



Precept
management consultancy

SECURITY RISK ASSESSMENT

Intercontinental Hotel Muscat, Oman; 14th-16th June 2010

The S2 Security Risk Assessment workshop is designed to instruct security and public safety personnel in the dynamics of security risk and effective methodology for evaluating risk and designing countermeasures strategies.

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

WORKSHOP DETAILS

- Duration: Three Days, 14th-16th June 2010, 8:30 am- 4:30 pm;
- Fees: RO 985/US\$ 2,575/AED 9,400 (*including workshop materials, lunch & breaks at the venue*);
- Venue: Muscat, Oman;
- Presenter: Craig S. Gundry, CPS, ATO, CHS-III

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.

WHAT WILL BE ACCOMPLISHED

Participants attending the S2 Security Risk Assessment Workshop will acquire the following skills and competencies:

- Understand risk management principles and the function of risk assessment in security planning;
- Recognize important characteristics of security related risk;
- Conduct security assessments by utilizing qualitative risk assessment methodology;
- Design prioritized security countermeasures strategies by utilizing cost-benefit analysis technique.

Please contact us for further information or click [here](#) to register

Precept Management Consultancy, P.O. Box 255, P.C. 112, Sultanate of Oman

Tel: +968 24497123, Fax: +968 24497222, E-mail: precept@omantel.net.om

Website: www.preceptmanagement.com

THE WORKSHOP

Day 1

08:30 – 10:30	Principles of Security Risk Management
10:30 – 12:00	Characteristics of Security Risk
12:00 – 13:00	Lunch
13:00 – 15:00	Characteristics of Security Risk (cont.)
15:00 – 16:30	Assessing Security Risk

Day One introduces the principles of risk management security related risk. Although the information in Day One is presented in lecture format, several workshop exercises aimed at reinforcing important concepts will be conducted in the classroom and discussed as a group.

Day 1 Outline:

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 Security Related Risk

2.1 Definition

2.2 Adversary Motives

2.3 Objectives of Adversaries

2.4 Target Selection Characteristics

2.5 Categories of Security Risk

2.5.1 Theft

2.5.2 Vandalism

2.5.3 Accidents & Occupational Hazards

2.5.4 Terrorism

2.5.4.1 Explosive Attack

2.5.4.2 Kidnapping

2.5.4.3 Armed Attack

2.5.4.4 Arson

2.5.4.5 Chemical/Biological/Radiological (CBR)

2.5.4.6 Nuclear

2.5.4.7 Cyber Attack

2.5.4.8 RFW/EMP Threats

2.5.5 Workplace Violence

Day 2

08:30 – 12:00	Assessing Security Risk
12:00 – 13:00	Lunch
13:00 – 16:30	Assessing Terrorism Related Risk (cont.)

Day Two is a continuation of classroom instruction from Day One and will focus on asset identification, threat analysis, and vulnerability assessment. During Day Two several in-class workshop exercises will be conducted to reinforce important concepts and aid students in applying risk management concepts in practical situations.

Day 2 Outline:

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 1: 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

3.3.3 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 2: 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 3: 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 4: Develop a Threat Rating Criteria

3.4 Step Three: Identify Asset Vulnerabilities

3.4.1 Vulnerability Assessment Principles

3.4.2 Areas of Vulnerability

3.4.2.1 Environmental Characteristics

3.4.2.2 Facility Characteristics

3.4.2.3 Personnel Behaviour

- 3.4.2.4 Location of Assets
- 3.4.2.5 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 3

- 08:30 – 12:00 Assessing Security Risk (cont.)
- 12:00 – 13:00 Lunch
- 13:00 – 16:30 Assessing Terrorism Related Risk (cont.)

Day Three is a continuation of classroom instruction from Day Two and will focus on assimilation of risk data and countermeasures planning using cost-benefit analysis techniques. In the afternoon of Day Three, an exercise will be conducted to assimilate all of the techniques described in the previous sections.

Day 3 Outline:

- 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
- 3.6 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 Identifying 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

THE COMPANY



Since 1998, the S2 Safety & Intelligence Institute has trained thousands of security, intelligence, and law enforcement professionals in critical public safety topics. With a staff of world class instructors, S2 has earned a reputation as one of the U.S.'s premier sources of security and public safety training.

S2 provide traditional classroom instruction and hands on training at their facility in Clearwater, Florida and at host locations throughout the United States. Through their sister company the, S2 Online Academy, they also deliver high quality distance education to students throughout the world.

S2 students represent hundreds of corporations and government organisations. Some examples of S2 clients include the Federal Bureau of Prisons, US Capitol Police, US Department of Justice, and US Special Operations Command.

PRESENTER'S PROFILE

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

Craig Gundry is the S2 Institute's lead instructor for anti-terrorism subjects and the Vice President of Special Projects for Critical Intervention Services (CIS). 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 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 on issues relating to terrorism and weapons of mass destruction and has provided expert commentary for numerous media organizations, including CNN and Fox News Network.

As an instructor, Mr. Gundry has been training security, police, and emergency responders in terrorism-related issues for over 16 years. His previous students have included security professionals, facility managers, military personnel, police officers, and federal officials from over 30 nations.