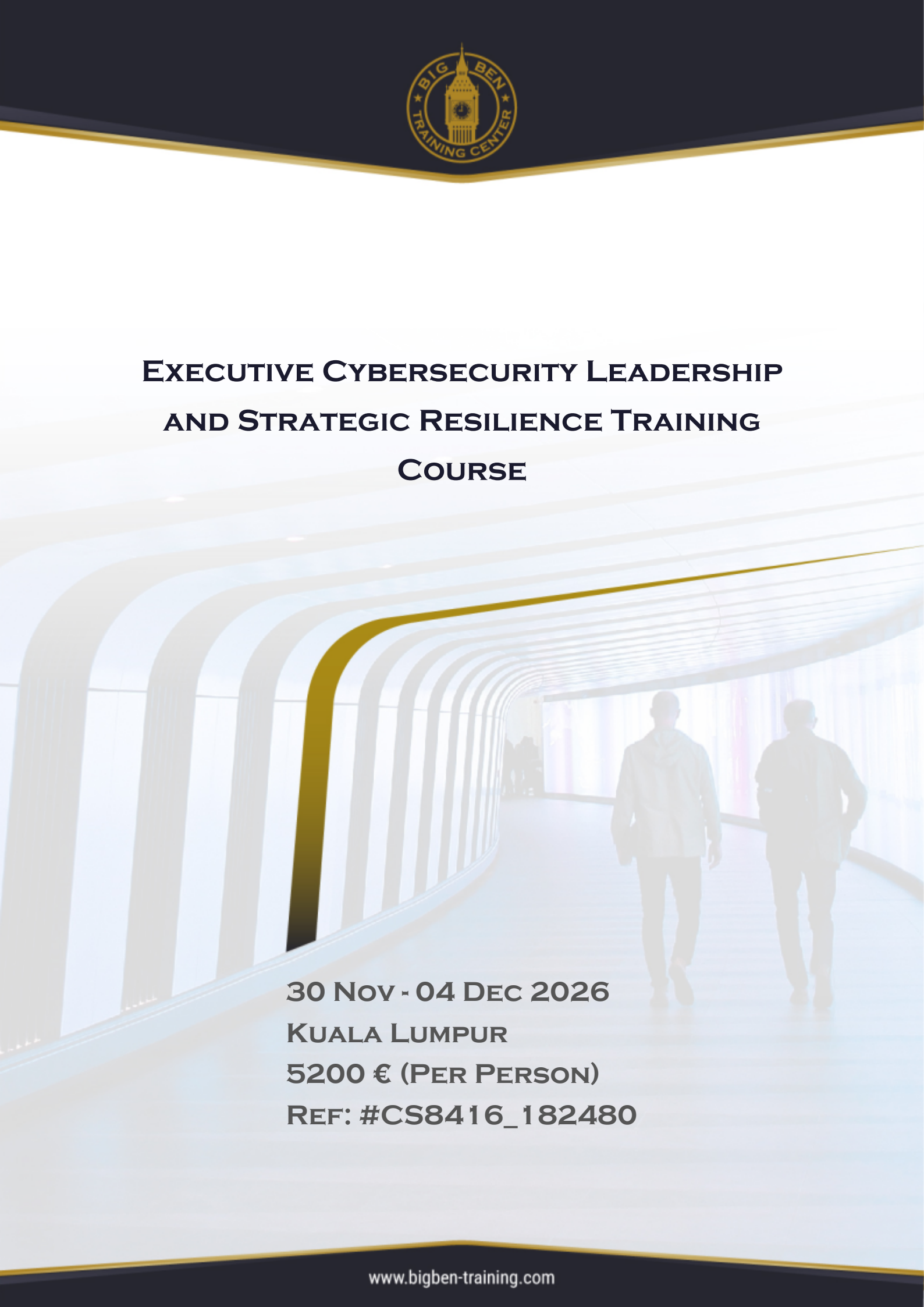
Executive Cybersecurity Leadership and Strategic Resilience Training Course



