

Perimeter & Physical Security: Are you Prepared?

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Beginner / Group-Live

PREREQUISITES: None

ADVANCED PREPARATION: None

Since the September 11th attacks, physical security requirements have increased significantly. Executives want to provide a safe and secure environment for their management and staff. They also want to ensure that the controls do not infringe on employee rights or result in unnecessary delays entering or leaving the building. This seminar is designed to provide the participants with the skills they need to perform a full proximity, perimeter and physical security assessment. The participants will learn how to conduct a structured, detailed threat analysis and to prepare risk assessments for each component of the review. They will then learn how to implement facility, employee and executive security procedures. The seminar includes unauthorized surveillance techniques. The instructor will also cover countermeasures and detection procedures. By the end of this session, the participants should be able to perform their first comprehensive security review of their facilities and employee and executive security.

WHO SHOULD ATTEND

This seminar is intended for internal auditors, asset protection managers, loss prevention and security officers. There are no prerequisites.

SEMINAR OUTLINE

- I Introduction**
 - The need for change
 - Assessing the risk
 - Tailoring the physical security audit
 - Understanding staff issues
 - Security versus accessibility
 - Special accommodations and bypass procedures
- II Policies and Procedures**
 - What needs to change
 - Expect resistance
 - Variations to policies by location
 - Policies/procedures for
 - staff
 - executives
 - trading partners/visitors
 - Access policies
 - Staged implementation
 - Security procedures
 - Risk / control tables & checklists
- III Perimeter Security**
 - Defining the perimeter
 - Implementing multiple perimeters
 - Staging security by perimeter
 - Security equipment and placement
 - Unsecured access points
 - "Right of way" security
 - Adjoining property risks
 - Underground access and parking risks
 - Shared building risks
- IV Proximity Security**
 - The need for proximity security
 - Protecting major facilities
 - Securing access points
 - Vehicle entry controls
 - Employee entry procedures
 - Guest entry procedures
 - Inspection and identification procedures
 - Preparing the proximity risk assessment
 - Risk / control tables & checklists
- V Physical Security**
 - Identifying all entry points
 - Public vs. non public access
 - Security equipment and placement
 - Entrance controls
 - Multiple ring security
 - Controlling access to sensitive areas
 - Access tokens & zone controls
 - Guest & consultant access control
 - Controlling service personnel and technicians
 - Monitoring the facility
- VI Employee and Executive Security**
 - Developing effective policies
 - Workplace procedures
 - Travel procedures
 - Executive floor issues
 - Executive protection programs
 - Sanitizing executive offices
 - Event and special activity security
 - Awareness and training programs
 - Preparing the employee risk assessment
 - Preparing the executive risk assessment
 - Risk / control tables & checklists
- VII Preparing for the Unknown**
 - Developing and testing event scenarios
 - Practicing employee procedures
 - Identifying potential threats
 - Preparing threat assessments
 - Using security consultants
 - Risk / control tables & checklists
- Service access point risks**
 - Mapping security "blind spots"
 - Identifying vantage points
 - Walking the perimeter
 - Preparing the Perimeter Risk Assessment
 - Risk / control tables & checklists
- Protecting against other hazards (fire, etc)**
 - Preparing the Physical risk assessment
 - Risk / control tables & checklists