons
- Destruction/damage/theft of assets (including people/property and intellectual assets)
- Subversion of the business environment to fulfill personal agendas
- Damage to business reputation arising from one of the above

Useful Metrics

There are several possible metrics to use, and each metric evaluates a different factor in security program effectiveness in order to achieve a complete picture of overall system effectiveness. Some metrics are useful for both new and existing security facilities, and others are applicable only to existing facilities.

- Metrics usable for existing security programs include:
 - Vulnerability/Countermeasure Matrix
 - Adversary Sequence Diagrams
 - Security events logs
 - Patrol logs (vulnerabilities spotting/violations spotting)
 - Annual risk analysis
- Metrics usable for proposed security programs include:
 - Vulnerability/Countermeasure Matrix
 - Adversary Sequence Diagrams

Security Event Logs

Security event logs are one of the best ways to determine overall security program effectiveness. Viewed annually, security logs will display trends and identify unresolved vulnerabilities. We are interested in both, but especially the unresolved vulnerabilities.

Patrol Logs

Patrol logs can also uncover unresolved vulnerabilities. Quality security program directors train their patrol officers to understand vulnerabilities and to spot them when they see them.

The patrol logs spreadsheet acts as a metric, listing patrol notes that are related to vulnerabilities and those that are not. The percentage of patrol notes related to vulnerabilities is a useful metric to determine that the security program is minimizing risk.

Annual Risk Analysis

Finally, the risk analysis should be updated annually. This presents an opportunity once each year to compare overall risk progression year over year. The delta between this year and previous years serves as a useful metric to determine risk progression.

Cost-Effectiveness Metrics

INTRODUCTION

One of the most difficult questions for management of any organization is how much to spend on different organization programs. Each organization has two types of programs, including revenue-producing and overhead programs. Even nonprofit organizations have revenue-producing programs. These usually are fund-raising or something similar used to raise funds to support the mission of the organization. For for-profit organizations, it is much more clear cut — the mission of the organization includes the selling of goods or services that are to result in the organization making a profit. If it does not make a profit, it has not fulfilled its mission.

Programs like human resources, accounting, facilities, and security are all administrative programs whose purpose is to support the primary mission of the organization through the provision of resources and the protection of those resources from risk.

For most administrative programs, the cost formula is clear cut. How much does it cost for this program to provide the services needed by the programs that directly support the mission of the organization? That then is the budget.

For the security program, the answer is not so clear cut. The security program must be funded adequately so that it can protect the assets of the organization from harm. But in any given year, little harm may occur naturally, and then suddenly in one year great harm can occur. Security programs must be effective at preventing “chronic” security problems and the “one-off” events that get everyone’s attention.

But in a year when there is no “one-off” event, it can easily appear that security’s budget is too much. And, unlike any other program, quite ironically, the better the job that the security program is doing, the less it seems that security is needed. No other program suffers like security from its own success.

It could probably be accurately said that most organizations’ security programs suffer from a lack of effective management metrics. And the lack of management metrics in any program is a certain source for program inefficiencies and possible mission failure.

The presence of useful management metrics not only helps assure the success of the mission of the program, but also helps the security program director justify and explain the legitimate needs for the program to upper management so that they can make informed financial decisions that are in the best interest of the organization. Cost-effectiveness metrics are at the heart of this approach.

WHAT ARE THE LIMITATIONS OF COST-EFFECTIVENESS METRICS?

The challenge of cost-effectiveness metrics is effectiveness. Cost-effectiveness has only two components: cost and effectiveness. As we have seen from Chapter 18, it is possible to measure effectiveness, and the measurement of cost is straightforward. But how do we derive cost-effectiveness?

There are many possible ways, most of which are either too complicated or conclude in meaningless results. For example, in order to determine overall program cost-effectiveness, we could apply a formula such as (security budget/security events). Such a formula will result in a dollar value per security event, but it is not a meaningful formula. For example, if we were able to achieve such effectiveness that only one event occurred, and our organization had a \$500,000 annual budget, then we would have a result of \$500,000 per security event. This is not only absolutely meaningless because it does not take into account security events that were deterred (an unknowable number), but it is also very alarming to budget makers. Context is everything.

But to create a useful result, one must constrain the arguments in order to get reasonable results. It is often helpful to reduce arguments to the ridiculous in order to understand the principles. Look at just such a simplistic but illustrative example.

If I want to protect my house and all of its occupants and belongings from harm, there are a wide array of options that include the reasonable and the ridiculous. A comparison of cost-effectiveness between just two extremes is this: In this competition for best cost-effectiveness, the contenders are my dog Spot! (that's his name: Spot!) versus the U.S. Navy.

In this corner: my dog Spot!

- Countermeasures include:
 - Detection sensors
 - Very good ears
 - Very good nose
 - Eyes (fur is in the way so these are not so good)
 - Assessment
 - Any person with food — good
 - Known person friendly to owner — good
 - Mailman — bad
 - Unknown person without food — bad
 - Delay
 - Spot!'s responses can act as a useful barrier to an intruder
 - Response
 - Spot! is quick on his feet and can reposition quickly to counter any movement by an intruder
 - Spot! barks
 - Spot! growls
 - Spot! bares his pointy teeth
 - Spot! will chase intruder up a tree or over a fence
 - Evidence-gathering tools
 - Pointy teeth

- Effectiveness Factors
 - Deterrence: Depends on the type of offender — unknowable.
 - Detection: Spot! is pretty good at detecting unknown intruders (and the mailman) — Say Spot! is 80% effective at detection.
 - Assessment: Spot! is weak here. (He thinks the mailman is fast food.) His IFF (identify friend and foe) circuit is weak. Say Spot! is 20% effective at assessment.
 - Delay: Spot! can be pretty good at delaying intrusion. Say he is 50% effective at delay.
 - Response: Spot! will definitely respond, both audibly running to engage the intruder and with his clashing pointy teeth. Only highly determined intruders will get past him. Spot! is 80% effective at response.
 - Evidence: This is not Spot!'s strong suit. He may bring back a shred of pants cuff but not much more. Spot! is 1% effective at evidence.
 - *Overall, Spot! is 49.2% effective.*
- Cost Factors
 - Capital cost
 - Original purchase price: \$25 at the animal shelter, including first set of shots.
 - Operating cost
 - Food: \$250/yr
 - Vet visits: \$100/yr
 - Dog license: \$10/yr
 - Upgrade to home insurance: \$40/yr
 - Total annual operating cost: \$400/yr

And in this corner: the U.S. Navy.

- Countermeasures include:
 - Detection
 - Thousands of underwater, airborne, and satellite sensors, human intelligence feeds from the Central Intelligence Agency (CIA) and the National Security Agency (NSA), also airborne visual sensors (unmanned and manned aerial vehicles) and law enforcement liaison (local, state, and federal) plus NCIS (Naval Criminal Investigative Service).
 - Assessment
 - Hundreds of millions of dollars budget for analysts
 - Delay
 - Delay through response and liaison with U.S. State Department and law enforcement liaison
 - Response
 - 11 Aircraft carriers
 - 14 Ballistic missile submarines
 - 4 Guided missile submarines
 - 97 Surface combatants
 - 53 Nuclear attack submarines
 - 33 Amphibious warfare ships
 - 32 Combat logistics ships
 - 29 Support/mine warfare ships
 - 9 Active reserves

- Unknown number of strategic sealift vessels
- The U.S. Navy can strike almost any target anywhere when assisted by aerial refueling planes
- Evidence-gathering tools
 - Video footage from aircraft and naval vessels
 - Ship and airborne radar
 - Human intelligence
 - Law enforcement liaison
- Effectiveness Factors
 - Deterrence: Pretty good deterrence, but still unknowable, probably higher than for Spot!
 - Detection: 99% effective
 - Assessment: 99% effective
 - Delay: 90% effective
 - Response: 99.5% effective
 - Evidence: 60% effective
 - Overall, the U.S. Navy is 90.5% effective. (*The U.S. Navy loses points for evidence, which is not its strong suit.*)
- Cost Factors
 - Annual budget: 2008 budget = \$159.8 billion*

Clearly, the U.S. Navy wins the effectiveness argument. Spot! is only 49.2% effective, whereas the U.S. Navy is 90.5% effective. However, Spot! wins the cost argument equally handily. The U.S. Navy's annual budget is \$159.8 billion, whereas Spot!'s annual budget is only \$400. Then the question becomes how much is too much? How much is too much cost, and equally, how much is too much effectiveness?

How do we determine which is more cost-effective? Perhaps we should consider the value of the assets under protection. Say that my home is worth \$150,000 and property assets are another \$100,000, including cars, furniture, tools, jewelry, and so forth. With a total of \$250,000 in assets to protect, Spot! is beginning to look like a bargain and the U.S. Navy is starting to look like massive cost-effectiveness overkill. But wait, there's more. I forgot the value of my family. Personal assets are replaceable, but family members are not. If one of the threats includes home-invasion robberies, which can be traumatic and sometimes fatal, I would do well to consider more protection than Spot! can provide.

I could stand to lose \$250,000 in assets, but the consequences of a home-invasion robbery are actually much higher. They could include lengthy hospitalization or a funeral for myself or a loved one. These are considered unacceptable consequences.

It is not really the asset value that we are protecting, it is, in fact, the consequences that we are protecting against. This is a most important principle that must be understood.

Even though I cannot afford to employ the U.S. Navy, and Spot! is a wonderful budget fit, I would like more protection and more effectiveness than Spot! alone can offer. When we combine Spot! with other protective measures, we can achieve a much higher level of effectiveness and still keep the budget within reasonable bounds.

Perhaps I should consider a complete home security program to include Spot! and a complement of burglar bars, reinforced doors, and locks alarm system with central station monitoring, motion-activated automated lighting, CCTV system, and a private patrol and response force. All this will be complemented by a set of home security policies

* www.finance.hq.navy.mil/FMB/08PRES/HIGHBOOK/Highlights_book.pdf page 1-15.

and procedures to help make sure that the family is security aware. The capital budget for all this is \$5,000 and the annual operating budget rises from \$400.00 for Spot! alone to \$1,600. If I have valuables and a high probability of intrusion, this is still quite a reasonable sum to spend to protect my family, home, and valuables that are certainly worth their asset value and, with the addition of casualty considerations, in fact are worth much more. And Spot! can take a day off occasionally.

Looking at the third option — the complete home security program — we find the following:

- Countermeasures
 - Detection sensors
 - Spot!
 - Alarm system
 - CCTV system programmed with motion detection
 - Private patrol
 - Assessment
 - Spot! — not so good.
 - Alarm system + central station monitoring — good
 - CCTV system central station monitored — very good
 - Delay
 - Spot! — good
 - Burglar bars — good
 - Reinforced doors and locks — good
 - Response
 - Spot! — good
 - Private response force — good
 - Automated lighting — good
 - Evidence-gathering tools
 - Spot! — not so good
 - Alarm system — good
 - CCTV with central station monitoring — very good
 - Private response force — very good
- Effectiveness Factors
 - Deterrence: Depends on the type of offender — unknowable
 - Detection: 95%
 - Assessment: 95%
 - Delay: 90%
 - Response: 90%
 - Evidence: 95%
 - *Overall, the complete home security program is 93% effective.*
- Cost Factors
 - Capital cost: \$5,000
 - Operating cost
 - Spot!: \$400/yr
 - Complete home security program: \$1,600/yr
 - Total annual cost: \$2,000/yr

It is really all about reasonable ratios to achieve reasonable security goals. We want the highest possible effectiveness for an affordable budget. Three questions present themselves:

1. What is the value of the possible consequences? (baseline for consideration)
2. What is an affordable budget to mitigate these consequences? (reasonable cost)
3. What is the highest effectiveness we can achieve within this budget? (highest effectiveness)

Research that I conducted throughout my long career indicates that well-prepared security programs for nonstrategic facilities usually have a capital budget range of between 1% and 2% of the cost of the facility alone, excluding fixtures, furnishings, and equipment (FF&E), and can go higher if the values of FF&E are high (such as for expensive medical equipment like magnetic resonance imaging [MRI] equipment, etc.). This budget estimate is appropriate for commercial, noncommercial, and critical infrastructure facilities. Exceptions include those facilities that house assets, the loss of which could constitute great harm to the community, such as chemical plants, nuclear power plants, nuclear weapons storage facilities, central banks, presidential palaces and the like. For these types of facilities, the capital and operating costs of the program should be entirely driven by the consequences.

Let me cite an example. I might want to buy a family car that is likely to protect my family in a serious crash (kudos to Volvo), but I do not have an imminent need for an armored limousine. However, if I were the founding president of what had grown from a small business into a National Critical Petrochemical Company, located in an area of the world where there is a history of kidnappings of corporate chief executive officers (CEOs) and their families, I would be foolhardy not to own an armored limousine and a proper security program for my home, office, and family. In such a case, an annual security budget of \$1,600 would be foolhardy. *Consequences drive the budget.*

In such a case, not only the consequences of the loss of the president or his family member drive the decision, but also the consequences of the loss of this person to the corporation and indeed the country drive the decision. This is why presidents and prime ministers are so well protected. But this is not always the case. In February 2009, the new Prime Minister of Zimbabwe, Morgan Tsvangirai, and his wife were driving in a sport utility vehicle (SUV) on a two-lane highway in Zimbabwe, going home to their ancestral village. They were accompanied only by their driver and an aide. There were no escort cars ahead or behind. On this very bad road, they had a head-on collision with a large truck, causing the Tsvangirai's SUV to roll over three times, killing Mr. Tsvangirai's beloved wife of 30 years, and mother to his six children, and whom most considered as a mother to their nation. The country mourned the loss of Mr. Tsvangirai's wife and closest confidant. Zimbabwe's president Robert Mugabe allegedly had considered the cost of executive protection for Mr. Tsvangirai, his political rival, to be too high, though he reserved such for himself. *Consequences drive the budget.*

For a nuclear power plant, the annual cost of security can be many times the cost of that for a nonnuclear power facility. *Consequences drive the budget.*

WHAT METRICS CAN BE USED TO DETERMINE COST-EFFECTIVENESS?

