BACKGROUND

The S2 Assessing Security Related Risk workshop is designed to instruct security and public safety personnel in the dynamics of security and terrorism related risk and effective methodology for evaluating security related risk.

The information presented in this workshop reflects best practices in risk management as applied in both the government and commercial sectors of the security industry.

WORKSHOP DETAILS

Duration: Five Days, 3rd – 7th May 2009, 8:30am - 4:30pm;

Fees: US$3,575 (*including workshop materials, lunch & breaks at the venue*);

Venue: Armed Forces Officers Club & Hotel, Abu Dhabi;

Presenter: Craig Gundry, CPS, ATO, CHS-III.

WHO SHOULD ATTEND

METHOD OF INSTRUCTION

The method of instruction includes a balanced mixture of classroom lecture and workshop exercises designed to teach students important theoretical concepts as well as practical application of risk management principles. This type of combined instruction has proven very successful in previous S2 risk assessment workshops.

CONTENTS

Students attending the S2 Assessing Security Related Risk workshop will acquire the following skills and competencies:

- Understand risk management principles and the function of risk assessment in security planning;
- Recognise important characteristics of terrorism related risk and modus operandi;
- Conduct security assessments by utilising qualitative risk assessment methodology;
- Evaluate the design of physical security systems utilising quantitative assessment models;
- Evaluate potential vulnerability of structures to blast loading from IEDs;
- Design prioritised security countermeasures strategies by utilising cost-benefit analysis techniques.

THE WORKSHOP

DAY 1

1. Principle 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 Security Related Risk
   2.1 Definition
   2.2 Ideological Motives
   2.3 Strategic Objectives of Terrorist Groups
   2.4 Types of Targets
   2.5 Target Selection Criteria
      2.5.1 Exercise 1: Could your organization be attractive as a target?
   2.6 Categories of Security Related Risk
      2.6.1 Explosive Attack
         2.6.1.1 Hand-Delivered IEDs
         2.6.1.2 Vehicle-Borne IEDs
         2.6.1.3 Projected Charges
         2.6.1.4 Mail Bombs
         2.6.1.5 Anti-Vehicle IEDs
      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
      2.6.8 RFW/EMP Threats
   2.7 Planning and Execution Phases
   2.8 Facts to Remember About Terrorism

DAY 2

3. Conducting the Risk Assessment
   3.1 Guidelines for Assessing Security 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 Adversaries
3.3.2.1 Exercise 4: Self – Assessment to Identify Potential 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 a Group 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
- 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 Behaviour
  - 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

3.5 Step Four: Evaluate Risk
- 3.5.1 Determining Risk Probability
- 3.5.2 Develop Probability/Critically Pairing System for Risk Definition
- 3.5.3 Establish Level of Risk and Risk Acceptability
  - 3.5.3.1 Case Examples

3.6 Step Five: Identify & Implement Countermeasures
- 3.6.1 Integrated Countermeasures Theory
  - 3.6.1.1 Proactive Countermeasures
  - 3.6.1.2 Reactive/Mitigative Countermeasures
- 3.6.2 Identify Potential Countermeasures
  - 3.6.2.1 Countermeasures Options
- 3.6.3 Countermeasures Cost-Benefit Analysis
  - 3.6.3.1 Determining the Potential Effectiveness of Countermeasures
3.6.3.2 Determining the Cost of Countermeasures
3.6.3.3 Determining Risk Reduction Goals
3.6.3.4 Applied Cost-Benefit Analysis

**DAY 3**

3.7 Risk Assessment Example: Electrical Power Plant

   4.1 US DOJ Chemical Plant Vulnerability Assessment Methodology
   4.2 DHS CFAT Security Vulnerability Assessment Methodology
   4.3 US DOE Electricity Utility Vulnerability Assessment Model
   4.4 CIA Security Vulnerability Assessment Methodology
   4.5 CARVER/CARVER + Shock

5. Special Vulnerability Assessment Techniques
   5.1 Summary of Techniques for Assessing Vulnerability
   5.2 Quantitative Intrusion Path Analysis
      5.2.1 Performance Based Physical Security Principles
         5.2.1.1 Physical Security Theory
         5.2.1.2 Adversary Paths
         5.2.1.3 Consideration Factors
         5.2.1.4 EASI Model
         5.2.1.5 Adversary Tasks

**DAY 4**

5.2.1.6 Intrusion Detection
   5.2.1.6.1 Probability of Detection
   5.2.1.7 Response Force Capability
   5.2.1.8 Adversary Sequence Diagrams
   5.2.1.9 Exercise: Physical Security Analysis Using EASI Model

5.3 Blast Vulnerability Assessment
   5.3.1 Blast Dynamics
      5.3.1.1 Types of Damaging Forces
      5.3.1.2 Overpressure
   5.3.2 Structural Response to Overpressure Loading
      5.3.2.1 Overpressure Range Effects Analysis
      5.3.2.2 Simplified Estimation Guidelines

5.3.3 Structural Design Factors
   5.3.3.1 Structural Shape
   5.3.3.2 Structural Support
   5.3.3.3 Façade Construction & Glazing
   5.3.3.4 Location of Assets

**DAY 5**

On Day Five, the class will be divided into groups based on the types of facilities they protect in their normal work routines. Each group will then be provided with
instructions to conduct an assessment of a model facility and will be provided with a series of worksheets to complete as part of this exercise. Each group will also be provided with a packet of detailed information about their model facility to use as a reference when completing the exercises. At the end of the day, each group will present the findings of their tabletop assessment to the rest of the class.

