Critical Infrastructure Protection and Resilience Strategy Training Course



16 - 20 Nov 2026

Boston

7500 € (Per Person)

Ref: #CYB6307_88385

Course Introduction / Overview:

In our increasingly interconnected world, the security and resilience of critical infrastructure are paramount to national security, economic stability, and public safety. This comprehensive training course provides an in-depth exploration of the principles and practices required to protect essential assets and systems from an all-hazards threat landscape, including cyberattacks, physical threats, and natural disasters. Drawing upon foundational concepts from experts like Stephen E. Flynn and his work in "The Edge of Disaster: Rebuilding a Resilient Nation", this program moves beyond traditional security paradigms to embrace a holistic, strategic approach to resilience. Participants will delve into the complexities of cyber-physical systems, interdependency analysis, and the critical role of public-private partnerships in building a robust protective posture. BIG BEN Training Center has designed this course to equip professionals with the foresight and skills to not only defend against current threats but also to anticipate and adapt to future challenges, ensuring the continuity of essential services in the face of adversity. This is not just a technical course; it is a strategic masterclass in safeguarding the lifelines of modern society.

Target Audience / This training course is suitable for:

- Infrastructure Sector Managers and Operators.
- Government Officials and National Security Advisors.
- Emergency Management and Response Planners.
- Corporate Security and Risk Management Professionals.
- IT and Cybersecurity Specialists for Industrial Control Systems.
- Law Enforcement and Intelligence Analysts.
- Urban Planners and Public Works Directors.
- Compliance and Regulatory Officers.
- Business Continuity and Disaster Recovery Planners.
- Supply Chain and Logistics Managers.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Oil, and Gas).
- Water and Wastewater Systems.
- Transportation Systems (Air, Road, Rail, and Maritime).
- Information and Communication Technology.
- Banking and Financial Services.
- Public Health and Healthcare.
- Government Facilities and Defense Industrial Base.
- Commercial Facilities and Real Estate.
- Food and Agriculture.
- Chemical and Hazardous Materials.

Target Organizations Departments:

- Corporate Security and Asset Protection.
- Operations and Facility Management.
- Risk Management and Compliance.
- Information Technology and Cybersecurity.
- Emergency Management and Crisis Response.
- Strategic Planning and Policy Development.
- Health, Safety, and Environment (HSE).
- Supply Chain and Logistics.
- Legal and Regulatory Affairs.
- Internal Audit and Assurance.

Course Offerings:

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

- Develop a comprehensive risk assessment framework for critical assets.
- Analyze complex interdependencies between different infrastructure sectors.
- Design and implement integrated cyber and physical security strategies.
- Formulate robust incident response and disaster recovery plans.
- Evaluate and apply relevant national and international standards and regulations.
- Lead public-private partnership initiatives for enhanced regional resilience.
- Conduct effective vulnerability assessments for industrial control systems (ICS).
- Master crisis communication techniques during infrastructure disruptions.
- Develop metrics to measure and improve organizational resilience over time.
- Apply strategic foresight to anticipate emerging threats to critical infrastructure.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, moving beyond theoretical lectures to foster real-world problem-solving skills. This course utilizes a blended learning approach that includes expert-led presentations, in-depth case study analyses of historical infrastructure failures, and collaborative group workshops. Participants will engage in tabletop exercises and simulations that challenge them to respond to complex, multi-faceted crisis scenarios, such as a coordinated cyber-physical attack on a power grid. Team-based projects will focus on developing a complete resilience strategy for a model organization, requiring participants to conduct risk assessments, analyze interdependencies, and present their plans for peer and instructor review. Emphasis is placed on active participation, with facilitated discussions and Q&A sessions encouraging the sharing of diverse experiences and perspectives. This hands-on, engaging environment ensures that participants not only grasp the critical concepts but also develop the confidence and competence to apply them directly within their own organizations.

Course Agenda (Course Units):

Unit One: Foundations of Critical Infrastructure Protection

- Defining critical infrastructure and its essential role in society.
- Historical context and evolution of infrastructure protection.
- Overview of the 16 critical infrastructure sectors.
- Understanding the all-hazards threat landscape.
- Key legal, regulatory, and policy frameworks.
- The fundamental principles of security convergence (cyber-physical).
- Introduction to public-private partnerships in CIP.

Unit Two: Risk Management and Vulnerability Assessment

- Conducting a comprehensive threat and hazard identification process.
- Methodologies for vulnerability assessment of physical and cyber assets.
- Quantitative and qualitative risk analysis techniques.
- Developing and using a risk assessment matrix.
- Business Impact Analysis (BIA) for critical functions.
- Understanding and mapping infrastructure interdependencies.
- Prioritizing assets and systems for protection efforts.

Unit three: Securing Cyber-Physical and Industrial Control Systems

- Introduction to Industrial Control Systems (ICS) and SCADA.
- Common vulnerabilities in operational technology (OT) environments.
- Strategies for securing legacy and modern ICS architectures.
- Network segmentation and access control for OT systems.
- Threat intelligence and monitoring for cyber-physical threats.
- Incident response specific to ICS and SCADA environments.
- Aligning with standards like the NIST Cybersecurity Framework.

Unit Four: Building and Implementing Resilience Strategies

- The distinction between protection, security, and resilience.
- Developing a strategic framework for organizational resilience.
- Business continuity planning for essential services.
- Disaster recovery strategies for critical IT and OT systems.
- Building resilience into the supply chain.
- The role of redundancy, diversity, and adaptability.
- Developing and testing emergency response and evacuation plans.

Unit Five: Crisis Management, Recovery, and Future Outlook

- Principles of the Incident Command System (ICS) for infrastructure events.
- Effective crisis communication strategies for stakeholders and the public.
- Coordinating response and recovery with external agencies.
- Post-incident analysis and continuous improvement.
- Emerging threats: AI, quantum computing, and climate change impacts.
- The future of smart infrastructure and its security challenges.
- Capstone exercise: Developing a comprehensive CIP and resilience plan.

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 increasing systemic interdependencies, how can a single organization effectively build resilience when its critical functions rely on external infrastructures it does not control?

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

This course distinguishes itself by adopting a truly strategic and integrated perspective on infrastructure resilience, moving beyond siloed technical training. While many programs focus narrowly on either cybersecurity or physical security, this curriculum is built on the principle of security convergence, treating cyber-physical systems as a single, interconnected domain. It emphasizes the complex web of interdependencies between sectors, a critical aspect often overlooked, teaching participants how to analyze and mitigate cascading failures. The methodology prioritizes strategic thinking and policy development over mere tool-based training, empowering leaders to build robust, adaptive resilience frameworks. Through advanced simulations and case studies drawn from real-world events, participants do not just learn theory; they actively engage in the complex decision-making required during a crisis. The focus is on creating proactive, forward-looking leaders who can build resilient organizations capable of withstanding and recovering from the sophisticated, multi-faceted threats of the 21st century.