Remembering that we found a way to estimate effectiveness and cost is self-evident, how then do we compose a formula to estimate cost-effectiveness? If we are comparing systems that have the same cost and different effectiveness, this is quite simple. For example,

	System 1	System 2	System 3
Cost	1,000,000	1,000,000	1,000,000
Effectiveness	60%	75%	90%
Cost/Effectiveness	60%	70%	80%

FIGURE 19.1 Cost-Effectiveness: Example 1

	System 4	System 5	System 6
Cost	1,000,000	1,100,000	1,200,000
Effectiveness	60%	60%	60%
Cost/Effectiveness	60%	54.5%	50%

FIGURE 19.2 Cost-Effectiveness: Example 2

	System 7	System 8	System 9
Cost	1,000,000	1,100,000	1,200,000
Effectiveness	60%	75%	90%
Cost/Effectiveness	60%	68%	75%

FIGURE 19.3 Cost-Effectiveness: Example 3

see Figure 19.1. As costs stay the same, the difference in cost-effectiveness is the difference only in effectiveness.

The answers above are the result of multiplying each cost by each effectiveness, factored to 1. We assume that because all costs are the same, they are all equal to a factor of 1. ($\text{Cost1} * \text{Effectiveness1}$), ($\text{Cost2} * \text{Effectiveness2}$), and ($\text{Cost3} * \text{Effectiveness3}$).

The comparison is equally easy when the prices differ but the effectiveness is the same, as shown in Figure 19.2. As costs of each system rise, the difference in cost-effectiveness becomes the reduced value of effectiveness versus increasing costs.

The answers are also the result of multiplying each cost by each effectiveness with costs again factored to multiples of 1. We achieve this by dividing the baseline cost (in this case \$1,000,000) by the cost under consideration. The result is $\$1,000,000 = 1$, $\$1,100,000 = 0.909$, and $\$1,200,000 = 0.833$. Therefore, the results in Figure 19.2 derive from factoring all costs to multiples of 1: $((\text{Cost1} = 1) * \text{Effectiveness1})$, $((\text{Cost2} = 0.909) * \text{Effectiveness2})$, and $((\text{Cost3} = 0.833) * \text{Effectiveness3})$.

This method also works equally well for differing costs and differing effectiveness, as shown in Figure 19.3.

The answers are also the result of multiplying each cost by each effectiveness with costs again factored to multiples of 1 — that is, $\$1,000,000 = 1$, so $\$1,100,000 = 0.909$, and $\$1,200,000 = 0.833$. Therefore, the results in Figure 19.3 derive from factoring all costs to multiples of 1: $((\text{Cost1} = 1) * \text{Effectiveness1})$, $((\text{Cost2} = 0.909) * \text{Effectiveness2})$, and $((\text{Cost3} = 0.833) * \text{Effectiveness3})$.

The complexities of changing costs and changing effectiveness are resolved by factoring all costs against a baseline of 1 for the lowest cost. This assures that all ratios result from a single point of comparison. All costs are compared to the lowest cost, and all effectiveness numbers are compared to the ratio of the system cost under comparison, to the baseline cost. Therefore, all results are relational.

This formula is simple:

$$(\text{SystemCost1}/\text{SystemCost1}) * \text{Effectiveness1}$$

$$(\text{SystemCost1}/\text{SystemCost2}) * \text{Effectiveness2}$$

$$(\text{SystemCost1}/\text{SystemCost3}) * \text{Effectiveness3}$$

The baseline cost is always divided by the cost under consideration so that all costs reduce the value of effectiveness by the factor of the increase of the cost over the baseline cost.

Go back to our first example to test this formula to the extreme. Figure 19.4 presents the same formula being applied to the protection of my home, where the alternatives are (1) my dog Spot!, (2) complete home security program, and (3) U.S. Navy. This example factors in capital costs plus first-year annual costs.

Although Spot! is very cost effective, his overall effectiveness is below 70%. As a rule of thumb, I do not consider any packages of countermeasure solutions that fall below 70%. If we throw out Spot! and consider only the complete program versus the U.S. Navy, we get the results presented in Figure 19.5.

The hands-down winner is the complete home security program. If you doubt these results, consider that it actually does not matter whether we use the least cost, middle cost, or most cost as the baseline reference. Revising the numbers to use the U.S. Navy as the baseline, we get the results presented in Figure 19.6.

Are these the same ratios? Yes, they are:

- From Figure 19.5: $93/0.0000039643 = 23459374.9$.
- From Figure 19.6: $2,123,057,142.9/90.5 = 23459194.9$.

As it is messy to have any ratios above 1 (100%), I always use the lowest system that achieves a minimum of 70 as the baseline number for calculation.

	Spot!	Complete Program	US Navy
Cost	\$425	\$7,000	\$159,800,000,000
Effectiveness	49.2%	93%	90.5%
Cost/Effectiveness	49.2%	5.6%	.0000002407%

FIGURE 19.4 Cost-Effectiveness: Example 4

	Spot!	Complete Program	US Navy
Cost	\$425	\$7,000	\$159,800,000,000
Effectiveness	49.2%	93%	90.5%
Cost/Effectiveness		93%	.0000039643%

FIGURE 19.5 Cost-Effectiveness: Example 5

	US Navy	Complete Program
Cost	\$159,800,000,000	\$7,000
Effectiveness	90.5%	93%
Cost/Effectiveness	90.5%	2,123,057,142.9%

FIGURE 19.6 Cost-Effectiveness: Example 6

	Complete Program	Spot!	US Navy
Cost	\$7,000	\$425	\$159,800,000,000
Effectiveness	93%	49.2%	90.5%
Cost/Effectiveness	93%	871.3%	.0000039643%

FIGURE 19.7 Cost-Effectiveness: Example 7

	System 4	System 5	System 6
Cost	1,000,000	1,100,000	1,200,000
Effectiveness	60%	75%	90%
Cost/Effectiveness	66%	75%	82.5%

FIGURE 19.8 Cost-Effectiveness: Example 8

See how this works when we compare all three results again in Figure 19.7.

When comparing our reasonably similar systems, just to last and finally check the validity of the numbers, throw out the system that is below 70% effective and use the 75% effective system as the baseline number for calculation, as shown in Figure 19.8.

Although the numbers shift, their relationships stay the same. Remember the cost number used as the baseline will always result in the cost-to-effectiveness ratio being the same as the effectiveness number. All other system numbers will line up relative to the baseline number.

Are they the same ratios? Yes, they are, as we can see below:

- From the first comparison where system 4 was used as the baseline number, the ratios between system 4, system 5, and system 6 were 60%, 68.2%, and 75%. These relate to the following ratios between these three percentages: 60% = 1, 68.2% = 0.88, and 75% = 0.8.
- From the second comparison where system 5 was used as the baseline number, the ratios between system 4, system 5, and system 6 were 66%, 75%, and 82.5%. These relate to the following ratios between these three percentages: 66% = 1, 75% = 0.88, and 82.5% = 0.8.
- The ratios are always the same.

If I am going over this formula to the point of nausea, it is because it is highly important to understand it completely. Many mistakes are made by analysts who think they understand cost-effectiveness but in fact do not.

This formula may be used to compare capital costs, operating costs, or system component costs and their effectiveness ratios. This is a reliable formula.

COMMUNICATING PRIORITIES EFFECTIVELY

Making the Case

Virtually every organization is under financial challenges. Understanding that many program directors are vying for the same budget dollars, it is necessary for the security program manager to make a clear case for security program budget dollars.

I often say that accounting and security programs have much in common. They both are required to comply with codes and regulations and limit the organization's exposure to risks (in one case, financial risk, and in the other, security risks).

But accounting organizations make a far better case for their needs and successes than do most security organizations. We can change that. The process of developing a comprehensive risk analysis will go a long way to making the case. Though many may read no more than the executive summary, it should include a summary paragraph of each section and graphics illustrating the risk summary. The proposed countermeasure budget should be based on a comprehensive solution with a caveat that it can be adjusted to accommodate implementation phasing.

- Develop the Arguments

- *Determine the priorities of management.* This simple but often overlooked item is essential to targeting management's interests in budgeting arguments. Priorities can be determined from annual statements, memos issued by management to employees, and by directly asking executive management to outline their priorities for the next fiscal year in an e-mail. They will appreciate your interest.
- *Identify points of view of stakeholders and acknowledge them.* In order for the security program to get its own share of the overall budget, you will have to contend with other organization stakeholders who have their own priorities and agendas. By understanding these, you can make the case for security program countermeasures in the context of all these other competing agendas. By preparing the argument in this context and acknowledging the points of view, all of which need executive management's attention, you are more likely to succeed than if the argument is made in the absence of this information. This helps executive management to place the security program in the context of the overall organization's needs. This is one of the most important elements of a successful presentation.
- *Provide a list of consequences.* The only reason to have a security program is to prevent the unwanted consequences of not having a security program. This is what risk analysis is all about. By identifying all risks and consequences, executive management can develop the priorities of its budget. It is useful to create a comprehensive list of consequences and pose the question to executive management as to which of the consequences would be acceptable losses. This is not a rhetorical question, and it is not intended to provoke management. It is a logical question directly related to prioritizing budgets. Remember, all risks can be dealt with in one of several ways:
 - You can accept the loss.
 - You can duplicate the asset.
 - You can insure the asset.
 - You can protect the asset.

Executive management needs to make these decisions about all assets, and this list gives them the tools to do so.

- *Provide tiered countermeasure budgets versus solutions.* Chapters 17, 18, and 19 (17, "Countermeasure Selection and Budgeting Tools"; 18, "Security Effectiveness Metrics"; and 19, "Cost-Effectiveness Metrics") will assist in preparing a workable tiered plan. The tiered plan should present achievable goals versus budgets and explain clearly what cannot be achieved (what risks

will be accepted) for deferred budgets. Chapter 18 includes a spreadsheet tool (the Decision Matrix) that helps present what can and cannot be achieved with various budget options. Management needs to understand what risks they are accepting for budgets that they defer or program elements they decide not to budget.

- Use a Decision Matrix to help committees reach a consensus when there is no agreement on the choice of a particular approach. Chapter 17 explains and illustrates the use of the Decision Matrix.
- *Present the Case.* Now it is time to present your case. Good budget presentations are formed as an argument.

BASIS OF ARGUMENT

I recommend the following approach (get agreement at each step):

- Explain that the overall role of security is to protect the mission of the organization against individuals who would attack or misuse its assets for their own purposes.
- Explain the four kinds of assets every organization has:
 1. People
 2. Property
 3. Proprietary information
 4. Business reputation
- Explain the three types of users:
 1. Those who share the mission of the organization
 2. Those who oppose the mission of the organization
 3. Those who mostly share and sometimes work in opposition to the mission of the organization (crimes; misuse of organizational assets for personal purposes; creation of security risks to people, property, and information; and disgracing organization's reputation by their behaviors).
- Explain the types of threat actors:
 - Terrorists
 - Economic criminals
 - Violent criminals
 - Petty criminals
 - Subversives (including persistent policy offenders)
- Explain the overall vulnerabilities and potential consequences of threat actions against those vulnerabilities.
- Explain the types of countermeasures available to address the threats and vulnerabilities:
 - Hi-tech
 - Lo-tech
 - No-tech
 - Baseline security program (comprising all three types above)
 - Special countermeasures to address unique vulnerabilities
- Explain that for a security program to be effective, it must include all three elements (hi-tech, lo-tech, and no-tech, and a baseline security program to address policy, criminal, and terrorism threats and special countermeasures to address criminal and terrorism threats).

- Present the threats and consequences.
- Present the baseline security program elements and their benefits and risks.
- Present the proposed security program and budget.
- Identify each budget item with a vulnerability or vulnerabilities and its potential consequences.
- As you go through this list, ask management to check off which consequences are acceptable losses, which they can duplicate, which they can insure, and which they would like to protect.
- Let management draw its own conclusions. Its conclusions may not be entirely what you want as the program manager, but this approach, when used repeatedly, plants the seeds of understanding of priorities. Also, when asked to check off what consequences are acceptable, early in the discussion, there is a higher likelihood that management will find the resources to meet the needs to protect against the unacceptable consequences.
- Ask management what conclusions it reaches resulting from these considerations and if it needs further assistance with any elements. It is a good idea to either gain consensus step by step or to stop at key points and gain consensus. As management agrees with each individual element of the presentation, it is more likely that it will also agree with the need to fund the programs that can avoid the unwanted consequences. After saying yes so many times along the way to the argument's conclusions, it is less likely that they will say no to fund critical elements.

Countering Arguments

Management may bring up questions or objections to programs. In all cases, it is best to refer back to authority, so preparation is essential. The best authority is always the formation documents of the organization, its mission statement, or its core policies and procedures or codes and regulations.

Other authorities include crime statistics (to support threat claims, particularly relating to violent crimes) and industry or community crime trends.

Credible data presented in an unemotional way (“Just the facts, ma’am!”)* are always more forceful than emotional pleas. Never let ego enter the equation — not yours and not theirs. Defer to egotistical arguments with a statement like, “I know you will decide what is best for the organization when you have time to examine the data.” This kind of response helps management defer potentially bad decisions until later after it has time to collect its thoughts.

Security program managers need to fully understand the power of personal relationships in an organization. Time spent with key decision makers, influencers, and stakeholders can help you build a chorus of support during presentations when you need it most. Make sure you understand what your supporters and opposing stakeholders need so that you can provide legitimate support at key times. Make sure they understand that you are a supporter of their own department’s cause in management discussions.

Always refer back to potential consequences and their relationship to programs. Remind management that you are not driving toward a particular solution, but you want it to have the information necessary to make the best possible decisions.

* Credit to Joe Friday, *Dragnet* (TV series).

FIGURE 19.9 Complete Cost-Effectiveness Matrix

COMPLETE COST-EFFECTIVENESS MATRIX

Those readers who are not interested in building their own matrices may skip the balance of this chapter. Following are instructions for building the Cost-Effectiveness Matrix.

In Chapter 18, we studied how to build a matrix to evaluate the effectiveness of various aspects of the security program and the entire program. In this chapter, we will review how to build the Cost-Effectiveness Matrix.

The Cost-Effectiveness Matrix is by far the most complex and complicated matrix you can build. It is not for the faint of heart and can take many hours to build. However, if you have built the Security Program Effectiveness Matrix from Chapter 18, you are already about halfway finished building the Cost-Effectiveness Matrix. Congratulate yourself — before you begin the instructions, you are already halfway finished.

