Corporate Counter-Terrorism and Security Strategy Training Course



26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #SM4086_131233

Course Introduction / Overview:

This comprehensive training course is designed to equip corporate security leaders with the advanced knowledge and strategic frameworks necessary to protect their organizations from the evolving threat of terrorism. In a world where corporate entities are increasingly targeted, a reactive security posture is no longer sufficient. This program focuses on building proactive, intelligence-led counter-terrorism strategies that integrate physical security, cybersecurity, and human factors. Drawing upon contemporary security theories and real-world case studies, the curriculum provides a holistic approach to risk management and threat mitigation. As noted by security scholar Bruce Hoffman in his seminal work, "Inside Terrorism," understanding the motivations and methodologies of terrorist groups is fundamental to developing effective countermeasures. This course, offered by BIG BEN Training Center, moves beyond theoretical concepts to provide practical, actionable skills in threat assessment, crisis management, and emergency response planning. Participants will learn to create resilient security architectures that safeguard assets, personnel, and corporate reputation against a spectrum of modern threats, ensuring business continuity and organizational stability in an uncertain global landscape.

Target Audience / This training course is suitable for:

- Corporate Security Directors and Managers.
- Chief Security Officers (CSOs).
- Risk Management Professionals.
- Facility and Operations Managers.
- Business Continuity Planners.
- Crisis Management Team Leaders.
- Law Enforcement and Intelligence Officers transitioning to the private sector.
- Human Resources and Legal Compliance Officers.
- Executive Protection Specialists.

Target Sectors and Industries:

- Financial Services and Banking.
- Energy, Oil, and Gas sectors.
- Critical National Infrastructure.
- Aviation and Transportation.
- Hospitality and Large-Scale Event Management.
- Telecommunications and Technology.
- Major Retail and Commercial Real Estate.
- Pharmaceutical and Chemical Industries.
- Government agencies and public sector organizations.

Target Organizations Departments:

- Corporate Security and Loss Prevention.
- Risk Management and Compliance.
- Operations and Facilities Management.
- Executive Leadership and C-Suite.
- Human Resources.
- Legal and General Counsel.
- Information Technology and Cybersecurity.
- Crisis Management and Emergency Response Teams.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop a comprehensive corporate counter-terrorism strategy aligned with organizational goals.
- Conduct detailed threat, vulnerability, and risk assessments for corporate assets.
- Analyze terrorist tactics, motivations, and targeting methodologies.
- Integrate physical security measures with cybersecurity protocols for a layered defense.
- Establish and manage a corporate intelligence gathering and analysis program.
- Design and implement effective crisis management and emergency response plans.
- Develop strategies to mitigate insider threats and prevent radicalization in the workplace.
- Lead and coordinate with public sector security and intelligence agencies.
- Enhance business continuity and organizational resilience against terrorist threats.
- Formulate security policies that are both effective and legally compliant.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical, ensuring that participants can immediately apply their learning in a real-world corporate environment. We move beyond traditional lectures to foster a dynamic learning atmosphere built on active participation and collaborative problem-solving. The course heavily utilizes case studies of actual terrorist incidents involving corporations, allowing participants to deconstruct events, analyze security failures, and identify successful mitigation strategies. Interactive workshops and group exercises will challenge attendees to develop threat assessments, design security plans for hypothetical facilities, and draft crisis communication protocols. A significant portion of the training will be dedicated to simulation-based learning, where participants will engage in realistic scenarios that test their decision-making skills under pressure. Expert-led discussions will provide a platform for sharing experiences and best practices, while continuous feedback from instructors ensures a deep and lasting understanding of the core concepts. This hands-on approach guarantees that participants leave not just with knowledge, but with the confidence and competence to lead their organization's counter-terrorism efforts.

Course Agenda (Course Units):

Unit One: The Modern Terrorist Threat to Corporations

- Understanding the Evolution of Global Terrorism.
- Ideologies, Motivations, and Objectives of Modern Terrorist Groups.
- Corporate Targeting Rationale and Methodologies.
- Lone-Wolf Actors versus Organized Cells.
- The Convergence of Physical and Cyber Terrorism.
- Case Studies of Terrorist Attacks on Corporate Targets.
- Introduction to Counter-Terrorism Legal and Ethical Frameworks.

Unit Two: Intelligence-Led Threat and Vulnerability Assessment

- Fundamentals of Corporate Security Intelligence.
- Open-Source Intelligence (OSINT) Gathering Techniques.
- Developing a Corporate Threat Intelligence Program.
- Conducting Comprehensive Site Vulnerability Assessments (SVAs).
- The CARVER Target Analysis and Vulnerability Assessment Methodology.
- Identifying and Analyzing Potential Insider Threats.
- Predictive Analysis and Early Warning Indicators.

Unit Three: Designing Proactive Security Architectures

- Principles of Layered Security and Defense-in-Depth.
- Advanced Physical Security Measures and CPTED Principles.
- Integrating Access Control, Surveillance, and Intrusion Detection Systems.
- Securing Supply Chains and Logistics against Terrorist Infiltration.
- Developing a Robust Mail and Package Screening Program.
- Cybersecurity Protocols to Counter Terrorist-Related Digital Threats.
- Personnel Security, Vetting, and Background Checks.

Unit Four: Crisis Management and Emergency Response

- Developing a Corporate Crisis Management Framework.
- Establishing an Emergency Operations Center (EOC).
- Incident Command System (ICS) for Corporate Security.
- Crafting Effective Crisis Communication Strategies for Internal and External Stakeholders.
- Bomb Threat Management and Response Protocols.
- Active Assailant and Hostage Situation Response Planning.
- Coordinating with Law Enforcement and First Responders.

Unit Five: Strategic Leadership and Organizational Resilience

- Leading a Security Team During a High-Stress Incident.
- Post-Incident Recovery and Business Continuity Planning.
- Training and Drills for Corporate Security and General Staff.
- Building a Security-Aware Culture within the Organization.
- Public-Private Partnerships in Counter-Terrorism.
- Countering Terrorist Financing and Corporate Responsibility.
- Future Trends and Emerging Threats in Corporate Security.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an era of evolving digital and ideological threats, how can a static corporate security policy remain effective without infringing on employee privacy?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond conventional security training to adopt a strategic, intelligence-driven C-suite perspective on counter-terrorism. While many programs focus solely on reactive, physical security measures, this curriculum deeply integrates the critical pillars of threat intelligence, cybersecurity, and the human element, reflecting the complex nature of modern threats. We emphasize a proactive, predictive approach, teaching participants not just how to respond to an attack, but how to anticipate and disrupt threats before they materialize. The course content is rooted in advanced academic theory, such as the principles of risk analysis and game theory in security, yet is delivered through highly practical, hands-on simulations and real-world case studies. Unlike generic security courses, this program is specifically tailored to the corporate environment, addressing unique challenges like brand reputation, business continuity, and the legal intricacies of private-sector security operations. The focus on leadership and strategic communication equips participants to effectively articulate risk and justify security investments to executive boards, making them not just security managers, but strategic business partners in their organizations.