CONTENTS

CHAPTER 1 *INTRODUCTION TO SECURITY RISK ASSESSMENT AND MANAGEMENT* 1

Introduction 1
Business Definition 1
Security Versus Risk 2
Framework for Risk Management 2
Value at Risk 5
Calculation of Risk 6
Risk Assessment Versus Risk Management 6
Risk Management Plans 8
Threat Scenarios 9
Statistics and Mathematics 10
Pairing Vulnerability and Threat Data 11
Setting Priorities 13
Other Definitions of Risk Assessment 14
Business Definition for Risk Assessment 14
Broad Definition for Risk Assessment 15
Quantitative Risk Assessment 15
Qualitative Risk Assessment 15
  Threats 15
  Vulnerabilities 15
Countermeasures for Vulnerabilities 16
  The D's of security systems 16
Sample Threat Scenario No. 1 18
  Background 18
Sample Threat Scenario No. 2 23
  Background 23

CHAPTER 2 *RISK ASSESSMENT BASICS* 29

Street Calculus and Perceived Risk 29
  Street Calculus 29
Security Risk Assessment Structure 32
Value at Risk 32
Sandia Laboratory's Risk Assessment Analysis 34
Annualized Cost Analysis of Risk 35
Scenario-Driven Cost Risk Analysis 36
  Real-world example 37

Model-Based Risk Analysis 38
MBRA example case 39
Risk Management by Fault Tree Methods and Risk-Informed Decision Management 39
Fault tree analysis 39
RIDM 42

CHAPTER 3 *ASSESSING TYPES OF ATTACKS AND THREATS WITH DATA SOURCES* 62

Weapons 62
AK-47 62
M16 62
Sniper rifles 63
Muzzle Energies for Various Cartridges 63
Rifle Grenades 63
Rocket-Propelled Grenades and Mortars 64
Explosive Energies 65
Impact of explosives 66
Other Types of Incidents and Accidents 68

CHAPTER 4 *EVALUATING A COMPANY'S PROTECTIVE SYSTEMS* 70

Surveys and Assessments 70
Site Security Assessments 71
Checklists 71
Cybersecurity checklist 71
Lighting 72
Perimeter Barriers: Design Notes and Comments 74
CCTV 79
Windows and Doors 81

CHAPTER 5 *PORT SECURITY* 82

Ranking Threats 82
Natural threats 82
Man-made/accidental threats 82
Intentional acts—delivery vectors 83
Weapon threats 83
Levels of Port Security 83
Security response plans 84
Recommended procedures 84
Identification Procedures for Personnel Screening 85
Employees 85
Vendors/contractors/vessel pilots 85
Truck drivers/passengers 85
Visitors (all personnel not falling into other categories) 86
Government employees 86
Vessel personnel access through a facility 86
Search requirements 86
Acceptable identification 87
Access control 87
Vessel Arrival and Security Procedures While Moored 87

Internal Security 88
Vehicle control 88
Rail security 88
Key/ID/access card control 88
Computer security 89
Security rounds 89
Perimeter Security and Restricted Areas 89
Barriers 89
Fencing 89
Lighting 90
Security Alarms/Video Surveillance/Communications Systems 90
Alarms 90
Video surveillance 90
Communications systems 91
Training and Security Awareness 91
Floating Barriers 91

CHAPTER 6 *BASICS OF CYBERSECURITY* 93

Communications Life Cycle 93
Some Solutions to the Problem of Cybercrime 94
General recommendations 94
Communications Security 96
Communications as Transactions 96
Telephone System Security 96
Radio Communications 97
Digital Communications 97
Cybersecurity 98
Vulnerability assessment 98
Unknowns and alternatives 99
How to Perform the Vulnerability Assessment 99
Critical success factors 99
Optimum assessment team size 101
Communications Procedure Design: Hints and Helps 101
Benefits: Identified 102
Example 102
Cyber Threat Matrix: Categories of Loss and Frequency 103
Setting up Internet Security 104
External versus internal testing 105
Security focus 105
Browser and domain security 105
Data encryption 106
Cybersecurity Tools 107

CHAPTER 7 *SCENARIO PLANNING AND ANALYSES* 109

Introduction 109
FTA, Markov Chains, and Monte Carlo Methods 110
Fuzzy fault trees 111
Markov chains and Bayesian analysis 111

Other Complimentary Techniques 112
Fishbone (Ishikawa) diagrams 112
Pareto charts 114
Sample of Initial Analysis 114
FMEA 119
DHS Analysis and Plans 120
Bow-Tie Analysis 124
Example 125
Hazops and Process Safety Management 127
Process safety information: General 127
PHA and HAZOPS 128
ALOHA, CAMEO, and Security Planning Tools 129
The Colored Books 133
Generic Guideline for the Calculation of Risk Inherent in the Carriage of Dangerous Goods by Rail 133
The Orange Book: Management of Risk—Principles and Concepts 133
The Green Book: Methods for the Determination of Possible Damage to People and Objects Resulting from Release of Hazardous Materials, CPR-16E 135
The Yellow Book: Methods for the Calculation of Physical Effects due to the Releases of Hazardous Materials (Liquids and Gases), CPR-14E 137
The Red Book: Methods for Determining and Processing Probabilities, CPR-12 137
The Purple Book: Guidelines for Quantitative Risk Assessment, PGS 3 137
Sample outline for emergency response 141

CHAPTER 8 *SECURITY SYSTEM DESIGN AND IMPLEMENTATION: PRACTICAL NOTES* 148

Security Threat-Level Factors 148
Considered Factors 148
Vehicle bombs 149
Standoff weapons 151
Minimum standoff distances 151
Security System Design 153
Perimeter barriers 154
Active vehicle barriers 154
Entry roadways 155
Entry control stations 156
Reinforcement of buildings and infrastructure 156
Windows 156
Security system lighting 157
Lighting system design 157
Electronic Security Systems Design 157
Alarm configurations and design 158
Access control 159
Employee screening 160
Visitor identification and control 160
Packages, personnel, and vehicle control 161
Lock and key systems 161
Security forces 162
Cargo security 162
Port security systems 163

Review and Assessment of Engineering Design and Implementation 163
Auditing and evaluation 163
Risk assessment team 164
Blank sheet approach to auditing and evaluation 165
Business approach to auditing and evaluation 165
Benchmarking 166
How to evaluate a physical security system? 167
Security systems audits 167
What to review? 168
Implementation of risk assessment 174
SQUARE: Prioritizing security requirements 177
Security monitoring and enforcement 179
Security awareness program 180
Proposed future training requirements 180
Security management 180
The differing roles of the security department 181
Stress management techniques 181
Security management techniques 184
Conclusion 186

Appendix I 187
Appendix II 196
Index 000