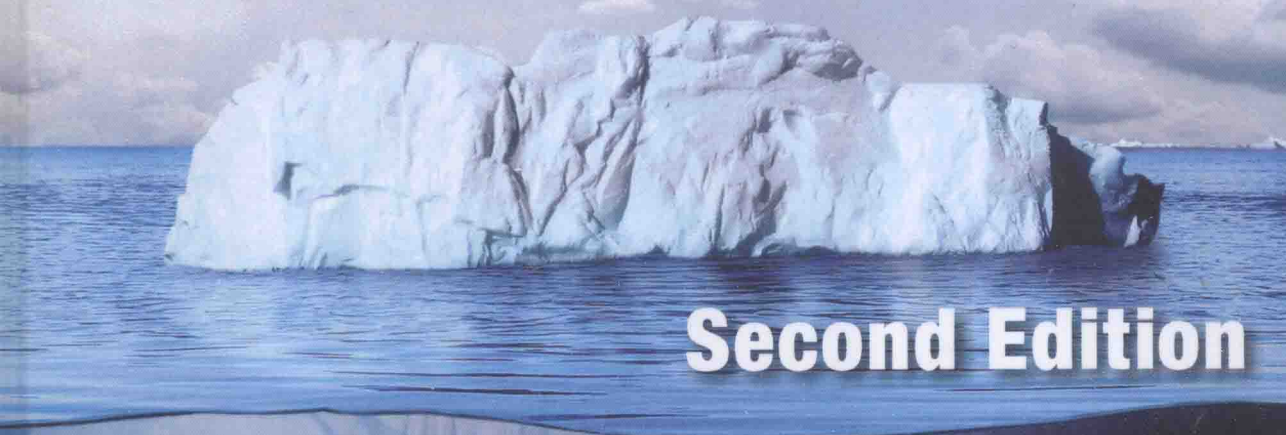

Second Edition

Risk Analysis and Security Countermeasure Selection

Thomas L. Norman
CPP/PSP/CSC

CRC Press
Taylor & Francis Group

Second Edition

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

Printed on acid-free paper
Version Date: 20150514

International Standard Book Number-13: 978-1-4822-4419-9 (Hardback)

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

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

Second Edition

Risk Analysis and Security Countermeasure Selection

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, the 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 ten attackers used simple methods, tactics, and weapons (a moving shooter attack) to kill and injure many 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.

Based on statements by Ajmal Amir, the only terrorist who was captured alive, this horrible crime was spawned by Lashkar-e-Taiba, a foreign terrorist organization operating from within Pakistan, with training and planning help from Al-Qaeda. 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; to undermine the existing Indian regime; to destabilize relations between India and Pakistan; to encourage the election of more militant Indian parliamentarians with an eye toward further destabilizing Indo-Pakistan relations; to cause India to put pressure on the moderate Pakistani regime, thus undermining their popularity within Pakistan and leading toward regime change there; 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 to create chaos and possibly anarchy inside Pakistan in order to effect regime change and thus pave the way for a Taliban-like regime that would gain access to nuclear weapons for 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, is being opposed by a

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

I had completed a risk assessment for a major Indian firm only 2 months earlier, which 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, making them easy targets for rapid action forces. These should be coupled with off-site command and control capabilities for any Tier 1 terrorist target; these move 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 provides 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. This is especially true when many lives depend on the quality of their ill-conceived and hopelessly inadequate recommendations based solely on 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.

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 and 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. Governments have always been aware of security, as they 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 refreshing, startling, and concerning all at the same time.

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's 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 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 models (including the Central Intelligence Agency model) promoted by the U.S. Armed Forces, the U.S. Department of State, the Department of Justice, the Federal Emergency Management Agency, and the Department of Homeland Security (DHS), and models created by Sandia National Laboratories, 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 understand 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 these data and present them 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 unique

* There is one book on "vulnerability" that does teach analysis: *Vulnerability Assessment of Physical Protection Systems* by Mary Lynn Garcia[1]. Mary Lynn Garcia is a light in the wilderness.

program for each. It is the commoditization of data services to the best advantage for stakeholders and 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 DHS. 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 terminals, to retail malls, to airports, to hotels, to office towers, and 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 from 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 also 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 the 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.

REFERENCE

1. Garcia, M. L. 2005. *Vulnerability Assessment of Physical Protection Systems.* Butterworth-Heinemann, Oxford.

Acknowledgments

I am deeply thankful to my very lovely wife, Dr. Nadia Norman, who has retired from a lifelong career in medicine, and who endured endless hours of my absence while I completed the second edition of this book.

