



Assessing Terrorism Related Risk

Seminar Description & Outline

Copyright 2004 by the S2 Safety & Intelligence Institute
S2 Safety & Intelligence Institute, 1261 South Missouri Ave, Clearwater, FL 33756
Tel. (727) 461-0066 / Fax (727) 449-1269 / WEB: <http://www.s2institute.com>

Class Details

Description: The Assessing Terrorism Related Risk workshop is designed to aid security and public safety planners in developing an effective methodology for evaluating terrorism related risk. This program introduces the various types of terrorism related risk and walks the students through the process of conducting a qualitative risk assessment. Exercises are used to aid the students in understanding the process of risk assessment and how to apply risk management principles in anti-terrorism and security planning.

In addition to exploring risk management principles, students are introduced to unique challenges and solutions for evaluating vulnerability to specific types of terrorist attack scenarios. Some of the vulnerability assessment methods explored during this portion of the program include quantitative performance-based physical security assessment, qualitative blast vulnerability assessment, and analysis of vehicle barrier design and performance.

Audience: Security Managers, Facility Managers, Military Force Protection Officers, Emergency Planners, and City/Gov't Planning Officials

Restrictions: Verified Security, Law Enforcement, and Government Employees Only.

CEU/In-Service Training Credit: CHS-certified practitioners are eligible for 16-hours of CEUs through the American College of Forensic Examiners.

Presentation Time: The S2 Assessing Terrorism Related Risk workshop is presented in two 8-hour days. Classes typically start at 9:00AM and finish by 5:00PM.

Class Outline

DAY ONE

1. Principles of Risk Management

- 1.1 What is Risk?
 - 1.1.1 Risk Definitions
 - 1.1.2 Risk Elements

- 1.1.3 Risk Expressions
- 1.2 Fundamental Risk Management Concepts
- 1.3 Risk Assessment Approaches
 - 1.3.1 Quantitative Risk Assessment
 - 1.3.2 Qualitative Risk Assessment
- 1.4 Basic Qualitative Risk Assessment Model
- 1.5 Example of Risk Management Principles: Driving to Work

2. Characteristics of Terrorism Related Risk

- 2.1 Definition
- 2.2 Ideological Motives
- 2.3 Strategic Objectives of Terrorist Groups
- 2.4 Types of Terrorist Targets
- 2.5 Target Selection Criteria
 - 2.5.1 *Exercise 1: Could your organization be attractive as a terrorist target?*
- 2.6 Categories of Terrorism Related Risk
 - 2.6.1 Explosive Attack
 - 2.6.2 Kidnapping
 - 2.6.3 Armed Attack
 - 2.6.3.1 Hijacking
 - 2.6.3.2 Armed Occupation
 - 2.6.3.3 Barricaded Hostage
 - 2.6.4 Arson
 - 2.6.5 Chemical/Biological/Radiological (CBR)
 - 2.6.6 Nuclear
 - 2.6.7 Cyber Attack
- 2.7 Terrorist Planning and Execution Phases
- 2.8 Facts to Remember About Terrorism

3. Conducting the Risk Assessment

- 3.1 Guidelines for Assessing Terrorism Related Risk
- 3.2 Step One: Identify and Profile Assets
 - 3.2.1 Asset Identification
 - 3.2.2 Sources of Asset Information
 - 3.2.3 Identification of Undesirable Events
 - 3.2.3.1 *Exercise 2: Asset Inventory*
 - 3.2.4 Asset Valuation
 - 3.2.4.1 Asset Valuation Considerations
 - 3.2.4.2 Establishing Asset Valuation Criteria
 - 3.2.4.3 Examples of Asset Valuation Scales
 - 3.2.4.4 *Exercise 3: Develop a Criteria Scale for Rating Criticality*
- 3.3 Step Two: Identify and Profile Threats (a.k.a. "Threat Analysis")
 - 3.3.1 Categories of Threats
 - 3.3.2 Identifying Potential Terrorist Adversaries
 - 3.3.2.1 *Exercise 4: Self-Assessment to Identify Potential Terrorist Adversaries*
 - 3.3.3 Adversary Assessment
 - 3.3.3.1 Sources of Adversary Information
 - 3.3.3.2 Determination of INTENT and CAPABILITY
 - 3.3.3.3 Analysis of Critical Threat Modus Operandi
 - 3.3.3.3.1 *Exercise 5: Assess Al-Qaeda as a Potential Adversary*
 - 3.3.3.3.2 Identification of Potential Risks Based on Threat M.O.
 - 3.3.3.3.3 Development of Design Basis Threats (DBTs)
 - 3.3.4 Development of Threat Scenarios
 - 3.3.4.1 *Exercise 6: Develop Several Threat Scenarios*

