Executive Cyber Security and Boardroom Communication Training Course

14 - 18 Dec 2026

Rome

5800 € (Per Person)

Ref: #CYB8091_88860

Course Introduction / Overview:

In today's hyper-connected digital landscape, cybersecurity has evolved from a technical IT issue into a critical boardroom-level concern that directly impacts business strategy, financial stability, and corporate reputation. This advanced program is meticulously designed for senior leaders and board members who are responsible for organizational oversight and strategic direction. The course demystifies complex cybersecurity concepts, translating them into the language of business risk and opportunity. As highlighted by experts like Peter W. Singer in his influential book "Cybersecurity and Cyberwar: What Everyone Needs to Know", understanding the strategic implications of cyber threats is no longer optional for leadership. This training course from BIG BEN Training Center provides a comprehensive framework for establishing robust cybersecurity governance, managing cyber risk effectively, and fostering a culture of security throughout the organization. Participants will move beyond technical jargon to master the art of boardroom communication, enabling them to ask the right questions, challenge assumptions, and make informed decisions that build long-term cyber resilience and secure the organization's future.

Target Audience / This training course is suitable for:

- Board Members and Directors.
- C-Level Executives (CEO, CFO, COO, CIO).
- Chief Information Security Officers (CISOs) and IT Directors.
- Senior Vice Presidents and Business Unit Leaders.
- Risk, Compliance, and Legal Officers.
- Corporate Governance Professionals.
- Senior government officials and policymakers.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Energy, Oil, and Gas.
- Telecommunications and Technology.
- Government Agencies and Public Sector Organizations.
- Retail and E-commerce.
- Manufacturing and Critical Infrastructure.
- Professional Services and Consulting.

Target Organizations Departments:

- Executive Leadership and C-Suite.
- Board of Directors.
- Information Technology and Information Security.
- Risk Management and Corporate Governance.
- Legal and Compliance.
- Internal Audit and Assurance.
- Corporate Communications and Public Relations.
- Strategic Planning and Business Development.

Course Offerings:

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

- Translate complex technical cyber threats into clear business impact and financial risk.
- Develop and implement a comprehensive cybersecurity governance framework.
- Define and articulate the organization's cyber risk appetite to stakeholders.
- Master communication techniques for presenting cybersecurity matters to the board.
- Lead effectively during a significant cyber incident or data breach.
- Evaluate the ROI of cybersecurity investments and align them with business objectives.
- Navigate the complex landscape of cybersecurity regulations and compliance requirements.
- Foster a proactive, security-first culture across all levels of the organization.
- Critically assess and manage third-party and supply chain cyber risks.
- Formulate a strategic vision for long-term organizational cyber resilience.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and directly applicable to the challenges faced by senior leaders. This course moves beyond traditional lectures to create a dynamic learning environment centered on strategic thinking and practical application. A cornerstone of our approach is the extensive use of real-world case studies, analyzing major corporate cyber breaches from a leadership and governance perspective to extract actionable lessons. Participants will engage in simulated boardroom meetings where they must debate cybersecurity investment proposals, respond to breach scenarios, and craft communication strategies under pressure. These interactive sessions, facilitated by expert instructors, encourage peer-to-peer learning and the sharing of diverse industry experiences. Group discussions, strategic planning exercises, and practical workshops on risk assessment and communication ensure that theoretical concepts are firmly grounded in the realities of executive decision-making. Continuous feedback and guided reflection are integrated throughout the program, empowering participants to immediately apply their new skills and strategic insights within their own organizations.

Course Agenda (Course Units):

Unit One: The Strategic Cyber Landscape for Executive Leaders

- The evolution of cyber threats from technical problems to business-critical risks.
- Understanding the motivations and methods of modern threat actors.
- Analyzing the financial and reputational impact of high-profile data breaches.
- The intersection of cybersecurity with corporate strategy and digital transformation.
- Fundamentals of strategic threat intelligence for non-technical leaders.
- Defining cybersecurity as a driver of business enablement and competitive advantage.
- Case Study Analysis: A major corporate breach and its boardroom fallout.

Unit Two: Cybersecurity Governance and Risk Management Frameworks

- Establishing clear roles and responsibilities for the board and C-suite.
- Key principles of effective cybersecurity governance.
- Implementing frameworks like the NIST Cybersecurity Framework (CSF) and ISO 27001.
- Defining and managing the organization's cyber risk appetite.
- Navigating the global landscape of data privacy and security regulations.
- The board's oversight responsibility in vendor and supply chain risk management.
- Developing key performance indicators (KPIs) and metrics for cybersecurity.

Unit Three: Building a Cyber-Resilient and Security-Aware Organization

- Developing a comprehensive, business-aligned cybersecurity strategy.
- The economics of cybersecurity: Budgeting and demonstrating return on investment (ROI).
- Fostering a strong security culture from the boardroom to the front line.
- Key considerations for securing cloud adoption, IoT, and emerging technologies.
- Strategies for attracting, developing, and retaining top cybersecurity talent.
- The role of cyber insurance in a holistic risk management program.
- Conducting effective cybersecurity drills and tabletop exercises for leadership.

Unit Four: The Art of Boardroom and Stakeholder Communication

- Translating technical jargon into the language of business risk and opportunity.
- Crafting compelling narratives to secure board buy-in for security initiatives.
- Designing effective cybersecurity dashboards and reports for an executive audience.
- Techniques for presenting complex risk scenarios with clarity and impact.
- Communicating with investors, regulators, and customers about cybersecurity posture.
- Managing internal communications to build trust and awareness.
- Workshop: Developing and presenting a cybersecurity business case to a mock board.

Unit Five: Executive Leadership in Crisis and Incident Response

- The executive's critical role before, during, and after a cyber incident.
- Fundamentals of a strategic crisis management and communication plan.
- Making critical decisions under pressure with incomplete information.
- Engaging with legal counsel, forensic investigators, and public relations teams.
- Managing regulatory disclosure requirements and potential liabilities.
- Leading the post-incident review to drive organizational learning and improvement.
- Simulation Exercise: Navigating a complex data breach scenario from the C-suite.

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 can a board effectively balance the drive for digital innovation with the imperative of robust cyber risk oversight?

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

This training course distinguishes itself by being exclusively designed for the strategic mindset of senior executives and board members, deliberately avoiding deeply technical jargon. Unlike programs that focus on the "how" of cybersecurity implementation, this course concentrates on the "why" and "so what" from a business leadership perspective. Its core value lies in bridging the critical communication gap between technical security teams and the boardroom. The curriculum is built around interactive, high-stakes simulations and case studies that mirror the complex, real-world decisions leaders face, rather than passive lectures. Participants learn not just what questions to ask their CISO, but how to interpret the answers in the context of business risk, financial impact, and strategic goals. The emphasis on communication, governance, and crisis leadership provides a unique and holistic skill set, empowering attendees to steer their organizations with confidence and build true, sustainable cyber resilience that is woven into the fabric of the corporate strategy, not just bolted on as an IT function.