Figure 19.9 illustrates the Complete Cost-Effectiveness Matrix for a small project. The Complete Cost-Effectiveness Matrix also serves to illustrate and support the recommendations for the baseline security program and for the antiterrorism measures.

It is obvious from Figure 19.9 that the Complete Cost-Effectiveness Matrix is a very large and complicated spreadsheet. However, it is not beyond your ability. We will break the spreadsheet down into its constituent elements in the next several illustrations, and it will become obvious how the spreadsheet is assembled. The Complete Cost-Effectiveness Matrix for a very small project is illustrated in Figure 19.9. As you can see, it is a very large and complicated worksheet.

COMPLETE COST-EFFECTIVENESS MATRIX ELEMENTS

Although the Complete Cost-Effectiveness Matrix is large and complex, it is composed of a relatively small number of elements that we will break down in sufficient detail, illustrating each element separately for understanding. Together, these will compose the Complete Cost-Effectiveness Matrix. These include:

- Title
- Security Program Recommendations Summary Board
- Vertical Elements
 - Headers
 - Risk items

- Divisions of risk items by category (baseline security program and antiterrorism measures)
- Column totals
- Column totals (broken out by baseline security program and antiterrorism measures)
- Horizontal Elements
 - Risk descriptions
 - Item number
 - Page reference in the risk analysis report
 - Area
 - Location
 - Vulnerability class
 - Vulnerability description
 - Risk level
 - Countermeasure options
 - Cost elements
 - CCTV
 - Alarm/access control
 - Physical security
 - Operations
 - IT/communications
 - Mitigation value
 - Access
 - Deterrent estimate
 - Detection
 - Assessment
 - Delay
 - Response
 - Evidence
 - Risks by rankings
 - High
 - Medium
 - Low
 - Budgets by risk rankings
 - High
 - Medium
 - Low
 - Phase recommendations
 - Immediate action items
 - Phase 1
 - Phase 2
 - Phase 3
 - Budgets by phase recommendations
 - Immediate action items
 - Phase 1
 - Phase 2
 - Phase 3

Security Program Recommendations - Summary Board				
Risk Rankings>	High	Medium	Low	Totals
Phases> Immediate Action Items	518,400	1,000	0	519,400
Phase 1	428,000	435,000	0	863,000
Phase 2	28,000	0	0	28,000
Phase 3	0	0	0	0
	974,400	436,000	0	1,410,400

FIGURE 19.10 Summary Board

- Budget breakdowns by phases and consequences
 - Immediate action items
 - High
 - Medium
 - Low
 - Phase 1 items
 - High
 - Medium
 - Low
 - Phase 2 items
 - High
 - Medium
 - Low
 - Phase 3 items
 - High
 - Medium
 - Low

Security Program Recommendations Summary Board

Perhaps the most interesting part of the spreadsheet for consultants and decision makers is the security program recommendations summary board, shown in Figure 19.10. The security program recommendations summary board illustrates the recommendation budgets by consequence rankings and by implementation recommendations. It also provides breakdowns and totals in both dimensions.

Vertical and Horizontal Elements

The spreadsheet is broken into vertical and horizontal elements. The key vertical elements include the column headers, section breakdowns (baseline security program versus anti-terrorism measures), list of vulnerabilities, and column totals.

Vertical Elements

For the purposes of illustration, Figure 19.11 hides several columns so that you can easily see the big picture. Figure 19.11 illustrates the major vertical elements. A few

FIGURE 19.11 Vertical Elements

vulnerabilities are also illustrated in this figure for context. Note that most of the figures shown here hide irrelevant or redundant columns or rows so that the principle is more simply illustrated to facilitate understanding.

Horizontal Elements

Horizontal elements include risk descriptions, countermeasure options, cost elements, mitigation values, risk rankings, and budgets (by risk rankings and phase recommendations), and finally, phase recommendations and budgets by phase recommendations with budgets breakdowns both by phases and risk rankings.

Risk Descriptions

The left-most columns horizontally define the risks in the following manners (Figure 19.12):

- What is the vulnerability item number? (This should also align with item numbers in the Risk Analysis Report.)
- On what page in the report can this vulnerability description be found?
- What general area of the facility does this vulnerability concern?
- What specific location does the vulnerability concern?
- What class of offender does this vulnerability concern?
- What is the vulnerability description (brief descriptor)?
- What is the risk ranking?

Countermeasure Options and Cost Elements

The next set of columns defines the countermeasures and their rough-order magnitude budget estimates. These are broken out by the types of countermeasure technologies that they fall into. Figure 19.13 illustrates a simplified example.

Countermeasure Mitigation Values

Refer to Chapter 18 for instructions on how to prepare the security countermeasure effectiveness table. As you can see, it serves well as the basis for the Complete Cost-Effectiveness Matrix, simply by inserting the additional required rows and columns that are needed to complete the Complete Cost-Effectiveness Matrix. (For more on countermeasure mitigation values, see Figure 19.14.)

Risk Rankings and Budgets

The next section horizontally breaks out the budgets by risk rankings. Note that I used three columns corresponding to the risk rankings (high, medium, and low). This is to more simply total the vulnerabilities of each ranking and to facilitate budget extrapolation from

	A	B	C	D	E	F	G
1	Mega Towers						
2	Physical Security Assessment						
3 Countermeasure Cost Effectiveness and Budget							
11					Vulnerability		
12					Class		
13	Item	Page	Area	Location	Vulnerability	Risk	
14							
15							
16	1.01	5,67	All	All	Every Class	Security Program Development	Medium
17	1.02	5	All	All	Every Class	Security Policy Enforcement	Medium
18	1.03	5,66	All	All	Every Class	Outdated Security Policies	High
19	1.04	5,66	All	All	Every Class	Outdated Security Procedures	High
20	1.05	5,66	All	All	Every Class	Outdated Post Orders	High
46	1.31	5,67	Main Floor	Main Doors	Every Class	All Exterior Openings No Alarm	Medium
47	1.32	5,67	Main Floor	Main Doors	Every Class	Many Exterior Doors Left Open	Medium
48	1.33	5,67	Main Floor	Main Doors	Economic & Violence	Banned Persons Hard to Recognize	Medium
49							
50							
51	1.34		Main Floor	All	Terrorism	In the Dark about Developing Problems	High
52	1.35	5,67	Site	Site	Terrorism	Vulnerable to Vehicle Intrusion	High
53	1.36		East Drive		Terrorism	Forced Vehicle Entry	High
64	1.45		Main Floor	East Drive	Terrorism	Forced Vehicle Entry	High
65	1.46		Main Floor	Rear of Building	Terrorism & Economic	Forced Entry	High
66	1.47		Site	Property Entrance	Terrorism	Forced Vehicle Entry	High
67	1.48		Main Floor	Stage Door	Terrorism	Forced Entry	High
68	1.49		Site	Vehicle Screening	Terrorism	Explosives in Vehicle	High
69							

FIGURE 19.12 Risk Descriptions

	A	F	G	H	I	J	K	L	M	N
1	Mega Towers									
2	Physical Security Assessment									
3	Countermeasure Cost Effectiveness and Budget									
11										
12	Risk	Countermeasure								
13	Vulnerability									
14										
15										
16										
17										
18										
19										
20										
46										
47										
48										
49										
50										
51										
52										
53										
64										
65										
66										
67										
68										
69										
70										
71										
72										
73										

FIGURE 19.13 Countermeasure Options and Cost Elements

	A	H	P	Q	R	S	T	U	V
1	Mega Towers								
2	Physical Security Assessment								
3	Countermeasure Cost Effectiveness and Budget								
11									
12									
13	Item	Countermeasure	Access	Deterrent	Detection	Assess	Mitigation Value	Evidence	Total
14									
15		Baseline Security Program							
16	1.01	Develop a Security Steering Committee							0%
17	1.02	Consider an Inspections Department							0%
18	1.03	Develop New Security Policies							0%
19	1.04	Develop New Security Procedures							0%
20	1.05	Develop New Post Orders	14%	14%	14%	14%	14%	14%	98%
46	1.31	Alarm on All Exterior Openings	14%	14%	14%	14%	14%	14%	56%
47	1.32	Access Control on Most Exterior Doors	14%	7%	14%	7%	14%	14%	98%
48	1.33	Facial Recognition Software							70%
49									
50		Antiterrorism Measures							
51	1.34	Subscribe to Commercial Intelligence Briefing Service					12%		12%
52	1.35	East I Drive In/West Drive Out	14%	14%	14%	14%	14%	14%	70%
53	1.36	Reinforce Main Gates (2 in)	14%	14%	14%	14%	14%	14%	70%
64	1.45	Fixed Crash-Resistant Bollards @ Main Entry	14%	14%	14%	14%	14%	14%	42%
65	1.46	Burglar Bars on Rear Windows <4 meters	14%	14%	14%	14%	14%	14%	42%
66	1.47	K-12 Barrier at Property Entrance	14%	14%	14%	14%	14%	14%	56%
67	1.48	Reinforce Stage Door	14%	14%	14%	14%	14%	14%	98%
68	1.49	Explosive Sniffing Dogs	14%	14%	14%	14%	14%	14%	98%
69									0%
70									

FIGURE 19.14 Countermeasure Mitigation Values

the countermeasure cost estimates in cells to the left. The budgets are taken by multiplying the risk ranking cell (*always a value of 1 to serve for calculation purposes to follow*) times the cost total row “N” (from Figure 19.13). Figure 19.15 illustrates the risk rankings and budgets by risk ranking. This set of columns gives us the risk dimension costing for the security program summary board at the top of the sheet. (See Figure 19.10.)

Phase Recommendations and Phasing Budgets

The next dimension is provided by planning the work into phasing recommendations. Few clients will approach the entire set of security program recommendations in a single effort. The consultant who breaks out his or her recommendation by recommended phases usually gets a much warmer reception. Rather than leaving it to the client to figure out how to phase the project, it is useful to make a recommendation for phasing. Although the actual phasing may vary as the details of each phasing plan are evaluated by the client, this approach helps assure that the program succeeds in reaching the phasing evaluation effort.

In Figure 19.16, please note that the values for the phases are calculated based upon the budgets in columns to the left times the “1” in the phasing cells (AC ~ AF) shown in Figure 19.16.

Budget Breakdowns by Phases and Risks

The final set of columns is used entirely to populate the security program summary board at the top of the page. (See Figure 19.10.) These are divided into four sets of columns as follows:

- Immediate Action Items
 - With subcolumns for:
 - High risk
 - Medium risk
 - Low risk
 - Phase 1
 - With subcolumns for:
 - High risk
 - Medium risk
 - Low risk
 - Phase 2
 - With subcolumns for:
 - High risk
 - Medium risk
 - Low risk
 - Phase 3
 - With subcolumns for:
 - High risk
 - Medium risk
 - Low risk

	A	F	G	H	W	X	Y	Z	AA	AB
11	Mega Towers									
12										
13	Item	Vulnerability	Risk	Countermeasure	Risk	High	Medium	Low	High	Budget
14										
15										
16	1.01	Security Program Development	Medium	Baseline Security Program	Develop a Security Steering Committee	1	1	0	0	
17	1.02	Security Policy Enforcement	Medium	Consider an Inspections Department	Develop New Security Policies	1	1	0	0	
18	1.03	Outdated Security Policies	High	Develop New Security Procedures	Develop New Post Orders	1	1	20000	0	0
19	1.04	Outdated Security Procedures	High	Develop New Post Orders	Develop New Post Orders	1	1	20000	0	0
20	1.05	Outdated Post Orders	High	Develop New Post Orders	Develop New Post Orders	1	1	10000	0	0
46	1.31	All Exterior Openings No Alarm	Medium	Alarm on All Exterior Openings	Alarm on All Exterior Openings	1	1	0	40000	0
47	1.32	Many Exterior Doors Left Open	Medium	Access Control on Most Exterior Doors	Access Control on Most Exterior Doors	1	1	0	40000	0
48	1.33	Banned Persons Hard to Recognize	Medium	Facial Recognition Software	Facial Recognition Software	1	1	0	25000	0
49										
50										
51	1.34	In the Dark about Developing Problems	High	Anti-Terrorism Measures	Subscribe to Commercial Intelligence Briefing Service	1	1	400	0	0
52	1.35	Vulnerable to Vehicle Intrusion	High		East Drive In/West Drive Out	1	1	0	0	0
53	1.36	Forced Vehicle Entry	High		Reinforce Main Gates (2 In)	1	1	160000	0	0
64	1.45	Forced Vehicle Entry	High		Fixed Crash-Resistant Bollards @ Main Entry	1	1	12000	0	0
65	1.46	Forced Entry	High		Burglar Bars on Rear Windows >4 meters	1	1	1000	0	0
66	1.47	Forced Vehicle Entry	High		K-12 Barrier at Property Entrance	1	1	75000	0	0
67	1.48	Forced Entry	High		Reinforce Stage Door	1	1	4000	0	0
68	1.49	Explosives in Vehicle	High		Explosive Sniffing Dogs	1	1	20000	0	0
69								0	0	0
70						42	7	0	974,400	436,000
71										1,410,400

FIGURE 19.15 Risk Rankings and Budgets

FIGURE 19.16 Phasing and Phased Budgets

	A	H	AK	AL	AM	AN	AO	AP	
1	Mega Towers								
12	Item	Countermeasure							
13	Physical Security Assessment								
14	Countermeasure Cost Effectiveness and Budget								
15	Baseline Security Program								
16	1.01 Develop a Security Steering Committee			0	0	0	0	0	
17	1.02 Consider an Inspections Department			0	0	0	0	0	
18	1.03 Develop New Security Policies			20,000	0	0	0	0	
19	1.04 Develop New Security Procedures			20,000	0	0	0	0	
20	1.05 Develop New Post Orders			10,000	0	0	0	0	
46	1.31 Alarm on All Exterior Openings			0	0	0	40,000	0	
47	1.32 Access Control on Most Exterior Doors			0	0	0	40,000	0	
48	1.33 Facial Recognition Software			0	0	0	25,000	0	
49									
50	Antiterrorism Measures								
51	1.34 Subscribe to Commercial Intelligence Briefing Service			400	0	0	0	0	
52	1.35 East Drive In/West Drive Out			0	0	0	0	0	
53	1.36 Reinforce Main Gates (2 In)			160,000	0	0	0	0	
64	1.45 Fixed Crash-Resistant Bollards @ Main Entry			12,000	0	0	0	0	
65	1.46 Burglar Bars on Rear Windows <4 meters			1,000	0	0	0	0	
66	1.47 K-12 Barrier at Property Entrance			75,000	0	0	0	0	
67	1.48 Reinforce Stage Door			4,000	0	0	0	0	
68	1.49 Explosive Sniffing Dogs			0	0	0	200,000	0	
69				0	0	0	0	0	
70				518,400	1,000	428,000	435,000	519,400	
71								863,000	

FIGURE 19.17 Budget Breakdowns

These breakdowns array the individual budget numbers into information that can directly populate the cells in the security program summary board at the top of the Complete Cost-Effectiveness Matrix.