- 3.3.5 Development of Threat Rating Criteria
 - 3.3.5.1 Alternative Expressions of Threat
 - 3.3.5.2 *Exercise 7: Develop a Threat Rating Criteria*
- 3.4 Step Three: Identify Asset Vulnerabilities (a.k.a. “Vulnerability Assessment”)
 - 3.4.1 Vulnerability Assessment Principles
 - 3.4.2 Terrorism-Related Vulnerability Issues
 - 3.4.2.1 Protective Counterintelligence/OPSEC
 - 3.4.2.2 Access Control/Physical Security
 - 3.4.2.3 Damage Mitigation
 - 3.4.2.4 Contingency Response
 - 3.4.3 Areas of Vulnerability
 - 3.4.3.1 Environmental Characteristics
 - 3.4.3.2 Facility Characteristics
 - 3.4.3.3 Personnel Behavior
 - 3.4.3.4 Location of Assets
 - 3.4.3.5 Operational and Personnel Practices
 - 3.4.4 Vulnerability Assessment Approaches
 - 3.4.4.1 Compliance-Oriented Assessment Approaches
 - 3.4.4.2 Performance-Oriented Assessment Approaches
 - 3.4.4.3 Security Assessment Surveys
 - 3.4.4.4 Quantitative Path Intrusion Analysis
 - 3.4.4.4.1 Path Analysis Models and Software
 - 3.4.4.5 Fault Tree Analysis
 - 3.4.4.6 Practical Field Tests (a.k.a. “Red Team Exercises”)
 - 3.4.5 Completing the Vulnerability Assessment
 - 3.4.6 Developing a Vulnerability Rating Criteria

DAY TWO

- 3.5 Step Four: Evaluate Risk
 - 3.5.1 Determining Risk Probability
 - 3.5.2 Develop Probability/Criticality Pairing System for Risk Definition
 - 3.5.3 Establish Level of Risk and Risk Acceptability
 - 3.5.3.1 Case Examples
 - 3.5 Step Five: Identify & Implement Countermeasures
 - 3.5.1 Integrated Countermeasures Theory
 - 3.5.1.1 Proactive Countermeasures
 - 3.5.1.2 Reactive/Mitigative Countermeasures
 - 3.5.2 Identifying Potential Countermeasures
 - 3.5.2.1 Countermeasures Options
 - 3.5.3 Countermeasures Cost-Benefit Analysis
 - 3.5.3.1 Determining the Potential Effectiveness of Countermeasures
 - 3.5.3.2 Determining the Cost of Countermeasures
 - 3.5.3.3 Determining Risk Reduction Goals
 - 3.5.3.4 Applied Cost-Benefit Analysis
- ## 4. Special Issues in Identifying Vulnerability to Terrorist Attacks
- 4.1 Vulnerability Evaluation Methodologies
 - 4.1.1 Comparison of Threat Scenarios and Evaluation Methodologies
 - 4.2 Quantitative Path Intrusion Analysis
 - 4.2.1 Physical Security Theory
 - 4.2.1.1 Physical Security System Functions
 - 4.2.1.2 Integrated Systems
 - 4.2.1.3 Performance Definition
 - 4.2.1.4 Common Design Flaws

- 4.2.2 Probability of Adversary Sequence Interruption
 - 4.2.2.1 Adversary Task & Path Concepts
 - 4.2.2.2 Delay Time Calculation
 - 4.2.2.3 Integrated Relationship of Detection, Delay, and Response
 - 4.2.2.4 Probability of Interruption/Likelihood of Adversary Success
 - 4.2.2.5 Additional Factors Influencing System Effectiveness
- 4.2.3 Estimate of Adversary Sequence Interruption (EASI) Model
 - 4.2.3.1 EASI Input Parameters
 - 4.2.3.1.1 Determining Adversary Tasks and Delay Time
 - 4.2.3.1.2 Estimation of Probability of Detection
 - 4.2.3.1.3 Evaluation of Response Force Capabilities
 - 4.2.3.2 Adversary Path Analysis Using EASI Model
- 4.2.4 Adversary Sequence Diagrams (ASDs)
 - 4.2.4.1 *Exercise: ASD Diagram of XYZ Agrochem Nitrogen Plant*
 - 4.2.4.2 *Exercise: In-Class Analysis Using EASI Model*
- 4.2.5 Relating Quantitative Values to Qualitative Values
- 4.3 Blast Vulnerability Analysis: A Simplified Approach
 - 4.3.1 Basic Blast Dynamics
 - 4.3.1.1 Types of Explosions
 - 4.3.1.2 Chemical Explosions
 - 4.3.1.3 Destructive Forces in Conventional Explosions
 - 4.3.1.3.1 Overpressure
 - 4.3.1.3.2 Impulse
 - 4.3.1.3.3 Fragmentation
 - 4.3.2 Possible Charge Sizes in Common Bombs
 - 4.3.2.1 Max Charge Size for Various Containers/Vehicles
 - 4.3.2.2 Determining Overpressure for Various Charge Sizes
 - 4.3.2.3 Overpressure Dynamics
 - 4.3.3 Potential Facility Damage/Injuries from Overpressure Exposure
 - 4.3.3.1 Applied Overpressure Range Analysis
 - 4.3.3.2 Factors Influencing Potential Blast Vulnerability
 - 4.3.4 TSWG Bomb Damage Estimation Methods
- 4.4 Overt Vehicle Intrusion Analysis: A Simplified Approach
 - 4.4.1 Assessing Vulnerability to Overt Vehicle Entry Attacks
 - 4.4.1.1 Identifying Necessary Vehicle Exclusion Zones
 - 4.4.1.2 Identifying Possible Vehicle Approaches
 - 4.4.2 Vehicle Barrier Strength
 - 4.4.2.1 Max Kinetic Energy as Performance Measure
 - 4.4.2.2 Determining Max KE for Vehicle Attack Scenarios
 - 4.4.2.2.1 Common Vehicle Weights
 - 4.4.2.2.2 Determining Max Vehicle Velocity
 - 4.4.2.3 Characteristics of Common Vehicle Barriers
 - 4.4.2.3.1 Passive Vehicle Barriers
 - 4.4.2.3.2 Active Vehicle Barriers
 - 4.4.3 Determination of Barrier Effectiveness