I am thankful to my adopted home of Beirut, Lebanon, and my wonderful business associates, Cheikh Nabil el Khazen and Mr. Adel Mardelli, for 15 years of constant encouragement and support, especially for their support for my efforts toward perfection in the craft of risk analysis and security systems design.

I am also grateful to my business associates Mr. Benjamin Butchko, CPP; Mr. Charles Goslin, CPP, CISSP; Ms. Megan Bradley, and Mr. Michael Newsome (Butchko, Inc.), who I work with enjoyably every day in Houston, Texas.

Both teams, in Beirut and Houston, are dream teams in terms of qualifications, consideration, professionalism, and kindness.

I am grateful for the review and guiding comments on the manuscript by Ben Butchko and Charles Goslin. Additional thanks to Mr. Malcom Nance, Mr. David Moore, CPP (Acutech Consulting Group); Mr. Ross Johnson, CPP (ASIS International); and Ms. Mary Lynn Garcia (Sandia National Labs) for their excellent and groundbreaking work in this subject field.

I am grateful to Mr. Mark Listewnick and Ms. Jennifer Abbott, from Taylor & Francis Group (CRC Press), for their constant encouragement and patience. Thanks to Mark for seeking me out to write the first edition and to Jennifer who guided me flawlessly through the second edition.

I am endlessly grateful to ASIS International, the Petroleum, Chemical and Extraction Technologies (PCE) Council, and Mr. Ross Johnson, CPP (who chairs that 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 grateful to the many consultants and security practitioners who have picked my brain and encouraged me to write this book about risk analysis, and to 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 thankful 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.

Author

Thomas L. Norman, CPP/PSP/CSC, is an internationally acclaimed security risk management consultant with experience in the United States, the Middle East, Europe, Africa, and Asia. As the author of the industry reference manual on integrated security system design, and with more than 35 years of experience in design, construction management, and commissioning, Mr. Norman is one of the industry's leading design consultants, worldwide. Mr. Norman has developed formulas and detailed processes that are used by the entire security industry to calculate the effectiveness of security programs and security program elements and also overall security program cost-effectiveness. Mr. Norman has authored five books and coauthored two others (for the American Institute of Architects; *Security Planning and Design: A Guide for Architects and Building Owners*; *Integrated Security Systems Design*, first and second editions; *Risk Analysis and Security Countermeasures Selection*, first and second editions; the latest ASIS International Physical Security Professional (PSP) certification study materials; and *Electronic Access Control*. Mr. Norman's works have been quoted and referenced by organizations such as the Cato Institute, National Broadcasting Company (NBC), and Security Management.

Contents

Preface xxvii

Acknowledgments xxxi

Author xxxiii

SECTION I RISK ANALYSIS

Chapter 1 Risk Analysis: The Basis for Appropriate and Economical Countermeasures 3

For Students Using This Book in an Academic Environment 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

References 18

Q&A 18

Questions 18

Answers 20

Chapter 2 Risk Analysis Basics and DHS-Approved Risk Analysis Methods 21

Introduction 21

U.S. Department of Homeland Security Concerns 21

Risk Analysis for Facilities and Structures 22

Many Interested Stakeholders and Agendas 23

Commercially Available Software Tools 26
Risk Analysis Basics 26
Risk Assessment Steps 28
DHS-Approved Risk Assessment Methodologies 30
Which Methodology to Use? 32
Community versus Facility Methodologies 32
Strengths and Weaknesses of Major Methodologies 32
CFATS Information 34
CSAT Top Screen 34
CSAT Security Vulnerability Assessment (SVA) 35
Summary 35
Introduction 35
Risk Analysis for Facilities and Structures 35
Many Interested Stakeholders and Agendas 36
Commercially Available Software Tools 36
Risk Analysis Basics 36
Risk Assessment Steps 37
Which Methodology to Use? 37
Strengths and Weaknesses of Major Methodologies 37
References 38
Q&A 39
Questions 39
Answers 40
Chapter 3 Risk Analysis Skills and Tools 41
Introduction 41
Security Risk Analysis Skills 43
Security Risk Analysis Tools 44
Skill #1: Gathering Data 44
Interviews 45
Types of Data Required 45
Get the Organization's Mission Statement 45
Understand the Organization's Programs (Business Units) 46
Assets by Classification 46
Existing Countermeasures 48
Skill #2: Research and Evidence Gathering 48
Interviews 48