For Figure 19.17, please note that the values shown in the phasing columns are separated by risk based upon a multiple of the values in the phasing columns from Figure 19.16 and risk column from Figure 19.15. For example, the values in column AK (Figure 19.17) are derived from the values of column AG (Figure 19.16) and the values in column W (Figure 19.15).

For simplification and so that this illustration can be readable in the space available in a book figure, only the immediate action items and phase 1 are shown; however, as is obvious, columns are also created for phase 2 and phase 3, if applicable.

SUMMARY

The security program must be funded adequately so that it can protect the assets of the organization from harm. Most organizations' security programs suffer from a lack of effective management metrics. The lack of management metrics in any program is a certain source for program inefficiencies and possible mission failure. Useful management metrics not only help ensure the success of the mission of the program, but also help the security program director justify and explain the needs for the program to upper management so that they can make informed financial decisions that are in the best interest of the organization. Cost-effectiveness metrics are at the heart of this approach.

The Limitations of Cost-Effectiveness Metrics

Cost-effectiveness has only two components: cost and effectiveness. The biggest challenge of cost-effectiveness metrics is effectiveness. Cost-effectiveness is all about reasonable ratios to achieve reasonable security goals. We want the highest possible effectiveness for an affordable budget. Three questions present themselves:

1. What is the value of the possible consequences? (baseline for consideration)
2. What is an affordable budget to mitigate these consequences? (reasonable cost)
3. What is the highest effectiveness we can achieve within this budget? (highest effectiveness)

Well-prepared security programs for nonstrategic facilities usually have a capital budget range of between 1% and 2% of the cost of the facility alone, excluding fixtures, furnishings, and equipment. This budget estimate is appropriate for commercial, non-commercial, and critical infrastructure facilities. However, exceptions include facilities that house assets, the loss of which could constitute great harm to the community, such as chemical plants, nuclear power plants, nuclear weapons storage facilities, central banks, presidential palaces, and the like. For these types of facilities, the capital and operating costs of the program should be entirely driven by the consequences.

For a nuclear power plant, the annual cost of security can be many times the cost of that for a nonnuclear power facility.

Cost-Effectiveness Metrics

With an efficient way to estimate effectiveness, and cost being self-evident, we can devise a formula to estimate cost-effectiveness. The comparison is easy when the prices differ but the effectiveness is the same. As costs of each system rise, the difference in cost/effectiveness becomes the reduced value of effectiveness versus increasing costs. This formula is as follows:

$$(\text{SystemCost1}/\text{SystemCost1}) * \text{Effectiveness1}$$

$$(\text{SystemCost1}/\text{SystemCost2}) * \text{Effectiveness2}$$

$$(\text{SystemCost1}/\text{SystemCost3}) * \text{Effectiveness3}$$

The baseline cost is always divided by the cost under consideration so that all costs reduce the value of effectiveness by the factor of the increase of the cost over the baseline cost.

Communicating Priorities Effectively

Making the Case

As virtually every organization is under financial challenges, understanding that many program directors are vying for the same budget dollars, it is necessary for the security program manager to make a clear case for security program budget dollars.

- Develop the Arguments
 - Determine the priorities of management
 - Identify points of view of stakeholders and acknowledge them
 - Provide a list of consequences
 - Remember, all risks can be dealt with in one of several ways:
 - You can accept the loss.
 - You can duplicate the asset.
 - You can insure the asset.
 - You can protect the asset.
- Executive management needs to make these decisions about all assets, and this list gives them the tools to do so.
- Provide tiered countermeasure budgets versus solutions.
- Use a Decision Matrix to help committees reach a consensus when there is no agreement on the choice of a particular approach.
- Present the Case: Good budget presentations are formed as an argument.

Writing Effective Reports

INTRODUCTION

At the completion of this chapter, you will understand how to write effective reports including the four main documents that a presentation should include, the elements of a well-received report, report supplements, and the elements of a good boardroom screen presentation.

Up to now, we have been discussing all of the tools necessary to create a good Risk Analysis Report. The Risk Analysis Report is the only thing decision makers will see; thus, it is the only element of the work that they will care about, so despite all the hard work, research, and analysis that the analyst has expended, if the report is flawed in any way, that will be all the decision makers will notice. The form and content should be complete, easy to read, digestible, and comprehensive.

Reports typically include four main documents:

1. The Comprehensive Report
2. Countermeasures Budgets
3. A Microsoft PowerPoint Presentation
4. Handouts for the Presentation

- *The Comprehensive Report*

The comprehensive report is the heart of the presentation (hereinafter we will call this “the report”). Except for the budgets and the executive summary, the other documents may be viewed only briefly and superficially. The report presents all the data in two forms: the executive summary and detailed sections. The executive summary should contain all the essential points of the detailed sections but in a form that is brief and easy to interpret. The detailed sections will contain the “meat” of the report and will provide the support for the conclusions, recommendations, and all statements in the summary section.

- *Countermeasure Budgets*

Countermeasure budgets are also presented in two versions: summary and detailed spreadsheets. The summary section contains the totaled results from the detailed sections. Ideally, the detailed sections should be broken out by hi-tech, lo-tech, and no-tech programs, and may be further broken down from those broad areas. Microsoft Excel allows for related spreadsheets to be viewed as individual pages of the same workbook. Using this method, one can create

a summary sheet that totals the results of all other sheets, for inclusion in the executive summary of the report.

- *PowerPoint Presentation*

A PowerPoint presentation is useful when presenting the Risk Analysis Report to a group or to a high executive. PowerPoint presentations allow condensed information to be presented in a manner that is easy to digest and can be highly graphic. They also guide the presentation and help recipients stay on point in their comments.

- *Handouts for Presentation*

Handouts echo the PowerPoint presentation and allow the recipients to follow along and make notes to facilitate their own memory, or for later discussion.

These documents together comprise the total report, and these alone make the case for security program needs. If the report fails in any way, the security program will not be supported or funded properly to achieve its goals. Failure can occur in several ways:

- Flawed presentation
- Flawed analysis (obvious bias, unsupported conclusions, etc.)
- Budgets that exceed the appropriate in the context of the overall project

Presentation

The client's report committee will most likely want a formal report presentation. Two types of readers review the Risk Analysis Report: readers who skim the document and readers who read and study the detail in the document. The comprehensive report must speak to both.

Key presentation elements for success include:

- Presentation should review project purposes and objectives
- Presentation should follow a predictable outline (handouts help here)
- Presenter should stay on logical key points and not stray to irrelevant minutia
- Presenter should make the case for any interventions (countermeasures) proposed
- Presenter should show a budget, ideally phased by priorities
- Presenter should answer all the questions about consequences and budgets

Graphics

Graphics are most helpful in explaining concepts and making points. Common useful graphics include

- *Risk Analysis Process Map:* A graphic showing the steps of analysis (see Figure 20.1).
- *Assets Map:* A list of assets by categories/criticalities
- *Threat Actor Map:* A list of threat actors, ranked
- *Vulnerabilities Map:* A list of vulnerabilities, sorted by assets
- *Risk Map:* V² graphics
- *Countermeasures Examples:* Photos of implementations and products

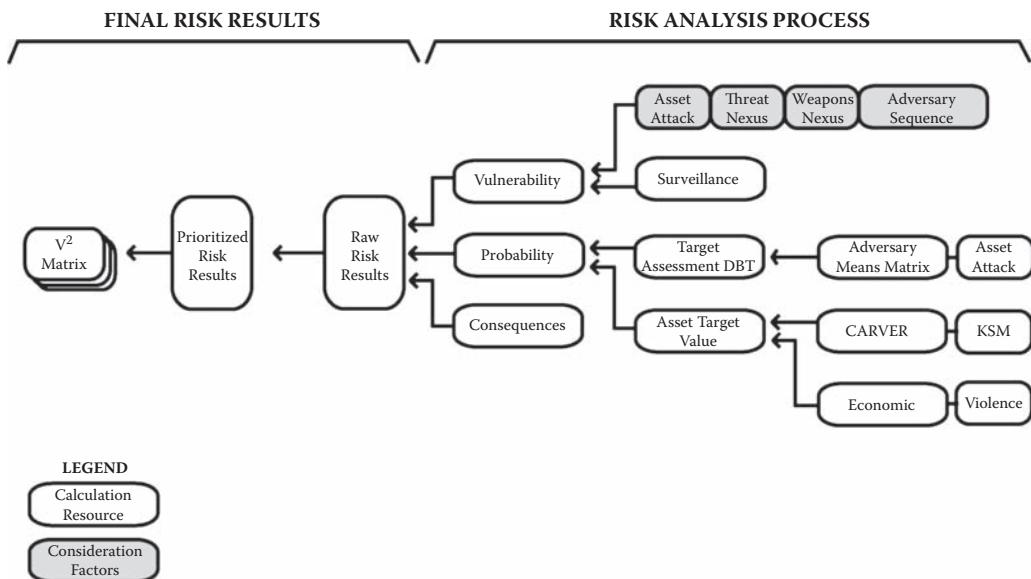


FIGURE 20.1 Risk Analysis Process Map

- *Budget Summary*: Colored graphic of budgets/phased
- *Risk Register*: Table outlining all above (optional)

Preparation for a Successful Presentation

The risk analyst should prepare and present the report in a manner that will be well received by the intended recipients. This requires research into two main areas: business culture and personal biases:

- *Business Culture*: The business culture of the organization to receive the report may vary significantly from one organization to the next. Some organizations want a focus on numbers and validation, and others are more interested in the consequences of countermeasures to their business operations. The analyst should research and understand such factors while preparing the report and the presentation. Tips to the business culture can be gathered from the organization's mission statement and from observing how management discusses and relates to its employees, contractors, vendors, customers, the public, activist groups, and the media. The following types of business cultures are common:
 - *Top-Down*: Top-down cultures impose business behaviors from top management downwards and impose behaviors by edict. These organizations are common in militaries and highly structured organizations that are rules driven.
 - *Lateral*: Lateral cultures are more democratic and sometimes chaotic. Objectives are set and achieved by consensus.
- *Personal Biases*: Similarly, the personal biases of key recipients will largely affect the acceptance of the presentation and conclusions. Each person inherently brings at least three biases with them to a project:

- Their Industry's Agenda
- Their Organization's Agenda
- Their Personal Agenda
- Personal biases vary as substantially as the recipients. The more information one can gather about the key recipients, the better. The following types of personalities are common:
 - *General Biases:* Different people have different ways of seeing things. Some are cautious, and others are aggressive. Some are deliberative, and others rush to decisions. Some are consensus builders, and others are forceful and opinionated, and still others are timid.
 - *Industry Biases:* Each project participant also brings their industry biases to the project. They will naturally look out for the best interests of their building system or industry in all discussions of the work.
 - *Organizational Biases:* Each participant may also keep in mind the best interests of the organization he or she works for, constantly looking to protect and defend his or her organization's reputation and project position, looking for opportunities to improve his or her position through opportunities for additional services, self-directed compliments, and so forth.
 - *Personnel Biases:*
 - *Executive biases:* Executive biases are focused on the purpose and objectives (including business culture objectives) and budget. As these are sometimes in conflict with each other, executive biases can be confounding to other team members as they try to understand why executives will sometimes focus on the project's purpose, objectives, and business culture and then may later shift focus to budget, sometimes apparently abandoning purpose and objectives. Also it is common for business culture objectives to be poorly understood or stated, as these are often assumptions that are not well translated into objectives.
 - *Administrative biases:* Administrative biases are focused on business and project process over project purpose and project objectives. (Effective project managers often exhibit a combination of both executive and administrative biases.)
 - *Technical biases:*
 - *Tactical:* Tactical technical biases are focused on the tactical technical details of how to achieve the project objectives (which products, types of cables, lenses, etc.). It is common for technical personnel to become distracted by minutiae to the detriment of project purposes and objectives. However, technical personnel who maintain focus on project purposes and objects are extremely valuable.
 - *Analytical:* Analytical technical biases are usually focused more on project purposes and objectives and on how to use technical tools to achieve those. These people are highly valuable to the project process as they are able to discuss technical details in a way that maintains the focus and achieves support of other project team members. They are also especially valuable in coordination efforts.
 - *Egocentric:* Egocentric personalities can overlay any of the others. Every project member has some ego. More productive project members set aside their own personal biases for the betterment of the project and

organization. Lesser individuals view everything through the lens of their own perception and always in the best short-term interest of themselves and their allies often to the detriment of the project.

Understanding the industry, organization, and personal biases of each project participant is of great value in being able to prepare and present the report in a manner that will be well received by every key project stakeholder.

Executive and administrative personalities usually prefer presentations that focus on the project purpose and objectives and how the findings fit those objectives, and by extension, “what” interventions are necessary to assure that the organization’s programs are not disrupted by security events. Executive and administrative personalities are also highly concerned about the cost of any interventions. Executive personalities are more interested in the consequences of such interventions on their business culture.

Technical personalities are more interested in “how” such interventions will be implemented.

Each participant also filters the presentation by their industry, organization, and personal biases and by how it affects their position in the group.

Virtually all stakeholders are concerned about the security budget or operations infringing on their own budget or operations.

Sensitivity to these issues will help result in better analysis, better conclusions, and better acceptance.

THE COMPREHENSIVE RISK ANALYSIS REPORT

Executive Summary

The executive summary provides the essential delivery of all of the data of the report. The executive summary will be read by everyone who sees the report; thus, it must be complete, highly readable, and convincing.

