Cybersecurity Incident Response and Crisis Communication Training Course

02 - 06 Nov 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #IT3157_202750

Course Introduction / Overview:

In today's hyper-connected digital landscape, the question is not if an organization will face a cybersecurity incident, but when. The effectiveness of the response determines the extent of the damage, from financial loss to reputational ruin. This comprehensive training course is meticulously designed to bridge the critical gap between technical incident response and strategic crisis communication. It moves beyond theoretical frameworks to provide actionable strategies for managing the entire lifecycle of a security breach. As noted by cybersecurity expert Kevin Mandia, a pioneer in incident response, preparation is paramount. This course, offered by BIG BEN Training Center, instills the principles outlined in seminal works like "Incident Response & Computer Forensics," ensuring participants can not only contain a technical threat but also manage the narrative, maintain stakeholder trust, and protect the organization's brand. We will explore everything from initial detection and digital forensics to crafting press releases and briefing executive leadership. This program equips professionals with a dual-pronged skill set, enabling them to navigate the complexities of a modern cyber crisis with confidence, resilience, and strategic foresight, transforming a potential catastrophe into a managed event.

Target Audience / This training course is suitable for:

- Incident Response Team Members.
- IT Security Managers and Analysts.
- Public Relations and Corporate Communications Professionals.
- Legal and Compliance Officers.
- Risk Management Personnel.
- Executive Leadership and C-Suite Members (CEO, CIO, CISO).
- Business Continuity and Disaster Recovery Planners.
- IT Auditors and Consultants.
- Human Resources Managers.
- Customer Support and Service Managers.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Government and Public Sector Agencies.
- Technology and Telecommunications.
- Retail and E-commerce.

- Energy and Utilities.
- Manufacturing and Industrial Control Systems.
- Education and Research Institutions.
- Consulting and Professional Services.

Target Organizations Departments:

- Information Technology and Information Security.
- Public Relations and Corporate Communications.
- Legal and Regulatory Compliance.
- Executive Management and Board of Directors.
- Risk Management.
- Internal Audit.
- Human Resources.
- Customer Relations and Support.
- Operations.

Course Offerings:

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

- Develop and implement a comprehensive cybersecurity incident response plan based on industry frameworks like NIST.
- Master the incident response lifecycle from preparation and detection to containment, eradication, and recovery.
- Conduct initial digital forensic analysis to identify the scope and nature of a security breach.
- Create a strategic crisis communication playbook tailored to various cybersecurity incident scenarios.
- Manage media relations and control the public narrative during a high-pressure cyber crisis.
- Effectively communicate with all stakeholders, including employees, customers, regulators, and the board.
- Lead and participate in tabletop exercises to test and refine incident response and communication plans.
- Understand the key legal, regulatory, and compliance obligations associated with data breaches.
- Perform a thorough post-incident analysis to identify root causes and implement lessons learned.
- Align technical response efforts with communication strategies to protect organizational reputation.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants gain tangible skills they can apply immediately. This course moves beyond traditional lectures by integrating a blended learning approach. A significant portion of the training is dedicated to hands-on, scenario-based learning, including realistic tabletop exercises that simulate a live cyber crisis. Participants will work in teams to manage a developing incident, making critical decisions under pressure and experiencing the interplay between technical response and public relations. The curriculum is enriched with detailed case studies of real-world data breaches, allowing for in-depth analysis of what went right and what went wrong. Facilitated group discussions, expert-led presentations, and

interactive Q&A sessions encourage collaborative problem-solving and knowledge sharing. Participants will receive continuous feedback from experienced instructors, helping them to refine their incident response plans and crisis communication messages. This dynamic and engaging approach ensures a deep understanding of both the technical and strategic components of managing cybersecurity incidents effectively.

Course Agenda (Course Units)

Unit One: Foundations of Integrated Incident Management

- Introduction to Cybersecurity Incident Response.
- The Incident Response Lifecycle: Preparation, Detection, Analysis, Containment, Eradication, and Recovery.
- Understanding Key Frameworks: NIST, ISO 27001, and SANS.
- Building the Cyber Incident Response Team (CIRT) and Defining Roles.
- The Critical Role of Crisis Communication in Incident Response.
- Mapping Stakeholders and Understanding Their Communication Needs.
- Legal and Regulatory Compliance Landscape for Data Breaches.

Unit Two: Technical Investigation and Containment

- Incident Detection and Triage Techniques.
- Fundamentals of Network and Host-Based Forensics.
- Log Analysis for Security Incident Investigation.
- Malware Analysis and Reverse Engineering Basics.
- Containment Strategies to Limit Damage and Prevent Spread.
- Eradication of Threats and Securing Affected Systems.
- Recovery Planning and Business Continuity Integration.

Unit Three: Developing the Crisis Communication Strategy

- Principles of Effective Crisis Communication.
- Creating a Scalable Crisis Communication Plan and Playbook.
- Crafting Clear, Consistent, and Empathetic Key Messages.
- Identifying and Training a Crisis Communication Team and Spokespersons.
- Managing Internal Communications to Inform and Reassure Employees.
- Proactive vs. Reactive Communication Approaches.
- Utilizing Communication Channels Effectively During a Crisis.

Unit Four: Managing External Communications and Reputation

- Handling Media Inquiries and Conducting Press Briefings.
- Managing the Narrative on Social Media and Digital Platforms.
- Communicating with Customers and Business Partners.
- Engaging with Regulators, Law Enforcement, and Government Agencies.
- Reputation Management and Rebuilding Trust Post-Incident.

- Monitoring Public Sentiment and Countering Misinformation.
- Case Studies: Analyzing Communication Successes and Failures.

Unit Five: Integrated Simulation and Post-Incident Excellence

- Full-Scale Tabletop Exercise: Responding to a Simulated Cyber Attack.
- Integrating Technical and Communication Responses in Real-Time.
- Executive and Board-Level Briefing Practice.
- Conducting a Thorough Post-Incident Review and Root Cause Analysis.
- Documenting Lessons Learned and Driving Continuous Improvement.
- Updating and Refining Incident Response and Communication Plans.
- The Future of Incident Response and Emerging Threats.

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 a major data breach, where does the ethical line lie between full transparency with the public and the strategic withholding of information to prevent further exploitation by threat actors?

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

This course distinguishes itself by holistically integrating the technical discipline of cybersecurity incident response with the strategic art of crisis communication, a synergy often neglected in specialized training programs. While many courses focus on either the digital forensics of an attack or the public relations strategy, this program is built on the principle that the two are inseparable for successful crisis management. We move beyond theoretical knowledge by immersing participants in high-fidelity tabletop exercises that simulate the pressure and complexity of a real-world breach, forcing them to make coordinated technical and communicative decisions. The curriculum emphasizes the development of a unified playbook, ensuring that the actions of the IT security team are perfectly aligned with the messaging delivered to stakeholders. Rather than just teaching how to use specific tools, we focus on cultivating critical thinking and strategic leadership. The insights provided are drawn from deep analysis of real-world case studies, focusing on the decision-making processes that determine whether an organization weathers a cyber storm or suffers irreparable reputational damage.