Executive CISO Leadership for Modern Cybersecurity Training Course

14 - 18 Dec 2026

Milan

5900 € (Per Person)

Ref: #CYB5630_88206

Course Introduction / Overview:

The role of the Chief Information Security Officer (CISO) has evolved from a technical manager to a strategic business leader. This transformation demands a unique blend of deep technical knowledge, business acumen, and exceptional leadership skills. The Executive CISO Leadership for Modern Cybersecurity Training Course is meticulously designed to equip current and aspiring security executives with the comprehensive capabilities needed to navigate this complex landscape. As highlighted by cybersecurity expert and author Todd Fitzgerald in his book "CISO's Guide to Success", the modern CISO must be a master of communication, a strategic thinker, and a driver of organizational change. This course delves into these core competencies, moving beyond theoretical concepts to provide practical, actionable strategies for developing robust security programs, managing risk effectively, and aligning cybersecurity initiatives with overarching business objectives. At BIG BEN Training Center, we provide a learning environment that fosters the development of these critical skills, ensuring participants can confidently lead their organizations' defense against sophisticated cyber threats while enabling business innovation and growth. This program is your definitive roadmap to becoming a successful and influential CISO in today's dynamic digital world.

Target Audience / This training course is suitable for:

- Aspiring Chief Information Security Officers (CISOs).
- Current CISOs seeking to enhance their strategic leadership skills.
- Directors and Senior Managers of Information Security.
- IT Security and Cybersecurity Managers.
- Risk and Compliance Managers.
- Senior IT Leaders with security responsibilities.
- Business executives who want to understand cybersecurity leadership.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical.
- Technology and Telecommunications.
- Government and Public Sector Agencies.
- Retail and E-commerce.
- Energy and Utilities.
- Consulting and Professional Services.
- Manufacturing and Industrial Control Systems.

Target Organizations Departments:

- Information Technology (IT).
- Information Security and Cybersecurity.
- Risk Management.
- Compliance and Legal.
- Internal Audit.
- Executive Management.
- Operations.

Course Offerings:

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

- Develop and implement a comprehensive, business-aligned cybersecurity strategy.
- Master the principles of Governance, Risk, and Compliance (GRC) frameworks.
- Effectively communicate cybersecurity risks and strategies to the board and executive leadership.
- Lead and manage high-performing cybersecurity teams.
- Build and foster a strong security-aware culture throughout the organization.
- Develop and manage a strategic cybersecurity budget.
- Lead incident response and crisis management efforts with confidence.
- Evaluate and manage third-party and supply chain security risks.
- Navigate the legal and regulatory landscape of cybersecurity and data privacy.
- Align security initiatives with digital transformation and business innovation goals.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical, ensuring that participants can immediately apply their learning in a real-world context. We believe that executive leadership skills are best developed through active participation and collaborative problem-solving. The course combines expert-led instruction with a variety of engaging learning techniques. Participants will analyze real-world case studies of security breaches and successful CISO strategies, allowing them to dissect complex scenarios and understand the decision-making process at an executive level. Interactive group discussions and workshops encourage the sharing of diverse perspectives and experiences, enriching the learning for all attendees. Practical exercises and simulation activities will challenge participants to develop security roadmaps, present risk assessments to a mock board, and formulate incident response plans. Continuous feedback from the instructor and peers is a cornerstone of our approach, helping participants refine their leadership and communication styles. This blended learning environment ensures a deep and lasting understanding of the strategic responsibilities of a modern CISO.

Course Agenda (Course Units):

Unit One The Strategic CISO and Cybersecurity Governance

- The Evolution of the CISO Role from Technical Manager to Business Leader.
- Defining the Mission, Vision, and Strategy for a Cybersecurity Program.
- Developing a Comprehensive Cybersecurity Strategy Aligned with Business Goals.
- Understanding and Implementing Cybersecurity Governance Frameworks (NIST, ISO 27001).
- Establishing Key Performance Indicators (KPIs) and Metrics for Security.
- The CISO's Role in Corporate Governance and Digital Transformation.
- Legal, Ethical, and Professional Responsibilities of a CISO.

Unit Two Mastering Risk Management and Compliance

- Fundamentals of Information Security Risk Management.
- Conducting Business Impact Analysis (BIA) and Risk Assessments.
- Developing and Implementing a Risk Treatment and Mitigation Plan.
- Navigating the Global Regulatory Landscape (GDPR, CCPA, etc.).
- Building and Managing an Integrated Compliance Program.
- Third-Party and Supply Chain Risk Management Strategies.
- Communicating Risk Effectively to Technical and Non-Technical Stakeholders.

Unit Three Technical Leadership and Security Operations

- Overseeing Security Architecture and Engineering Functions.
- Leading a Modern Security Operations Center (SOC).
- Developing a Proactive Threat Intelligence Program.
- Mastering Incident Response and Crisis Management Leadership.
- Integrating Security into the Software Development Lifecycle (DevSecOps).
- Evaluating and Implementing Emerging Security Technologies.
- Managing Cloud Security Governance and Strategy.

Unit Four Building a Security-Centric Culture and High-Performing Teams

- The Psychology of Security Awareness and Human-Centric Security.
- Developing and Executing an Effective Security Awareness and Training Program.
- Strategies for Recruiting, Retaining, and Developing Cybersecurity Talent.
- Leading and Motivating Diverse and Geographically Distributed Security Teams.
- Managing Team Performance and Fostering a Culture of Continuous Improvement.
- Conflict Resolution and Influential Leadership within the Organization.
- Championing Security as a Shared Responsibility Across All Departments.

Unit Five Business Acumen and Board-Level Engagement

- Translating Technical Risk into Business Impact and Financial Terms.
- Developing, Justifying, and Managing the Cybersecurity Budget.
- Crafting Compelling Presentations for the Board of Directors and C-Suite.
- Building Strategic Alliances with Key Business Leaders (CEO, CFO, CIO).
- Negotiation and Vendor Management Skills for Security Leaders.
- The CISO's Role in Mergers and Acquisitions (M&A).
- Preparing for the Future of Cybersecurity and CISO Leadership.

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 digital transformation, how can a CISO champion security as a business enabler rather than a restrictive cost center?

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

This course distinguishes itself by focusing on the CISO's role as a strategic business partner, not just a technical guardian. While many programs concentrate solely on technical security domains or specific compliance frameworks, our curriculum integrates the three critical pillars of modern CISO success: strategic governance, technical leadership, and business acumen. We move beyond theory to immerse participants in real-world scenarios that challenge their decision-making, communication, and leadership skills. The content is designed to cultivate the executive presence required to effectively engage with boards of directors, justify security investments in financial terms, and build a pervasive culture of security. Unlike courses that offer a siloed view, we emphasize the interconnectedness of risk, compliance, operations, and business strategy. The focus on developing soft skills—such as influence, negotiation, and crisis communication—alongside hard skills ensure our participants are not just prepared to manage a security program, but to lead an organization through its most significant cybersecurity challenges and opportunities, positioning security as a key driver of business resilience and growth.