The executive summary should:

- Provide a document outline, identifying the sections and their general contents.
- State the project purpose and objectives.
- Identify the key assets.
- Identify the key threats.
- Identify the key vulnerabilities.
- Identify the key risks.
- Identify the key countermeasure program interventions.
- Present budgets.
- Make recommendations.

Introduction

The introduction frames the readers’ understanding of the rest of the document. This is done by providing the background information the reader needs to know to put the balance of the report into perspective. The introduction should include:

- *Project Authorization:* A statement including who authorized the report and for whom the report is being prepared (usually, but not always the same person or organizational unit).
- *Background Statement:* A background statement on the project should include
 - Its location
 - Project attributes (how many buildings, what types, usages, etc.)
 - Goals of the security program
 - Assessment Team Qualifications

Assessment Process

The assessment process section can be included in the introduction or may be separate. On smaller projects, I usually combine these. This section should include:

- The methodology selected
- Reason for selecting this particular methodology (why it best fits the project: budget, completeness, appropriateness to the industry, U.S. Department of Homeland Security [DHS] mandates, etc.)
- Methodology process map
- Assessment process planning

Facility Characterization

The facility characterization section is sometimes also called the asset characterization section. This section itemizes and categorizes all of the assets of the organization related to the project.

Each of the assets in question will include a system, asset, component, or critical node. Systems are whole functional organisms that are often crucial to the mission of the organization. Assets are individual facilities, buildings, business units, people, property, proprietary information, or the organization's business reputation. Components are individual elements of assets and systems. Critical nodes are elements that are critical to the operation of an entire system. If a critical node is lost, so, too, will be an entire system.

Then list all of the facility assets by the following categories:

- People
 - Key Executives
 - Managers and Employees
 - Contractors, Vendors, Visitors, and the Public
- Property
 - Individual Areas
 - Categorized by Facilities and Major Areas of Facilities
- Proprietary Information
 - Information Technology System
 - Special Servers and Mass Storage
 - Paper Files
 - Special Information Systems (Building Management System/Security, etc.)
- Business Reputation

Threat Assessment

The key elements of the threat assessment section include identification of the threat actors and the selection of a particular class of threat actor as the design basis threat.

There are five types of threat actors. It is useful to explain each of these in detail.

- Terrorists
 - Class I Terrorists (State Sponsored)
 - Class II Terrorists (Religious Extremist Professional Terrorists)
 - Class III Terrorists (Radical Revolutionary or Quasi-Religious Extremist)
 - Class IV Terrorists (Guerrilla/Mercenary Soldiers)
 - Class V Terrorists (Lone Wolves)
- Economic Criminals
 - Transnational Criminal Organizations
 - Organized Crime
 - Sophisticated Economic Criminals
 - Unsophisticated Economic Criminals
 - Street Criminals
 - Lone Wolves
- Nonterrorist Violent Criminals
 - Domestic Crimes Violent Criminals
 - Disgruntled Employee or Ex-Employee
 - Deranged Persons
- Subversives
 - Cause-Oriented Subversives
 - Nonaligned Subversives
 - Invasion of Privacy Threat Actors
 - Persistent Rule Violators
- Petty Criminals
 - Vandals
 - Pickpockets
 - Prostitutes, Pimps, and Panderers

The design basis threat is that class of threat actor against which the proposed security program is designed to effectively counter.

Although terrorism is the most potent threat, it may not be relevant to the organization or facility in question. If there is no history of terrorism against this type of organization or facility and if it does not meet many or most of the criteria of the terrorism asset target value profiles, it may not need to be considered as a valid threat. Ultimately, the client must make the decision whether or not to consider terrorist threat actors.

It may be good to discuss the relevant considerations in detail. Although the threat matrices identify all these factors, the matrix does not explain them. The two threat matrices include the Asset/Attack Matrix and the Adversary/Means Matrix. Both of these identify threat scenarios, and the Adversary/Means Matrix also identifies information about the threat actors' characteristics, including their motivation, capabilities, and history. Although these are estimated in the matrix, they can be explained in the threat assessment section of the report.

The analyst should explain in detail each column of the threat matrices so that the reader understands the context of the estimates.

Additionally, I recommend that the analyst should conduct research into each class of threat actor listed for which any serious consideration is recommended by the analyst, and provide references and evidence as to why each of these are relevant to the project. For example, if a particular terrorist group is relevant, cite examples that illustrate their relevance to the project.

The threat assessment section should conclude with a section on the design basis threat. Make a case for which class of threat actor is selected and why this is the most relevant. Also list the type of entry methods and weapons most used by the design basis threat. It will be these entry methods and weapons that the countermeasures program must be designed to counter.

Vulnerability Assessment

Vulnerability assessment involves the following steps:

- Define Scenarios and Evaluate Specific Consequences
- Evaluate Effectiveness of any Existing Security Measures
- Identify Vulnerabilities and Estimate the Degree of Vulnerability

These steps are carried out by utilizing the following steps:

- Utilize an Asset/Attack Matrix that identifies which attack scenarios are most effective against each asset.
- Utilize a Threat/Target Nexus Locations Matrix that identifies which areas are most likely to be used by threat actors.
- Utilize a Weapon/Target Nexus Locations Matrix that identifies which types of weapons are most likely to be used at each threat/target nexus location.
- Review surveillance opportunities for each major asset under consideration.
- Review vulnerabilities for each asset under consideration.
- Identify whether or not the vulnerability will be addressed by a baseline security program.
- Especially for those assets for which vulnerabilities are not addressed adequately by a baseline security program, list the criticality of each of those assets.
- For the purposes of the executive summary, prioritize assets by the criteria as described in Chapter 11.

The analyst should consider and report which assets are subject to which types of attack scenarios. Regardless of which analytical tool is used (commercial software or spreadsheet templates), this step must be accomplished for the vulnerability report to have meaning.

Most commercial software has a tool that evaluates each asset against each type of applicable threat scenario. The Asset/Attack Matrix is the template used to do this in the software template tools in this book, but any such tool will work as long as it considers each asset and each applicable threat scenario.

Vulnerability includes the following constituent components:

- Surveillance Opportunities
- Accessibility
- Intrinsic Vulnerability

The following factors mitigate intrinsic vulnerability:

- Existing and Natural Countermeasures
- Electronic Countermeasures
- Physical Countermeasures
- Operational Countermeasures

The result of the first three factors minus the last four equals vulnerability.

Asset / Attack Matrix

The Asset/Attack Matrix or its equivalent should be included in this section to support the vulnerability findings. Each aspect of the Asset/Attack Matrix should be explained in detail.

The analyst should explain the applicable threat scenarios in detail in the vulnerability section of the report and then show the evaluation of each asset for each scenario. This is the most basic vulnerability assessment, and most assessment tools do not go beyond this first step. The Excel templates in this book also provide for three other vulnerability evaluations.

Threat / Target Nexus Matrix

The Threat/Target Nexus Matrix evaluates circulation path nexus points that could be crossing points between especially vulnerable people (celebrities, C-level executives, female students, etc.) and potential threat actors. The Threat/Target Nexus Matrix helps the analyst identify areas of the facility where personal attacks could occur.

Weapon / Target Nexus Matrix

Similar to the Threat/Target Nexus Matrix, the Weapon/Target Nexus Matrix evaluates circulation path nexus points between especially vulnerable people and the types of weapons that could be used at those locations. For example, a vehicle drop-off area has a much wider range of weapons that can be used than does an executive elevator lobby. The Weapons/Target Nexus Matrix helps the analyst understand what types of weapons the victim might encounter at the circulation nexus points.

Surveillance Opportunities

Surveillance is a function of vulnerability. In order to carry out any type of attack (terrorism, economic crime, violent crime, subversive act, or petty crime), the perpetrator must know something about the facility and organization the perpetrator plans to attack. This requires surveillance. If surveillance is necessary for the attacker, then it is useful to understand that any threat actor performing surveillance is vulnerable to detection by an organization that has the skills to detect surveillance. This fact alone can reduce vulnerability.

Surveillance can be conducted several ways:

- Fixed Visual Surveillance
- Mobile Surveillance

- Acoustic Eavesdropping
- Electronic Surveillance (Wiretaps, Electronic Bugs, etc.)
- Information Technology System Surveillance
- Document/Information Interception

Minimizing the opportunities for surveillance or implementing a surveillance detection program can reduce the potential for all types of terrorism and criminal attacks.

The analyst should identify the types of surveillance possible, and, using the Surveillance Matrix or a similar tool, the analyst can identify those assets that are at most risk of surveillance.

Beware of risk analysis software tools that estimate vulnerability using only one cell labeled “Vulnerability.” This will almost always result in ineffective results. Vulnerability has many factors, and without considering each one individually, it is very easy to miss a factor that can raise the overall vulnerability of an asset, while thinking only of another factor. For example, an analyst who considers only accessibility in vulnerability would likely rank a bank vault with low vulnerability if the analyst was thinking about outside threat actors; without considering embezzlement, that would be a false ranking.

Risk Calculation

Risk = (Probability * Vulnerability * Consequences) or ((Probability + Vulnerability + Consequences)/3). There are numerous ways to calculate risk using a variety of tools. All such methods that take these three factors into consideration will result in a useful calculation.

By performing this calculation on all the assets under consideration, the analyst can reach individual risk calculations for all the assets under consideration. These can then be ranked for severity.

We will pause here to talk again about the differences between quantitative and qualitative analysis methods and how they relate to risk calculations. Qualitative analysis methods typically review many assets and then discard most after some initial consideration, leaving relatively few assets for the final risk analysis.

I have seen qualitative reports that considered less than a dozen assets for a multi-hundred-million-dollar project. In my opinion, this is a woefully inadequate analysis. On one such project, where the owner hired two consultants just to be sure, I found a critical node that if attacked would have disabled all operations for the organization for up to 2 years while the critical node was being repaired. This attack scenario on a minor building system would have left the key facilities intact but completely unusable until repairs were made, which were estimated to be between 1 and 2 years. This critical node was completely missed by the other consultant who had discarded as irrelevant the asset that had the critical node. I also would have missed the critical node until I performed the full analysis, because it was not obvious until the analysis was complete. I have seen similar results on many projects. This is why I am a believer in a combination of quantitative and qualitative analysis. The combination of the both is far better than either one alone.

Countermeasures

There are three main factors to selecting countermeasures:

1. All vulnerabilities should be addressed to some extent by a comprehensive baseline security program.

2. Key assets should be identified that should receive special attention by reviewing countermeasure options, including:
 - Hi-tech options
 - Lo-tech options
 - No-tech options
3. Costs should be estimated for the following:
 - The baseline security program
 - Countermeasures to address key assets not adequately mitigated by the baseline security program

Baseline Security Program

Every facility requires a baseline security program. The Baseline security program should include all of the elements covered in detail in Chapter 15 “Countermeasure Goals and Strategies.” The key elements that should be discussed in some detail include:

- Security Program Mission Statement
- Policies and Procedures
- Security Management and Supervision
- Hi-Tech Elements
 - Alarm/access control system
 - Parking control system
 - Security video system
 - Security communications system
 - Command/control elements
- Lo-Tech Elements
 - Locks
 - Pedestrian and roadway barriers
 - Lighting
 - Signage
 - CPTED* elements
 - Security landscaping
 - Security architectural elements
- No-Tech Elements
 - Security management elements
 - Security guard program
 - Posts
 - Patrols
 - Security guard training program
 - VIP handling program
 - Security awareness program
 - Physical security program
 - Security intelligence program
 - Countersurveillance program
 - Emergency preparedness and response program
 - Civil disorder preparedness and response program

* CPTED (crime prevention through environmental design) is a scientifically proven architectural discipline that helps reduce criminal behavior by creating spaces that encourage appropriate behavior and reducing the likelihood of criminal activity.

- Law enforcement liaison program
- Security management metrics

Identifying Key Assets for Special Consideration

- Identify key vulnerabilities that are not adequately addressed by the baseline security program.
- Rank each of those vulnerabilities by:
 - Mitigated/not mitigated by the baseline security program (sort 1)
 - Above assets most vulnerable (sort 2)
 - Above assets (sorts 1 and 2) that are the highest asset target value (sort 3)
 - Above assets (sorts 1 through 3) that have the highest consequences (sort 4)
- For the above filtered assets (those with special vulnerabilities), focus on key countermeasures that exceed the baseline security program and which could mitigate the vulnerabilities. (See more about this in Chapter 16, “Types of Countermeasures.”) The essentials include:
 - Can the asset be easily replaced, duplicated, or insured?
 - Consider each special vulnerability as to access. (What is the asset? What is the threat scenario? Who is the likely threat actor? What access is available to attack the asset?)
 - How can access be limited or denied to unauthorized persons?
 - What about unauthorized access using force?
 - What about access by insiders, contractors, and vendors?
 - Can the vulnerability be mitigated by limiting access?
 - How could access be limited (safe, bullet-resistant/blast-resistant glass, guard, barriers, delaying technologies, etc.)
 - What other types of countermeasures could:
 - Control access
 - Deter
 - Detect
 - Help assess the threat act
 - Help respond to and delay a successful attack
 - Gather evidence
 - Could countersurveillance reduce the possibility of an attack?
 - What is the relative effectiveness of each of the possible countermeasures?
 - Are multiple countermeasures required to mitigate the threat?
 - What are the cost estimates of these countermeasures?
 - If multiple options are available, what are their overall effectiveness ratings and relative costs?
 - What are the cost-effectiveness rankings of the multiple options?
 - What are your recommendations?
 - What consequences on organizational operations (productivity, convenience, and business culture) will there be by using the recommended countermeasures?

Develop Countermeasure Budgets

Use the countermeasure budgeting tool or a similar tool to develop countermeasure budgets. Provide separate budgets for the baseline security program and for the special countermeasures.

Provide a budget summary sheet that identifies the key budget elements and recommended phasing.

Provide a detailed budget analysis for the baseline security program and for the special vulnerabilities.

Provide recommended countermeasure interventions (hi-tech, lo-tech, and no-tech) for the baseline security program and for the special vulnerabilities. Provide justification for each recommendation in terms of:

- Criticality of the assets protected
- Probability of a loss
- Consequences of the loss
- Probable effectiveness of mitigation using recommended countermeasures
- Cost of countermeasure recommended
- Consequences on organizational operations (productivity, convenience, and business culture)

Provide a Decision Matrix if multiple options are presented. (See Chapter 17, “Countermeasure Selection and Budgeting Tools.”)

