Converged Cyber-Physical Security Management Training Course



23 - 27 Nov 2026

Cape town

4600 € (Per Person)

Ref: #SM5554_281807

Course Introduction / Overview:

In today's interconnected world, the lines between the physical and digital realms are rapidly disappearing, creating complex cyber-physical systems (CPS) that are foundational to our critical infrastructure and modern enterprises. This convergence, while driving efficiency and innovation, also introduces a new spectrum of sophisticated risks where a cyber-attack can have devastating physical consequences. This course provides a comprehensive framework for understanding and managing these integrated threats. Drawing on principles outlined by experts like Martin C. Libicki in works such as "Cyberspace in Peace and War," this program moves beyond traditional, siloed security approaches. BIG BEN Training Center has designed this training to equip professionals with the strategic knowledge and practical skills to build a resilient, converged security program. Participants will learn to holistically assess vulnerabilities across IT, Operational Technology (OT), and physical security domains, developing unified governance, policies, and incident response plans to protect their organization's most critical assets from an evolving array of cyber-physical threats. This is an essential training for building a forward-looking security posture in a hyper-connected environment.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs).
- Physical Security Directors and Managers.
- IT Security Professionals and Analysts.
- Operational Technology (OT) and ICS Engineers.
- Enterprise Risk Management Professionals.
- Compliance and Audit Officers.
- Facility and Operations Managers.
- Corporate Security and Asset Protection Specialists.
- Business Continuity and Disaster Recovery Planners.
- System Integrators and Security Consultants.

Target Sectors and Industries:

- Energy and Utilities (Power Grids, Water Treatment).
- Manufacturing and Industrial Automation.
- Transportation and Logistics (Aviation, Rail, Maritime).
- Healthcare and Medical Device Management.
- Financial Services and Data Centers.
- Telecommunications and Network Infrastructure.
- Government, Defense, and Public Safety Agencies.
- Smart Cities and Building Management.
- Pharmaceutical and Chemical Industries.

Target Organizations Departments:

- Information Technology (IT) and Cybersecurity.
- Physical Security and Asset Protection.
- Operations and Facility Management.
- Risk Management and Corporate Governance.
- Internal Audit and Compliance.
- Engineering and Technical Services.
- Legal and Regulatory Affairs.
- Business Continuity and Crisis Management.
- Human Resources (Insider Threat Programs).

Course Offerings:

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

- Develop a strategic roadmap for security convergence within their organization.
- Conduct comprehensive risk assessments that cover integrated cyber-physical threats.
- Design and implement a unified security governance framework for IT, OT, and physical security.
- Analyze the unique vulnerabilities of Industrial Control Systems (ICS) and the Internet of Things (IoT).
- Integrate physical access control and video surveillance systems with cybersecurity monitoring.
- Create a converged security incident response plan (CSIRP) for coordinated action.
- Align security policies with industry standards and regulatory compliance requirements.
- Foster effective collaboration between traditionally siloed security and operations teams.
- Evaluate emerging technologies like AI and their impact on cyber-physical security.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring that participants can directly apply the learned concepts to their professional roles. This course moves beyond theoretical lectures by incorporating a dynamic blend of expert-led presentations, real-world case study analyses of major cyber-physical incidents, and collaborative group workshops. Participants will engage in tabletop exercises that simulate complex security breaches, forcing them to make critical decisions and coordinate responses between IT, OT, and physical security teams. Interactive Q&A sessions, peer-to-peer discussions, and practical problem-solving activities are woven throughout the five days to foster a deep and lasting understanding of converged security principles. Our approach emphasizes strategic thinking and framework development over vendor-specific tool training, providing a robust and adaptable skill set. The facilitator will provide continuous feedback, guiding participants as they build a foundational converged security plan tailored to a hypothetical organization, ensuring they leave with both knowledge and confidence.

Course Agenda (Course Units):

Unit One: Foundations of Modern Converged Security

- Introduction to Cyber-Physical Systems (CPS).
- The evolution from siloed security to a converged model.
- Understanding the domains of IT, OT, and Physical Security.
- Key differences in priorities and protocols (e.g., CIA vs. safety).
- The modern threat landscape for critical infrastructure.
- Analyzing motivations of threat actors in the cyber-physical realm.
- Case studies of historical cyber-physical attacks.

Unit Two: Risk Management for a Converged Environment

- Principles of Enterprise Security Risk Management (ESRM).
- Conducting an integrated cyber-physical risk assessment.
- Threat modeling for interconnected systems and IoT devices.
- Vulnerability analysis across digital and physical assets.
- Applying frameworks like the NIST Cybersecurity Framework to OT.
- Calculating risk and prioritizing mitigation efforts.
- Developing a unified risk register for the organization.

Unit Three: Integrating Security Controls and Technologies

- Technical security controls for Industrial Control Systems (ICS/SCADA).
- Best practices for securing Internet of Things (IoT) and IIoT devices.
- Integrating Physical Access Control Systems (PACS) with IT identity management.
- Leveraging video surveillance and analytics for threat detection.
- Network segmentation strategies for IT and OT environments.
- Implementing a Converged Security Operations Center (C-SOC) concept.
- Secure configuration management for cyber-physical assets.

Unit Four: Governance, Policy, and Compliance

- Developing a converged security governance structure.
- Creating unified security policies, standards, and procedures.
- Defining roles and responsibilities for converged security teams.
- Navigating the regulatory and legal landscape (e.g., NERC CIP, GDPR).
- Building a culture of security awareness across all departments.
- Managing third-party and supply chain cyber-physical risks.
- Strategies for effective communication with executive leadership and boards.

Unit Five: Converged Incident Response and Future Trends

- Building a Cyber-Physical Incident Response Plan (CPIRP).
- Coordinating response teams during a converged security event.
- Digital and physical forensics in a converged investigation.
- Business continuity and disaster recovery for cyber-physical disruptions.
- The role of Artificial Intelligence (AI) and Machine Learning (ML) in converged security.
- Preparing for future threats from quantum computing and advanced technologies.
- Developing a strategic roadmap and maturity model for security convergence.

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:

How might the principles of zero-trust architecture be adapted and implemented effectively in legacy Operational Technology (OT) environments where system availability and safety are paramount?

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

This training course distinguishes itself by adopting a holistic, strategy-first approach to the complex challenge of cyber-physical security. While many courses focus narrowly on the technical aspects of either cybersecurity or physical security, this program is uniquely designed to bridge the critical gap between these traditionally separate disciplines. We emphasize the development of a unified governance framework and a collaborative culture, which are the true foundations of a resilient converged security program. The curriculum is built around real-world case studies from critical infrastructure sectors, providing participants with practical insights into the consequences of failure and the hallmarks of success. Rather than concentrating on specific software or hardware, our focus is on building transferable skills in integrated risk assessment, threat modeling, and incident response coordination. Participants will not just learn about the tools; they will master the strategic thinking required to lead their organizations through the process of convergence, ensuring that security becomes an enabler of business operations, not a barrier. This strategic, people-and-process-centric methodology ensures the lessons learned are both timeless and immediately applicable.