Advanced Strategic Incident Response and Crisis Management Training Course

14 - 18 Dec 2026

Boston

7500 € (Per Person)

Ref: #CYB8889_89736

Course Introduction / Overview:

In today's interconnected and volatile environment, the ability to respond effectively to incidents and manage crises is no longer a specialized skill but a core business necessity. This course provides a comprehensive framework for mastering both the technical and strategic aspects of incident response and crisis management. It moves beyond reactive measures to instill a proactive mindset focused on preparedness, operational resilience, and reputation management. As highlighted by crisis management expert Dr. Eric K. Stern in his works, effective crisis leadership is about sense-making, decision-making, and meaning-making under pressure. This principle is a cornerstone of our curriculum. Participants will explore concepts from seminal texts like "The Politics of Crisis Management" to understand the complex interplay of technical response, stakeholder communication, and strategic leadership. BIG BEN Training Center has designed this program to equip professionals with the tools to develop robust incident response plans, lead with confidence during a crisis, and transform disruptive events into opportunities for organizational learning and improvement, ensuring business continuity and safeguarding brand integrity.

Target Audience / This training course is suitable for:

- Crisis Management Team Members.
- Incident Response Team Leaders and Members.
- IT and Cybersecurity Professionals.
- Business Continuity and Disaster Recovery Planners.
- Public Relations and Corporate Communications Specialists.
- Risk Management and Compliance Officers.
- Senior Executives and Department Heads (CIOs, CISOs, COOs).
- Legal and Human Resources Professionals.
- Operations and Facility Managers.
- Emergency Services and Public Sector Officials.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Information Technology and Telecommunications.
- Energy, Oil, and Gas.
- Government Agencies and Public Administration.
- Manufacturing and Supply Chain.
- Retail and E-commerce.
- Transportation and Logistics.
- Education and Research Institutions.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology and Cybersecurity.
- Corporate Communications and Public Relations.
- Risk Management and Compliance.
- Legal and General Counsel.
- Operations Management.
- Executive Leadership and C-Suite.
- Human Resources.
- Facilities and Physical Security.
- Business Continuity Planning.
- Internal Audit.

Course Offerings:

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

- Develop and implement a comprehensive incident response plan based on industry frameworks.
- Establish and manage an effective Computer Security Incident Response Team (CSIRT).
- Master the phases of the incident response lifecycle from preparation to post-incident analysis.
- Conduct thorough risk assessments to identify potential threats and vulnerabilities.
- Formulate and execute a strategic crisis communication plan for internal and external stakeholders.
- Lead with authority and make critical decisions under the pressure of a crisis.
- Manage media relations and control the narrative during a high-stakes event.
- Integrate incident response efforts with business continuity and disaster recovery plans.
- Conduct effective post-mortem reviews to drive continuous improvement.
- Ensure legal and regulatory compliance during incident handling and reporting.

Course Methodology:

This training course employs a dynamic and interactive learning methodology designed for maximum knowledge retention and practical application. At BIG BEN Training Center, we believe in learning by doing. The program is built around a blend of expert-led instruction, real-world case study analysis, and collaborative group discussions. A significant portion of the course is dedicated to hands-on, practical exercises, including tabletop simulations that challenge participants to respond to realistic incident and crisis scenarios in a controlled environment. These interactive sessions allow attendees to apply theoretical concepts, test their decision-making skills, and refine their response strategies. Participants will receive continuous feedback from experienced instructors and peers, fostering a rich learning environment. The methodology emphasizes teamwork, critical thinking, and problem-solving, ensuring that delegates leave not just with knowledge, but with the confidence and competence to lead their organizations through any disruptive event.

Course Agenda (Course Units):

Unit One: Foundations of Incident and Crisis Management

- Defining the difference between an incident, a crisis, and a disaster.
- Understanding the complete incident response lifecycle.
- Exploring key frameworks like NIST (National Institute of Standards and Technology) and SANS.
- The strategic importance of integrating incident response with business goals.
- Establishing the goals of a crisis management program.
- Legal, regulatory, and ethical considerations in incident handling.
- Introduction to building a culture of preparedness and resilience.

Unit Two: Preparedness and Proactive Planning

- Conducting comprehensive risk assessments and business impact analysis (BIA).
- Developing a robust Incident Response Plan (IRP).
- Forming and training the Computer Security Incident Response Team (CSIRT).
- Creating a strategic Crisis Management Plan (CMP).
- Identifying and preparing the Crisis Management Team (CMT).
- Developing pre-approved communication templates and protocols.
- Planning and executing effective training and awareness programs.

Unit Three: Incident Detection, Analysis, and Containment

- Techniques for effective incident detection and monitoring.
- Initial incident analysis, scoping, and prioritization.
- Strategies for evidence gathering and preservation (chain of custody).
- Implementing short-term and long-term containment strategies.
- Threat intelligence and its role in incident analysis.
- Coordinating with internal teams and external agencies.
- Documenting incident details accurately for future analysis.

Unit Four: Eradication, Recovery, and Post-Incident Learning

- Developing a systematic approach to eradicating threats from the environment.
- Validating the complete removal of the incident cause.
- Executing recovery procedures to restore systems and operations safely.
- Prioritizing recovery efforts based on the business impact analysis.
- Conducting a thorough post-incident review or post-mortem.
- Identifying lessons learned and creating actionable improvement plans.
- Updating response plans and security controls based on findings.

Unit Five: Strategic Crisis Communication and Leadership

- Activating the Crisis Management Plan and Team.
- The principles of effective leadership during a crisis.
- Developing and executing a crisis communication strategy.
- Managing internal and external stakeholder communications.
- Engaging with the media and managing public perception.
- Techniques for de-escalating situations and managing stress.
- Integrating crisis management with business continuity and long-term recovery.

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 rapid disinformation, how can an organization's crisis communication plan remain agile enough to protect its reputation without compromising legal or operational integrity?

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

This course distinguishes itself by offering a holistic and integrated curriculum that bridges the critical gap between technical incident response and strategic crisis management. While many programs focus solely on the IT-centric aspects of handling a breach, our approach recognizes that every technical incident has the potential to become a business-wide crisis affecting reputation, stakeholder trust, and financial stability. We emphasize the development of leadership and communication skills alongside technical competencies, preparing participants not just to fix a problem, but to lead an organization through turmoil. The curriculum is heavily weighted towards practical application, moving beyond theory with immersive tabletop exercises and simulations based on current, real-world events. This hands-on methodology ensures that participants develop muscle memory for critical decision-making under pressure. By focusing on the strategic alignment of response efforts with overarching business objectives, the course equips professionals with a comprehensive perspective, enabling them to protect and even enhance organizational resilience in the face of adversity.