Countermeasure Implementation Recommendations

Provide a recommended countermeasure implementation phasing plan. There are two types of phasing programs for construction-oriented projects and nonconstruction programs:

- *Construction-Oriented Programs:* For any programs that are focused on the construction of new facilities or major renovations of facilities, the countermeasure phasing program can be coordinated with the construction program. This typically follows a schedule, such as:
 - *Schematic (Planning) Phase:* The security program planning should occur during this phase
 - *Design Development Phase:* Policy development and security systems device placements planning should occur during this phase.
 - *Construction (Bid) Documents Development Phase:* Procedures development, program development, and staff planning should occur during this phase.
 - *Bidding Phase:* Bids for systems and guard services can go out at this time.
 - *Construction Phase:* The construction of the security systems, physical security elements, and guard staffing and training can occur during this phase.
 - *Project Completion:* Acceptance testing for systems and guard scenario training will occur during this phase.
- *Non-Construction-Oriented Programs:* Non-construction-oriented programs will follow the same steps, but they will be independent of coordination with a construction cycle. They will, however, need to be coordinated with ongoing operations.

Report Supplements

Risk Register

A risk register is a table that includes columns for:

- Risk Category
- Risk Name

- Risk Number
- Probability (1–3)
- Vulnerability (1–3)
- Consequences (1–3)
- Risk Score ($P * V * C$) or $((P + V + C)/3)$
- Mitigation Recommendation
- Contingency
- Action By
- Action When

A risk register (Figure 20.2) can most easily be assembled from the data in the Vulnerability/Countermeasure Matrix.

Footnotes

Reports that use ample footnotes are better received than reports that are unsupported. Footnotes give the analyst the opportunity to provide source references for statements made that might not be common public knowledge. Footnotes can also be used to define terms as they are introduced, or to expand by opinion or example on a point made in the text.

Tables

The following tables are very helpful in any sizable report:

- Table of contents, including chapter numbers and chapter names, major headings, and page numbers
- Table of figures

Index and Glossary

Following the report text, it is useful to provide an index and a glossary:

- *Index:* Better word processors have index functions that make creating an index relatively easy. Generally, the analyst can assemble the document into a single file (if not already formatted as such) and then scan the file for key words the analyst would like to include in the index. Then, using the index function in the word processor, that word will be marked for indexing, and the index function will automatically reference everywhere in the document that the word is used. Finally, the index function will alphabetize the index and add page numbers.
- *Glossary:* It is good to define any unfamiliar or industry-specific terms used throughout the report as the term is introduced. This can be done either in the text or in footnotes, and unfamiliar terms can also be assembled in a single place in the glossary. The glossary defines key terms used in the report in a single location. The index and footnotes are also the keys to building the glossary. The glossary can be built by opening a separate word-processing document named *glossary* and then scanning the footnotes and index for key words that you want to place in the glossary. Then go back and define each term in the glossary, using footnote references if necessary.

Attachments

Also recommended is the use of supporting attachments that could include such documents as:

Mega LNG Terminal Risk Register										
Risk Number	Risk Category	Risk Name	Probability	Vulnerability	Risk Score	Mitigation Recommendation	Contingency	Action By	Mitigation Action When	Contingency Action When
1.1	Perimeter	Civil Disorder	1	3	2	6	Coordinate with Police	Close Down Facility	Security Mgr.	Now
1.2	Perimeter	Car/Truck Bomb	1	3	3	9	K-12 Security Barriers & Procedures	Mitigation Plan	Capital Projects	On Event
1.3	Perimeter	Waterside Bomb	1	3	3	9	Waterfront Barrier	Patrol Boats	Security Committee	Phase 1
2.1	LNG Tanks	Airplane Attack	1	3	3	9	Radar Warning System	Mitigation Plan	Capital Projects	Immediate
2.2	Lobby	Swarming Attack	1	3	2	6	Access Control System	Full Height Counters	Capital Projects	On Event

FIGURE 20.2 Risk Register

- Terrorism Risk Determination Variables
- Bomb Threat Stand-Off Distances
- Chemical/Biological/Radiological Agent Threats
- Reports on Any Relevant Terrorist or Organized Crime Organizations
- Countermeasures Budgets

Countermeasure Budget Presentation

The summary and comprehensive budgets should be presented as attachments. See Chapter 17, “Countermeasure Selection and Budgeting Tools” for information on how to prepare countermeasure budgets. Then insert the budget as an attachment to the report.

A Microsoft PowerPoint Presentation

It is useful in most cases to prepare a PowerPoint presentation as a talking tool when presenting the risk analysis and countermeasures recommendations and budgets. When preparing the presentation, stay on the key points of the executive summary and follow that exactly.

Use illustrations of assets, threat actors, vulnerabilities, and risk analysis conclusions. Present an initial overview of the contents of the presentation, followed by sections and pages with each slide showing the section and the page relative to the overall contents. This helps the viewers maintain focus on the progress of the presentation.

Conclude with a questions-and-answers slide.

The slides that help viewers maintain focus are usually of light background colors, sans-serif fonts, and coordinated colors for the headers and subject fonts. The master slide should also include page numbers (page X of XX), and it helps to have a set of section names at the bottom that change color as you move through the section, such that sections already reviewed are shown on the left and are of a lighter color, the section now being viewed is more prominent, and sections to be viewed are a lighter color to the right.

For certain clients, having your name and contact coordinates in the footer also helps them to get back to you for further comment or questions. This is especially helpful if some viewers are midlevel managers who have lots to contribute but might feel intimidated in the midst of high-level executives. Their comments can be conveyed in a supplemental report later. If you have any known disruptive attendees, supplemental comments could be unwanted.

Handouts for the Presentation

Microsoft PowerPoint has a handouts print function that provides handouts in several formats. I have found that the “Three Slides per Page with Notes beside Format” is most useful, as the viewer can follow along and take notes for the questions-and-answers section. Handouts are always best when given in color.

SUMMARY

Reports typically include four main documents:

1. The Comprehensive Report
2. Countermeasures Budgets

3. A Microsoft PowerPoint Presentation
4. Handouts for the Presentation

The Comprehensive Report

The comprehensive report is the heart of the presentation. Except for budgets, the other documents may be viewed only briefly and superficially. The report presents all the data in two forms: summary and detailed sections. The summary typically contains all the essential points of the detailed sections but that is brief and easy to interpret. The detailed sections will contain the “meat” of the report and will provide the support for the conclusions, recommendations, and all statements in the summary section.

Countermeasures Budgets

Countermeasure budgets are also presented in two versions: summary and detailed spreadsheets. The summary section contains the totaled results from the detailed sections.

PowerPoint® Presentation

A PowerPoint presentation is useful when presenting the Risk Analysis Report to a group or to a high executive. PowerPoint presentations allow condensed information to be presented in a graphic manner that is easy to digest.

Handouts echo the PowerPoint presentation and allow the recipients to follow along and make notes to facilitate their own memory, or for later discussion.

Presentation

The client’s report committee will most likely want a formal report presentation. The two types of readers review the Risk Analysis Report are readers who skim the document, and readers who read and study the detail in the document. The comprehensive report must speak to both. Key presentation elements for success include:

- Presentation should review project purposes and objectives
- Presentation should follow a predictable outline (handouts help here)
- Presenters should stay on logical key points and not stray to irrelevant minutia
- Presenters should make the case for any interventions (countermeasures) proposed
- Presenters should show a budget, ideally phased by priorities
- Presenters should answer all the questions about consequences and budgets

Graphics

Graphics are most helpful in explaining concepts and making points. Common useful graphics include:

- *Risk Analysis Process Map:* A graphic showing the steps of analysis
- *Assets Map:* A list of assets by categories/criticalities
- *Threat Actor Map:* A list of threat actors, ranked
- *Vulnerabilities Map:* A list of vulnerabilities, sorted by assets
- *Risk Map:* V² graphics
- *Countermeasures Examples:* Photos of implementations and products
- *Budget Summary:* Colored graphic of budgets/phased

Preparation for a Successful Presentation

The risk analyst should prepare and present the report in a manner that will be well received by the intended recipients. This requires research into two main areas: business culture and personal biases.

- *Business Culture:* The two types of business cultures are top-down and lateral.
- *Personal Biases:* Similarly, the personal biases of key recipients will largely affect the acceptance of the presentation and conclusions. Each person inherently brings three biases with them to a project:
 - Their Industry's Agenda
 - Their Organization's Agenda
 - Their Personal Agenda

Index

A

Access cards, 269
active, 270
bar coded, 270–271
contactless smart, 271
key fobs, 270
magnetic stripe, 269
proximity, 270
radio frequency (RF) devices, 270
TWIC, 271
Wiegand wire cards, 269–270

Access control
after-hours, 228
card technologies, 269–271
credential reader technologies, 271–275
goal of, 250
and impediments to business, 260–261
policies for, 228
requirements, 92
restricted areas, 228
strategies, 251
surveying, 91–92
systems, 218, 228
types, 251

Accessibility, 26
posts, 230
vulnerability assessment, 153

Accidents, 113

AcuTech Consulting Services, 57
Adversary/Means Matrix, 59, 131, 133
attributes, 129
functions, 129
purpose, 129
worksheet instructions, 134–137

Adversary Sequence Diagram, 60, 148–150,
183, 330–331, 332

Aircraft, 312

Al Qaeda, 61, 117, 127, 142

Alarm systems, 154, 218; *see also* Detection
Alarms

duress, 254, 255, 281
false, 269, 277, 278, 279
hold-up, 254, 255
nuisance, 255
silent, 255

All hazards risk analysis, 114–115
American Bankers Association (ABA) stripe,
269

American Medical Association, 121

Analysis phase, 38

Analysis skills, 6–8

Analysis tools, 8

Animal Liberation Front (ALF), 326

Anthrax, 120

Antiterrorism

checkpoints, 299
expenditures, 161
resources, 118
vulnerability assessment, 144

API/NPRA (American Petroleum Institute/
National Petrochemical and Refiners
Association), 23

strengths and weaknesses, 31–32
versus Sandia model, 176–179

Archiving

of evidence, 304
redundant systems, 291
schemes, 290–291
storage media, 289
technologies, 288–290

*ASIS International's Protection of Assets
Manual*, 52

*ASIS International's Security Industry Buyers
Guide*, 52

ASIS International's Seminar and Exhibits, 52

ASME Innovative Technologies Institute, 29

ASME ITI Tools, 29

ASME RA-S, 31

Assassinations, 116, 117, 119, 153, 313

Asset/Attack Matrix, 127, 128, 129, 130,
144–146

Asset characterization, 17, 27

in Risk Analysis Report, 372

Asset Target Value Matrices, 60, 127, 184–186

Assets; *see also* Surveys

categorization of, 86–87
classes, 27, 42, 86
control policies, 229
cost of replacement, 103
criticality, 51

- diversion of, 315
 facility list, 88–90
 interviews about, 87–88
 listing, 59, 85–86, 88–90
 to the mission, 26, 28
 recuperation, 26
 research on, 90
 tools, 59
 tools for listing, 97–98
- Assumptions**
 critical thinking, 75
 understanding, 81
- Attacks**
 9/11 attacks, 60, 167, 325
 Columbine High School, 147–148
 cyber, 154
 detection, 254
 Mumbai, 142, 143, 147, 165
 objective parameters, 313
 scenarios, 132–133, 144, 310–312
- B**
- Badges**; *see* Access cards
- Barriers**, 219
 deployable, 296
 pedestrian, 296–297
 vehicle, 296
- Baseline security program**, 101, 130, 194
 countermeasures, 267–268
 deterrence package, 299–302
 elements, 265–267
- Best practices**, 207
- Biometric readers**, 274–275
- Black September**, 116
- Bombs**; *see* Explosive detection
- Border security**, 241
- Budgeting**, 378–379; *see also* Cost-effectiveness
 decisions, 199
 deliverables, 38
 phasing, 361
- Burglary**, 315, 325
- Business culture**
 complying with, 259–260
 and policy development, 211
 and presentations, 369
- Business organizations**
 customers, 43, 92
 functional organization chart, 42, 92
 hours of operation, 93
 impediments to operation, 260–261
 mission statements, 26, 28, 41
 processes, 41–42
- productivity, 27, 211
 surveying, 92–93
- Business reputation**, 27
 characterizing, 43
 crimes against, 328
- C**
- Cameras**; *see* Video detection systems
- CAP Index**, Inc., 50, 169, 183
- CARVER + Shock**, 32, 60, 166–167
- Casualties**, 27, 189
- CFATS**; *see* Chemical Facility Anti-Terrorism Standards
- Change**, 81
- Chemical Facility Anti-Terrorism Standards (CFATS)**, 32, 242
- Chemical security**, 242
- Chemical weapons**, 225
- Circulation Path/Threat Nexus Matrix**, 62, 183, 188
- Circulation Path/Weapons Nexus Matrix**, 62, 183, 188
- Civil disorder**, 326
- Closed-circuit television (CCTV)**, 56, 303, 308, 315
- Command, control, and communications (C³) consoles**, 288
- Communications systems**, 43, 218, 258, 266, 302
- Complete Cost-Effectiveness Matrix**, 353
 budget breakdowns by phase and risk, 361, 364, 365
 countermeasure costs, 357, 359
 countermeasure mitigation values, 357, 360
 elements, 353–355
 horizontal elements, 355, 357
 phase recommendations and budgets, 361, 363
 risk descriptors, 357, 358
 risk rankings and budgets, 357–358, 361, 362
 Summary Board, 355
 vertical elements, 355, 356, 357
- Comprehensive Report**, *see* Risk Analysis Report
- Conflict**, 81
- Consequence assessment**, 17, 51, 103
 components, 188–189
 sources, 113–114
 tools, 59
- Consequence Matrix**, 104
- Consequences**, 102
 and budgeting, 346
 versus criticalities, 101
 critical thinking, 76–77
 and degree of response, 334