The day will end around 16:00 with a presentation of student certificates.

THE INSTRUCTOR

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

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 management, 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 specialising 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 on issues relating to terrorism and weapons of mass destruction and has provided expert commentary for numerous media organisations, including CNN.

As an instructor, Mr. Gundry has been training security, police and emergency responders in terrorism-related issues for over 13 years. His previous students have included security professionals, facility managers, military personnel, police officers, and federal officials from over 30 nations.

ENROLLMENT

To register for the 2009 Abu Dhabi Assessing Security Related Risk workshop, use our online student enrollment and payment system.

Click the following link:

http://www.s2institute.com/content/_pages_advanced/_courses/atrr_abudhabi09.php
ENDORSEMENTS

We believe that there is no better way to convey the quality of our anti-terrorism instructional programs than through the words of our previous students. The following are some opinion statements from a handful of the thousands of students who have received anti-terrorism training from the S2 Safety & Intelligence Institute since 1998.

“I personally give thanks to S2 and CIS for the opportunity to attend the Anti-Terrorism Officer (ATO) training sessions. In all of my travels and training, military and civilian, I rarely have the pleasure of encountering such professional instructors and presentations. The knowledge possessed and demonstrated by the instructor staff sets the bar for all civilian training agencies to follow...The training you are providing to security personnel, military personnel and law enforcement professionals, is unmatched by civilian readiness training for the war on terror.”

J. White
Advanced Training Section, U.S. Special Operations Command

“The instructor knew all the subjects like the back of his hand.....A+++!”

SMSgt G. Enwright
Office of the Secretary of the Air Force, USAF

“This course is designed extremely well. I have had a few terrorism/ anti-terrorism classes, but none have come close to the intensity and historical background as the S2 course. Your course is what every law enforcement officer should be taking.”

R. Bast
U.S. Department of Treasury

“I just returned to the Washington area after attending the Terrorism Related Risk 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 Joint Counterintelligence Academy and taught the subject for CIA et al for some four years prior to my stint with DoD. 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 Analysis International

“I thought that the course was outstanding. I had previous training from the military on multiple levels, but this went much more in depth. I recommend this course to anyone in the field.”
SSG S. Scarliff
U.S. Army

“I thought this course was very well done. The handouts were great and the topics very relevant and up to date with what is currently going on. This is definitely a “must take” course for anyone dealing with physical security/anti-terrorism matters.”

C. Vernieuw
U.S. Army Research Institute of Environmental Medicine

“The scope and depth of instruction provides an awesome foundation for the development of a career in combating terrorism. I know the investment I made in this course will prove invaluable.”

J. Skerry, III
Sarasota County Sheriff’s Office

“Really excellent. A lot of practical advice that one can use in one’s everyday work. Excellent.”

J. Perios
Dolphin Energy, Ltd. “The course material was well presented and exceeds my expectations in every way. Mr. Gundry’s performance as an instructor along with his experience and real world case studies really made and impression... I highly recommend this course material for all federal entities.” R. Williams
U.S. Army

“This is a really good course and it provides a lot of very useful information about anti-terrorism issues. I would recommend it to others because it is very educational.”

R.W. Calvert
Department of National Defense, Canada
### COURSE REGISTRATION FORM

Fax (727) 210-0611

Return to: S2 Institute Registration, 1261 S. Missouri Avenue, Clearwater, FL 33756 • Tel. (727) 461-0066 • Fax: (727) 210-0611

To guarantee a seat in any S2 program, fax or mail your registration today!

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Course Date(s)</th>
<th>Course Tuition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Name, First Name, Middle Initial</th>
<th>Salutation (Mr., Mrs., etc)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization/Agency</th>
<th>Division or Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mailing Address</th>
<th>City</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zip Code</th>
<th>Country</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Emergency Contact Name and Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Registration Eligibility

*NOTE: All registration applicants for restricted classes are subject to identity verification.*

1. Are you a U.S. Citizen? Yes____________ No_________________ If NO, country of citizenship:__________________________________________

2. If you are registering for a restricted class, check the box that best describes your eligibility status.

- [ ] FL “D” License Holder
- [ ] FL “G” License Holder
- [ ] FL “C” or “CC” License Holder
- [ ] Full-Time Security Mgmt Professional
- [ ] Cert. Law Enforcement Officer
- [ ] U.S. Government Employee
- [ ] Human Resources Professional
- [ ] Other:_________________

### Payment Method

- [ ] Company/Government Purchase Order No.:_____________________________________
  *(Private organizations must call for approval)*

- [ ] Company/Agency Check
  *(Payable to: S2 Institute) (The Institute's Federal Tax ID Number is 59-3480247)*

- [ ] Credit Card  *(NOTE: Your card will be billed upon receipt and confirmation of enrollment.)*
  - [ ] American Express
  - [ ] Discover
  - [ ] MasterCard
  - [ ] Visa
  
  CARD NUMBER: __ __ __ __ - __ __ __ __ - __ __ __ __ - __ __ __ __
  Expiration Date (Mo./Yr.):_____/_____  Authorized Signature:_____________________________________

### CANCELLATION POLICY

Students will receive a full refund of fees if written notice of cancellation is received within 30+ days prior to course start date. Students will receive any paid fees, minus 25% of the course tuition, if notice of cancellation is received within 30 days of the course start date. If the student is a No-Show (with no prior notification), the Institute will not refund the fee.

### WHEN YOUR REGISTRATION FORM IS PROCESSED, YOU WILL RECEIVE A CONFIRMATION BY E-MAIL.