Internet Research 51
Telephone Research 53
Records Research 53
Surveys 53
Asset Classifications 54
Historical Data Relating to Security Events 54
Criticalities and Consequences Assessment 55
Bibliography Building 56
Countermeasures Research 56
Skill #3: Critical Thinking in the Risk Analysis Process 57
Skill #4: Quantitative Analysis 57
Skill #5: Qualitative Analysis 58
Converting Quantitative Data into Qualitative Data 59
Skill #6: Countermeasure Selection 59
Countermeasure Selection 59
Cost-Benefit Analysis 60
Skill #7: Report Writing 60
Tools 61
Commercially Available Software Tools 61
Lesser Software Tools 62
Affordable Tools Examples 62
Summary 67
Introduction 67
Tools 68
References 69
Q&A 69
Questions 69
Answers 70
Chapter 4 Critical Thinking and the Risk Analysis Process 71
Introduction 71
Overview of Critical Thinking 71
Importance of Critical Thinking 71
Analysis Requires Critical Thinking 73
The Eight Elements That Make Up the Thinking Process 75
The Concepts, Goals, Principles, and Elements of Critical Thinking 76
Critical Thinking Concepts and Goals 76

Principles 76
Elements of Critical Thinking 77
Purpose 77
The Question at Issue: Most Thinking Is about Problem Solving 78
Understand Our Own and Others' Points of View 78
Gather Assumptions 79
Gather Information 79
Examine the Implications and Possible Consequences Related to the Issue 80
Determine What Concepts, Theories, Definitions, Axioms, Laws, Principles and/or Models Are Applicable to the Issue 81
Draw Interpretations, Inferences, and Conclusions from the Data; Validate the Data; and Formulate Recommendations Based on the Results 81
Pseudocritical Thinking 82
Intellectual Traits 82
Importance of Integrating Critical Thinking into Everyday Thinking 82
Applying Critical Thinking to Risk Analysis 83
Inductive versus Deductive Reasoning 84
The Analysis Process 85
More about Critical Thinking 85
The Root of Problems 85
Summary 86
References 88
Q&A 88
Questions 88
Answers 90

Chapter 5 Asset Characterization and Identification 91
Introduction 91
Theory 91
Practice 91
Asset List 91
Asset Categorization 92
People 92
Property 92
Proprietary Information 93
Business Reputation 93
Interviews 93

Facility and Asset List 95
Research 97
Surveys 97
Tools 103
Summary 105
Theory 105
Practice 105
Facility and Asset List 106
Tools 106
Reference 106
Q&A 107
Questions 107
Answers 108

Chapter 6 Criticality and Consequence Analysis 109
Introduction 109
Twofold Approach 109
Criticality versus Consequence 109
Criticality 110
Visualization 111
Consequence Analysis 112
Building Your Own Criticality/Consequences Matrix 113
Criticality/Consequence Matrix Instructions 113
Summary 117
Criticality 118
Consequence Analysis 118
Q&A 118
Questions 118
Answers 120

Chapter 7 Threat Analysis 121
Introduction 121
Theory 121
Threats versus Hazards 121
All-Hazards Risk Analysis 124
Terrorists 126
Economic Criminals 128
Nonterrorist Violent Workplace Criminals 129

Subversives 131
Petty Criminals 132
Design Basis Threat 132
Practice 133
Tools 136
Adversary/Means Matrix 137
Purpose 137
Functions 137
Attributes 137
Example 138
Predictive Threat Assessment 145
Inductive versus Deductive Reasoning 147
Deductive Reasoning 147
Inductive Reasoning 147
Inductive Context 148
Predictive Threat Analysis 148
Predictive Risk Example 148
Summary 149
Threats versus Hazards 149
Design Basis Threat 150
Practice 150
Tools 151
Predictive Threat Assessment 151
References 151
Q&A 153
Questions 153
Answers 154

Chapter 8 Assessing Vulnerability 155
Introduction 155
Review of Vulnerability Assessment Model 156
Define Scenarios and Evaluate Specific Consequences 156
Asset/Attack Matrix 159
Threat/Target Nexus Matrix 159
Weapons/Target Nexus Matrix 162
Adversary Sequence Diagrams (ASD) and Path Analysis 164
Surveillance Opportunities Matrix 164