- examples, 103
as formula variable, 20
measurement of, 103
and risk prioritization, 195
variables, 26
- Consoles, 288
- Contractors
background checks, 228
business reputation characterization, 43
vetting, 94
- Control points, 211
- Cost-benefit analysis, 56
- Cost-effectiveness; *see also* Complete Cost-Effectiveness Matrix
basis of argument, 351–352
calculation methods, 346–349
countering arguments, 352
limitations of metrics, 342–346
making the case, 349–351
metric limitations, 342
recommendations summary board, 355
- Costs
of asset replacement, 103
methodologies, 23, 24
and risk prioritization, 195–196
of software programs, 24
training, 24
- Countermeasure budgets, 367–368
- Countermeasure Decision Matrix, 318
- Countermeasure Effectiveness Estimate (CEE), 335
- Countermeasure Effectiveness Matrix, 335
- Countermeasure Matrix, 156, 332–336
- Countermeasure Mitigation Values, 360
- Countermeasure Options Analysis Tool
- Countermeasure selection, 8, 55–56, 269
for assessment of threat, 255–256
consensus of decision makers, 317
cost-benefit analysis, 56
for criminal offenders, 315–316
deliverables, 38
for deterrence, 252–253
and exploits, 269
options and cost, 259
research, 52–53
threat action response, 257–258
- Countermeasures; *see also* Access control; Countermeasure selection; Detection baseline, 267–268
complaints about, 209–210
data gathering, 43
defining, 208–209
effectiveness metrics, 21, 307, 308–310, 316–317
- electronic, 26, 154–155
existing, 26, 43
functions, 308, 309
goals and functions chart, 262
goals of, 223–224, 250
hierarchy, 222
hi-tech elements, 218
implementation objectives, 250
legal challenges to, 209
lo-tech elements, 219
man-made, 154–155
natural, 26, 154
no-tech elements, 219–221
operational, 155
physical, 154
in Risk Analysis Report, 376–379
role of, 217–218
special, 225–226
supporting policies, 208–209, 221–222
- Countersurveillance, 225, 228
- CPTED program; *see* Crime prevention through environmental design
- Crime
data, 50
economic, 88, 133, 139, 326
incident likelihood estimates, 168–171
investigations, 227
organized, 165
prevention policies, 227–228
scenarios, 133
scenes, 304
workplace, 120
- Crime prevention through environmental design (CPTED) program, 55, 219, 261, 334
- Criminal organizations, 118
- Criminal records, 26, 50
- Criminals, 116, 165–166
economic, 118–120, 165, 314–315
information technology (IT), 165–166
lone, 120
petty, 123
sexual, 121
sophisticated, 119
street, 120
unsophisticated, 119
violent offender types, 120–122, 313–314
and vulnerability assessment, 141
- Crisis management
policy, 243, 244, 245
program, 95
- Critical infrastructure and key resources (CIKR)
protection, 241
regulations, 241
sectors, 21–22

- Critical Infrastructure Information Act, 240
- Critical thinking, 5, 67, 70, 81–84
 applicable concepts, 77
 applying to risk analysis, 80
 assumptions, 70, 75
 and biases, 69
 consequence examination, 76–77
 daily application, 79
 drawing inferences, 77
 elements, 71, 72, 73
 evidence of, 70–71
 goals of, 71–72
 implications, 76–77
 importance of, 68–70
 information gathering, 75–76
 intellectual traits, 78
 making recommendations, 72, 77–78
 and points of view, 74–75
 practicing, 79
 principles, 72–73
 and problem solving, 74, 81
 proficiency, 79
 pseudo-, 78
 purpose, 73–74
 resources on, 80
 skills, 7, 39, 53
- Criticalities, 20, 51
 assets to the mission, 26
 versus consequences, 101
 derivative, 102
 intrinsic, 102
 measure of, 101, 103
 and risk prioritization, 195
 scale for, 102–103
- Criticality analysis, 27
- Criticality/Consequence Matrix, 104–108
- Customers, 43, 92
- Cyberterrorism, 133
- D**
- Data classification, 54
- Data crunching, 53, 54
- Data gathering, 6
 assets by classification, 42–43
 business processes, 41–42
 existing countermeasures, 43
 failures, 40
 interviews, 40
 mission statement, 41
 primary data, 40
 types of data, 41
- Data input, 54
- Data mining, 53
- Decision Matrix, 9, 197, 317, 318
- Deliveries, 93, 229
- Department of Homeland Security (DHS)
 approaches to risk assessment, 19–20
 approved methodologies, 29–30
 approved software, 30
 current formula, 20
 grants from, 19, 20
 on information sharing, 241
 macro-risk approaches, 19–20
 on preparedness, 242
 on prevention, 241
 regulations from, 240–242
 tools, 29
- Deployable barriers, 296–297
- Design basis threat (DBT), 59, 124
- Detection; *see also* Detectors; Video detection systems
 assessment of threat, 255–256
 building perimeter, 278–279
 capacitance systems, 276
 confirmation, 255
 door position switches, 278–279
 of explosives, 281–284
 goals, 253–254
 interior space, 279–281
 intrusion, 254–255
 point detection, 281–284
 property perimeter, 276–278
 seismic systems, 276
 surveillance, 254
- Detectors
 fiber optic, 276
 ground-based radar, 278
 infrared, 277–278, 279
 laser light beams, 277–278
 leaky coax cable, 278
 microwave, 276–277
 photoelectric beam, 279
 pneumatic underground, 277
 thermal imaging, 281
 ultrasonic, 280–281
- Deterrence
 defining program, 298–302
 factors, 333
 goals, 252
 strategies, 252–253
- DHS; *see* Department of Homeland Security
- Diversion, 315
- Document theft, 315
- Duress alarms, 281
- Dyadem International Ltd., 57

E

- Economic crime, 88, 133, 139, 326
Economic Crimes Asset Target Value Matrix, 61, 169, 173
Economic Crimes Matrix, 185
Economic criminals, 118–120, 165, 314–315
Economic risks, 113
 resources, 114
Economic threats, 24
Embezzlement, 314–315
Emergency management; *see* Crisis management
Emergency security plans, 231
Emergency services
 liaison program, 302
 responders, 302
Employees
 background checks, 228
 business reputation characterization, 43
 disgruntled, 120–121
Employment regulations, 242
Enron, 328
Environment
 safe and secure, 261
 security hazards, 112
 surveys, 90–91
Environmental Liberation Front (ELF), 326
Equipment
 as assets, 43
 control policies, 229
 security hardware, 229
Escort systems, 226
Evidence gathering; *see also* Research
 at crime scene, 304
 defining the program, 304
 goals, 258
 for prosecution, 56, 345
 strategies, 258
 tools for, 345
 witness statements, 304
Explosive detection
 dogs, 282, 283
 electronics, 282, 283
 millimeter wave scanner, 282–283
 screening, 225
 undervehicle inspection, 283, 284, 312
 visual inspection, 282, 283
 X-rays, 281, 282

F

- Facilities
 commercial, 24
 critical infrastructure, 20

- existing, 152
guidelines, 20–22
new, 152

Facility characterization, 372
Federal Bureau of Investigation (FBI)
 local terrorism task force, 125
Federal Emergency Management Agency (FEMA) tools, 29
Fencing; *see* Barriers
Files, 86
 digital, 50
 paper, 43
Force Protection Exhibition and Demonstration (FPED), 118
Full-Scale Sandia Process, 31

G

- Gangs, 120
Garcia, Mary Lynn, 141, 322
Google, 46, 48
Google Maps, 91
Grenades, 311, 312
Guards; *see* Security officers
Guerrilla soldiers, 117–118
Guidelines, 207
Guiding principles, 208

H

- Hackers, 122, 327
Hazards
 likelihood information resources, 113–114
 natural, 112–113
 safety, 111–112
 security, 112
 versus threats, 111
Hazards Matrix, 86
Health Insurance Portability and Accountability Act, 240
HighBeam Research, 46
Hijacking, 312
HIPAA, 240
Historical data, 50, 113
Homeland Security Act, 22
Hostages, 312

I

- IEDs (Improvised Explosive Devices), 311
Incendiaries, 312
Incident reporting, 227
Infiltration scenarios, 310
Information security
 policy protection, 229
Information sharing, 241

- Information technology
 criminals, 165–166
 as proprietary information, 43
 security programs, 97, 218
- Information theft, 315
- Inspection systems, 281, 282, 283
- Integrated Security Systems Design* (Norman), 257
- Intelligence
 analysis, 80, 96
 commercial services, 301
 news connections, 302
 program, 95–96, 227, 300–301
 sources, 95–96, 301
- International Association for Counterterrorism and Security Professionals, 118
- Internet research, 46–48
- Interviews
 for asset categorization, 87–88
 data gathering, 40
 evidence gathering, 44–46
 preparation for, 44
- Invasion of privacy, 122–123, 327
- Investigations, 95, 227
 follow-up, 304
 program, 300
- J**
 Johnson & Johnson, 328
- K**
 Kahlid Sheikh Mohammed (KSM), 60, 142
 KSM-Asset Target Value for Terrorism Matrix, 60, 127
 KSM-Asset Target Value Model, 167–168
- L**
 Law enforcement liaison, 95, 227
 Lexis/Nexis, 46
 Lighting, 219, 297
 Likelihood; *see* Probability
 Loading docks, 228
 Lobby consoles, 288
 Locks, 219
 delayed egress, 295
 drop-bolt, 295
 electrified cylinder, 295
 electrified mortise, 294
 electrified panic hardware, 294
 and key control, 228
 magnetic, 294–295
- Los Angeles Police Department (LAPD), 122, 326
- Losses, 26, 51
 by asset, 189
 in Criticalities/Consequences Matrix, 59
 severity ranking, 28
- M**
 Macro-risk, 19
 Mail recipients, 229
 Mail rooms, 93, 228
 Management
 business reputation characterization, 43
 policy backing, 211
 priorities, 96, 196
 priority of security program, 96
 senior, 43
- Maritime Transportation Security Act (MTSA), 271
- Marriot Hotel, Pakistan, 124, 325
- Matrices
 Adversary/Means, 131, 133–137
 Asset/Attack, 127, 128, 129, 130
 Asset/Attack Matrix, 127, 128, 129, 130, 144–146
 Asset Target Value Matrices, 60, 184–186
 Asset Target Values, 60–62, 127
 Cost-Effectiveness Matrix, 353–355
 Criticality/Consequence, 104–108
 Decision Matrix, 9, 197, 317, 318
 KSM-Asset Target Value for Terrorism, 127
 spreadsheet instructions, 104–108
 Surveillance Opportunities, 150, 151
 Threat/Target Nexus Matrix, 146–147
 Vulnerability Detail Matrix, 157, 158
 Vulnerability Matrix, 156
 Weapons/Target Nexus, 147–148
- McAfee, 46
- Medical emergencies, 303
- Methodologies, 10–11, 20–21
 commercial software, 24–25
 costs, 23, 24
 DHS-approved, 29–30
 facility versus community, 31
 industry-specific, 30
 models, 23
 model scalability, 23, 24–25
 selection, 22, 31–32
 strengths and weaknesses, 31–32
- Microsoft Excel, 8, 37, 38
- Microsoft OneNote, 88
- Mission statements
 assets to, 26, 28
 data gathering, 41
 protecting, 28
- Models; *see* Methodologies

Moore, David A., 57
Moving shooters, 310–311
Muggers, 121

N

Nance, Malcolm W., 118, 126, 128
National Environmental Policy Act (NEPA), 240
National Fire Protection Association (NFPA)
Risk Assessment Checklist, 58
National Infrastructure Protection Plan
(NIPP), 22, 240
National Victim Center, 121
Natural countermeasures, 154
Natural hazards, 112–113
NEPA; *see* National Environmental Policy Act
Network attached storage (NAS), 290
Nongovernmental organizations (NGOs), 3,
41, 61, 96
Norman, Thomas L., 257
Nuclear facilities, 31, 32, 321

O

Office equipment, 43
Oil/gas/chemical sector, 23
Ordinary decent crime (ODC), 115, 124
Organization charts, 42, 92
Organized crime, 119

P

Pakistan suicide attack, 325
Palestinians, 116, 117
Parking
access control, 93, 228
lighting, 94
lot violence, 121
Patrol logs, 337
Patrols, 95, 227, 230, 299
People, as assets, 27
Perception, 81
Petty Crimes Matrix, 62
Photo ID badging, 95, 275, 288
Pocket Digital Light Meter, 50
Points of view
critical thinking, 74–75
understanding, 81
Policies, 206–207; *see also* Policy development
access control, 228
asset protection, 229
for authorities and responsibilities,
224–225
baseline, 245
benefits of having, 210–211
and business culture, 211
and business productivity, 211
circumvention, 211
compliance, 206, 209
control factors, 211
crime prevention, 227–228
emergency security plans, 231
enforceability, 210, 211
goals of, 222–223
individual responsibilities, 229
maintenance, 225
and procedures, 207–208
for protection of life, 225
role of, 217
statements, 245
in support of countermeasures, 208–210,
221–222
theory, 215–217
violations, 227
for VIPs, 230–231
Policy development
basic policies, 238–239, 245
change triggers, 235–236
impact statements, 236–237
implementation guidelines, 239–240, 245
nonregulatory-driven, 242–244
process steps, 235
regulatory-driven, 240–242
request review, 236
requirements, 238
review process, 237–238
Political risks, 113, 114
Position paper, 208
Posts, 95, 227, 230, 299
PowerPoint presentations, 368, 382
Preparedness, 222, 242
Presentations, 382
and business culture, 369
handouts, 368, 382
key elements, 368
and personal biases, 369–371
preparation, 369–371
Priorities; *see* Risk prioritization
Probability, 20, 161–162
assessment, 27
of criminal incidents, 168–171
definition, 25
economic crime, 169
factors, 180, 181–183
historical data, 26
petty crimes, 171
range of threat actors, 163–166
sources, 113–114
terrorism estimates, 162–163, 166–167
using criminal statistics, 168–169