About the Instructor

The primary instructor for the S2 Assessing Terrorism Related Risk workshop is Craig S. Gundry.

Craig S. Gundry, CPS, ATO, CHS-III

Craig Gundry, the Vice President of Special Projects for Critical Intervention Services (CIS), is the primary instructor for S2's Anti-Terrorism courses. Mr. Gundry is responsible for directing CIS consulting and training projects pertaining to terrorism and security, including the development of doctrine and training for the CIS Anti-Terrorism Officer Division. Prior to joining CIS, Mr. Gundry was the President of Palladium Media Group, a company specializing in training and consulting on explosive, chemical, and biological terrorism. Mr. Gundry's expertise in anti-terrorism began as a specialist in force protection with the United States Army.

Mr. Gundry is the author of the acclaimed Bomb Countermeasures for Security Professionals CD-ROM and a new book on assessing terrorism-related risk. Mr. Gundry is also a frequent consultant to the news media on issues relating to terrorism and weapons of mass destruction.

As an instructor, Mr. Gundry has been training security, police, and emergency responders in terrorism-related issues for over 10 years. His previous students have included security professionals, facility managers, military personnel, police officers, and federal officials.

Student Comments

Following are some recent statements from students who have attended the S2 Assessing Terrorism Related Risk workshop.

"I just returned to the Washington area after attending the Terrorism Related Risks 2 day course. This email is sent as kudos for a very interesting and informative course that will be of value to me and others that I interact with. Mr. Gundry is an outstanding instructor who displays a deep understanding of his subject, who keeps the interest of the students and created a solid course... Please note, that I am an intelligence and security professional with 40 years of experience in the field. I am currently the principal Analytical Risk Management instructor/facilitator for the DoD [REDACTED] Academy and taught the subject for CIA et al for some four years prior to my stint with [REDACTED]. I mention this to emphasize Mr. Gundry's evident expertise in the subject and the fact that old guys like me still have much to learn from others."

A. Pattakos, CPP, OCP (Colonel, USA-Retired)
Beta Analytics International

"The level of teaching was impressive. Craig did not skip a beat...I felt it was a large amount of information covered in a reasonable period of time and was put out in a manner that was understandable...Very informative!"

A. Volnino
Security Consultant

Hosting a Program

As an alternative to attending a scheduled Assessing Terrorism Related Risk workshop at the S2 training facility in Clearwater, organizations that would like to train their staff internally may host a seminar at their facility.

Prices and Fees

The price for presenting the two-day version of the S2 Assessing Terrorism Related Risk workshop is \$3,400.00. This price includes all instructor classroom time and travel time within the domestic United States. If the host facility is located outside of the United States, there may be additional charges for travel time.

The host will be charged for all instructor transportation and lodging expenses, including airfare, rental car or taxi fees, and hotel expenses. The host may coordinate travel and lodging directly or may leave travel coordination to the S2 staff.

Each student attending the program will receive a 180-page training manual and exercise worksheets. The host will be provided with a copy of the training manual in PDF-format for duplication prior to the scheduled class. If the host wishes S2 to provide the training manuals, manuals will be produced for the course for a fee of \$25.00 per manual.

Student Restrictions

S2 requests that all students attending the Assessing Terrorism Related Risk workshop are actively employed as security or law enforcement practitioners and have been subjected to background checks prior to their employment in their current positions. There are no restrictions on the number of students that may attend the two-day classroom program.

Presentation Requirements

The host will need to provide the following items on the day of the scheduled class:

1. Private classroom with appropriate seating for the number of students in attendance
2. Windows-compatible audio-visual projector (and extra bulb)
3. Projection screen and presentation table

Although the instructors will bring their own laptop computer for presentation, it is recommended that the host have an extra laptop computer with MS PowerPoint available in the event of a technical problem during the presentation.

Scheduling

Due to our busy project schedule, we recommend contacting us at least 60 days prior to any proposed training dates to confirm the instructor's availability. Once dates have been agreed upon, the host must provide a purchase order or a signed letter of agreement to secure the dates.

To schedule an S2 Assessing Terrorism Related Risk workshop, contact:

Tim O'Rourke, Executive Director
S2 Safety & Intelligence Institute
1261 South Missouri Ave

Clearwater, FL 33756
Tel. (727) 461-0066
Fax (727) 449-1269
Email: tim@s2institue.com