- variables, 26
 violent crime (nonterrorism), 169–171
- Probability Summary Matrix, 186, 187
- Problem solving
 and conflict, 81
 critical thinking, 74, 81
 and policies, 206
- Problems
 and change, 81
 perception, 81
 root of, 81
- Procedures, 207–208
 changes in, 237
- Procedures for Handling Protected Critical Infrastructure Information Act, 240
- Property
 access routes, 91, 92
 as assets, 27, 42–43
 building type, 92
 control policies, 229
 fence-lines, 91
 lost and found policy, 229
 perimeters, 91
 surveys, 91–92
- Proprietary information, 27, 43, 86, 92–93
- Protection of Assets Manual* (ASIS), 52
- Pseudo-critical thinking, 78
- Purdue University’s CORE, 46
- Q**
- Qualitative analysis, 7, 54–55
 converting quantitative data, 55
 vulnerability assessment, 155, 157
- Qualitative text, 37
- Qualitative versus quantitative, 5–6, 25
- Quantitative analysis, 7, 37, 53–54
- Questia, 46
- R**
- Radio frequency (RF) devices, 270
- RAM (Risk Assessment Methodology)
 DHS-approved, 30
 formula, 28
 model, 23
 security effectiveness, 321–323
 versions by industry, 28, 29
 versus API/NPRA, 176–179
- RAMCAP framework, 29, 32
- RAMCAP Plus, 57–58
- REAPS technologies, 257
- Records
 as proprietary information, 43
 research, 49
 vital, 43
- Regulations, 29–30
- Religious extremists, 117
- Report writing, 56
 skills, 8, 39
 software, 57–58
 tools, 56–57
- Reports; *see also* Presentations; Risk Analysis Report
 comprehensive, 367
 and critical thinking, 70–71
 deliverables, 38
 graphics, 368
 incident, 227
 post and patrol, 227
 recommendations, 63, 72–73, 78, 355
- Research, 6
 on assets, 90
 bibliography building, 51–52
 on countermeasures, 52–53
 of criticalities, 51
 for critical thinking, 75–76
 historical data, 50
 Internet, 46–48
 interviews, 44–46
 for prosecution, 56, 345
 records, 49
 surveys, 49–50
 telephone, 49
- Resources
 antiterrorism, 118
 on critical thinking, 80
 hazard likelihood, 113–114
- Response
 communications, 302
 and consequences, 334
 defining the program, 302–304
 degree of, 334
 goals, 257
 to nonevents, 299
 regulations, 242
 strategies, 257–258
 training requirements, 303
- Revolving doors, 295
- Riots, 122, 326
- Risk Analysis Report, 367; *see also* Presentations
 assessment process, 372
 attachments, 380, 382
 components, 14, 17
 countermeasure budget presentation, 382
 countermeasures, 376–379
 executive summary, 371
 facility characterization, 372

- footnotes, 380
glossary, 380
index, 380
introduction, 371–372
risk register, 379, 381
tables, 380
threat assessment, 373–374
vulnerability assessment, 374–376
- Risk assessment, 17, 27; *see also* Methodologies
 codes and standards, 29–20
 components, 20
 deliverables, 38
 objective, 175–177
 phases, 38
 practice, 13–15
 process, 178–180, 181–183
 science of, 4
 skills, 6–8, 18, 39–40
 steps, 27–29
 theory, 12–13
 tools, 8, 15–16, 40
- Risk Assessment Checklist (NFPA), 58
- Risk Calculation Matrix, 189–190
- Risk descriptions, 358
- Risk estimate, 15
- Risk factors, 21
- Risk formula
 additive, 20
 basic, 25, 161
 calculation steps, 189
 displaying results, 177–178
 mathematical result versus relationship, 175
 sorted results, 198
 unranked results, 190
 used by Homeland Security, 20, 161
 variables, 26
 weighted variables, 20
- Risk management, 17, 27
- Risk mitigation, 11
- Risk prioritization, 17, 27, 194–195
 best practices, 197–199
 and communication, 196–197
 by consequences, 195
 by cost, 195–196
 criteria, 193
 by criticality, 195
 by formula, 194
 by probability, 195
- Risk register, 14, 379, 381
- RiskWatch, 58
- Robbery, 121, 315
- S
Saboteurs, 122–123, 326
SAFETY; *see* Support Anti-Terrorism by Fostering Effective Technologies Act
- Safety hazards, 111–112
- Sandia Adversary Sequence Diagram, 37
- Sandia model; *see* RAM (Risk Assessment Methodology)
- Sandia National Laboratories, 23, 29, 31
- Sandia software tools, 30
- Sarbanes-Oxley (SOX) Act of 2002, 240–241
- Security awareness program, 227, 299–300
- Security checkpoints, 210, 251
- Security chief, 96, 224
- Security controls
 policies, 211
 technical versus staff, 211
- Security effectiveness
 commercial model, 324
 information needed, 328–329
 metrics for, 330
 theory, 321
 users of metrics, 323–324
 using Sandia model, 321–323
- Security events
 assessing, 224
 detect, 223
 evidence of, 224
 logs, 336–337
 reporting and follow-up, 223
 response to, 224
- Security hazards, 112
- Security Industry Buyers Guide* (ASIS), 52
- Security intelligence program, 227
- Security management
 offices, 288
 qualifications, 94
 responsibilities, 224
 surveying, 94
 training, 94–95
- Security officers, 302–303
 arming, 223, 303
 challenges by users, 209–210
 contracting, 303
 counseling role, 223
 and medical emergencies, 303
 performance evaluation, 211
 policies for, 229–230
 professionalism, 222
 training, 94–95, 211, 230
- Security patrols, 95, 227, 230, 299
- Security posts, 95, 227, 230, 299
- Security programs; *see also* Crisis management; Policies

- auditing, 222
 - awareness, 95
 - charter, 224
 - development, 205
 - disaster recovery, 95
 - information technology, 97
 - intelligence, 95–96
 - investigations, 95
 - law enforcement liaison, 95
 - metrics, 210
 - patrols, 95
 - posts, 95
 - priority to upper management, 96
 - as proprietary information, 43
 - recommendations summary board, 355
 - role of policies, 217
 - surveys, 93–97
 - Security systems
 - antennas, 294
 - archiving schemes, 290–291
 - archiving technologies, 288–290
 - digital infrastructures, 292–294
 - infrastructures, 291–294
 - licensed versus unlicensed, 293
 - Security zones, 94
 - Sexual assault, 121
 - Shipping/receiving docks, 93, 229
 - Shooters, 310–311
 - Shoplifting, 315
 - Signage, 219, 297–298
 - Snipers, 311
 - Software
 - report writing, 57–58
 - Software tools
 - affordability, 58–59
 - commercially available, 24–25
 - DHS-approved, 30
 - Sorted Risk Matrix, 63
 - SOX; *see* Sarbanes-Oxley Act of 2002
 - Space planning, 14
 - Spies, 122
 - Spreadsheets; *see* Matrices
 - Stakeholders, 22–24, 196–197, 350
 - Stalkers, 121–122
 - Standards, 207
 - Standoff weapons, 311
 - Stationary shooters, 311
 - Statistics
 - crime, 49, 168, 183
 - descriptive, 113
 - of historical data, 60, 113
 - Storage area network (SAN), 290
 - Subject matter expert (SME) analysis, 231, 237–238
 - Subversives, 116, 122–123, 326
 - Subversives and Petty Crimes Matrix, 61, 186
 - Suicide bombers, 132, 311
 - Support Anti-Terrorism by Fostering Effective Technologies (SAFETY Act), 240
 - Surveillance
 - detection, 254
 - opportunities, 26, 150, 188
 - Surveillance Matrix, 62, 150, 151, 188
 - Surveys, 49–50
 - deliverables, 38
 - environmental context, 90–91
 - note taking, 49
 - occupancy, 91
 - organizational, 92–93
 - photos/video, 49–50
 - political factors, 91
 - property context, 91–92
 - security context, 93–97
 - social factors, 91
 - time of day/night, 50
 - for vulnerabilities, 152–153
 - SVA (Security Vulnerability Assessment)
 - method, 23
 - SVA-Pro, 57
 - Symbianese Liberation Army (SLA), 117
- T**
- Target selection, 142
 - and area of operation, 182
 - CARVER method, 32, 60, 166
 - information, 126, 182
 - KSM-Asset Target Value Model, 167–168
 - terrorism, 26, 127, 142–143, 181
 - tool for Special Forces, 32, 166
 - Telephone research, 49
 - Templates, 37–38
 - Terrorism; *see also* Target selection
 - and asset target value estimates, 166–168
 - Asset Target Value Matrices, 60
 - attacks, 325
 - attack scenarios, 132–133, 182
 - objectives, 313
 - probability estimates, 162–163
 - strategies, 143
 - threat, 114–115
 - and vulnerability assessment, 141, 142
 - “Terrorism Awareness and Education” (Welch), 126
 - Terrorist Recognition Handbook* (Nance), 118, 126, 128
 - Terrorists
 - class descriptions, 116–118
 - classes of, 115

- government-trained, 116–117
organizations, 142
radical revolutionary, 117
- Theft, 88
of information, 315
internal, 314
risk, 162
- Threat actors, 26, 28; *see also* Criminals; Terrorists
characteristics, 125
current active list, 114
identification, 124–125
motivation, 132
professionalism, 131, 133
range of, 163
types, 115–116, 163–166
workplace crimes, 120–122
- Threat assessment, 14, 28, 111, 373–374
entry methods, 133
steps, 124–128
tools for, 128–129
weapons access, 132
- Threat identification, 13, 27, 28, 181
- Threat/Target Nexus Matrix, 146–147
- Threats
and countermeasure functions, 309
definition, 25, 115
as formula variable, 20, 25
likelihood, 26
scenarios, 132–133
types, 26
variables, 26
versus hazards, 111–113
- Tools, 8, 18; *see also* Matrices; Software
assets and consequences, 59
for listing assets, 97–98
probability assessment, 59–62
for risk analysis, 63
vulnerability assessment, 62, 187–188
- Total Mitigation Estimate (TME), 335
- Training
continuing education, 94
costs, 24
department managers, 96
in intelligence analysis, 96
in investigations, 95
need, 25
and policies, 211
in response, 303
security management, 94–95
security officers, 94–95, 211, 230
- Transnational criminal organizations, 118
- Transportation Worker Identification Credential (TWIC) cards, 271
- Travel security, 241
- Turnstiles, 295–296
- Tylenol tampering, 328
- U**
- University of California, Irvine, 46
- Unranked Risk Results, 190
- Unsorted Risk Matrix, 63
- U.S. Coast Guard, 22
- U.S. Department of Defense, 60
- U.S. Department of Health and Human Services, 240
- U.S. Department of Homeland Security (DHS),
see Department of Homeland Security
- V**
- Vandals, 123, 328
- VBIEDs (Vehicle-Borne Improvised Explosive Devices), 311, 312
- Vehicle gates, 296
- Vehicles
access, 93
as assets, 43
parking control, 93, 228
- Vendors, 43, 94
- Video detection systems
analog, 286
day/night imagers, 286
digital, 286
digital fish-eye PTZ, 286–287
fixed video cameras, 284–285
intelligent video software, 287–288
pan/tilt/zoom (PTZ) cameras, 285
pinhole cameras, 285
short-wave infrared, 287
thermal imaging, 287
visible light cameras, 284–285
- Video surveillance, 218
archiving, 304
- Violations
categorizing, 227
handling of, 238, 245
of policy, 227
safety, 112, 227
spotting, 337
- Violent crime
probability, 169–171
in workplaces, 120–121
- Violent Crimes Matrix, 61, 185
- VIP protection
circulation paths, 146–147
policies, 230–231
- Visitors, 94, 121

- Visual inspections, 281, 282, 283
 V^2 Matrix, 63, 180, 198, 199
Voice communication systems, 43
Vulnerabilities, 17
 in formulas, 20, 26
 intrinsic, 153–154
 spotting, 337
 variables, 26
Vulnerability assessment, 27, 186–187
 accessibility, 153
 calculation spreadsheet, 155
 considerations, 186–187
 defining scenarios, 142–144
 detail spreadsheet, 157, 158
 effect of man-made countermeasures, 154–155
 effect of natural countermeasures, 154
 for existing facilities, 152
 identifying intrinsic vulnerabilities, 153–154
 model, 141, 142
 for new facilities, 152
 qualitative analysis, 155, 156
 and qualitative analysis, 155, 157
 quantitative analysis, 153, 188
 in Risk Analysis Report, 374–376
 steps, 144
 survey points, 152–153
 tools, 62, 187–188
- Vulnerability Assessment of Physical Protection Systems* (Garcia), 322
Vulnerability/Countermeasure Matrix, 332–336
Vulnerability Detail Matrix, 157, 158
Vulnerability Matrix, 62, 156, 188
- W**
- Watercraft, 312
- Weapons
- access to, 132
 - categories of, 132
 - policies, 225, 229
 - screening, 225
 - standoff, 311
 - in the workplace, 225, 229
- Weapons/Target Nexus Matrix, 147–148
- Welch, Alicia L., 126
- Wiegand swipe readers, 272
- Wiegand wire cards, 269–270
- Witness statements, 304
- Workplace
- illegal substances, 229
 - personal security, 229
 - screening, 225
 - threat actors, 116, 120
 - violence, 120, 326
 - weapons in, 225, 229
- World News Connection (WNC), 302
- World Trade Center, 325
- World Trade Organization, 122

Risk Analysis and Security Countermeasure Selection

Thomas L. Norman, CPP/PSP/CSC

When properly conducted, risk analysis enlightens, informs, and illuminates, helping management organize their thinking into properly prioritized, cost-effective action. Poor analysis, on the other hand, usually results in vague programs with no clear direction and no metrics for measurement. Although there is plenty of information on risk analysis, it is rare to find a book that explains this highly complex subject with such startling clarity. Very few, if any, focus on the art of critical thinking and how to best apply it to the task of risk analysis.

The first comprehensive resource to explain how to evaluate the appropriateness of countermeasures, from a cost-effectiveness perspective, **Risk Analysis and Security Countermeasure Selection** details the entire risk analysis process in language that is easy to understand. It guides readers from basic principles to complex processes in a step-by-step fashion — evaluating Department of Homeland Security (DHS)-approved risk assessment methods, including CARVER, API/NPRA, RAMCAP, and various Sandia methodologies.

Using numerous case illustrations, the text clearly explains the five core principles of the risk analysis life cycle. It also supplies readers with a completely adaptable graphic risk analysis tool that is simple to use, can be applied in public or private industries, and works with all DHS-approved methods. This reader-friendly guide provides the tools and insight needed to effectively analyze risks and secure facilities in a broad range of industries, including DHS-designated critical infrastructure in the chemical, transportation, energy, telecommunications, and public health sectors.



CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

AU7870

ISBN: 978-1-4200-7870-1



www.crcpress.com