30 Nov - 04 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #CS8416_182480

Course Introduction / Overview:

In today's hyper-connected digital ecosystem, cybersecurity has transcended its traditional role as an IT function to become a critical pillar of executive leadership and corporate governance. This training course is meticulously designed for senior leaders who are the ultimate custodians of organizational value and reputation. It addresses the paradigm shift from reactive defense to proactive strategic resilience. We will explore the principles articulated by renowned security expert Bruce Schneier, who emphasizes that security is a process, not a product. Drawing inspiration from concepts in his book "Data and Goliath," the course delves into the complex interplay between technology, business strategy, and human factors. Participants will learn to navigate the intricate landscape of cyber threats, not as technical experts, but as strategic decision-makers. BIG BEN Training Center has developed this program to empower executives with the foresight to anticipate threats, the acumen to manage cyber risk as a core business function, and the leadership to foster a pervasive culture of security that underpins sustainable growth and innovation. This is not just a course about preventing breaches; it is a masterclass in leading an organization with confidence and resilience in the face of persistent cyber adversity.

Target Audience / This training course is suitable for:

- Chief Executive Officers (CEOs).
- Chief Information Officers (CIOs) and Chief Technology Officers (CTOs).
- Chief Information Security Officers (CISOs).
- Chief Financial Officers (CFOs) and Chief Operating Officers (COOs).
- Board of Directors and Audit Committee Members.
- Senior Vice Presidents and Vice Presidents.
- Heads of Legal, Risk, and Compliance Departments.
- Senior Government Officials and Public Sector Leaders.
- Aspiring C-suite executives and senior managers.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Energy, Utilities, and Critical Infrastructure.
- Technology and Telecommunications.
- Retail and E-commerce.
- Manufacturing and Industrial Control Systems.
- Government Agencies and Public Sector Organizations.
- Consulting and Professional Services.
- Transportation and Logistics.

Target Organizations Departments:

- Executive Management and Board of Directors.
- Information Technology and Information Security.
- Risk Management and Corporate Strategy.
- Legal and Compliance.
- Internal Audit and Governance.
- Operations and Business Continuity Planning.
- Finance and Investment.
- Human Resources.
- Corporate Communications and Public Relations.

Course Offerings:

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

- Develop a comprehensive cybersecurity governance framework aligned with business objectives.
- Articulate and manage the organization's cyber risk appetite effectively.
- Evaluate and justify strategic cybersecurity investments and calculate their return on investment.
- Lead with confidence and clarity during a high-stakes cyber incident.
- Foster a robust, security-aware culture throughout the entire organization.
- Understand and navigate the complex legal, regulatory, and compliance landscape.
- Assess and mitigate third-party and supply chain cyber risks.
- Communicate effectively with the board, stakeholders, and the public on cybersecurity matters.
- Integrate cybersecurity considerations into digital transformation and innovation initiatives.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum engagement and practical application, moving beyond theoretical lectures to foster true leadership capabilities. This course employs a blended learning approach centered on executive-level problem-solving. A significant portion of the program is dedicated to interactive tabletop exercises and sophisticated crisis simulations, where participants will navigate realistic cyber-attack scenarios in a controlled environment. We will utilize the case study method to deconstruct high-profile corporate breaches, analyzing the strategic decisions, communication failures, and recovery efforts of affected organizations. Facilitated group discussions and peer-to-peer learning will allow leaders to share insights and benchmark their own organizational practices against industry best standards. Expert-led sessions will break down complex topics like threat intelligence, cyber law, and risk quantification into actionable business language. Participants will work on developing practical artifacts, such as a draft incident response communication plan or a board-level reporting dashboard, ensuring that the skills learned are directly transferable to their professional roles. Our focus is on building strategic muscle memory for leading through cyber adversity.

Course Agenda (Course Units):

Unit One: The Executive's View of the Cyber Threat Landscape

- The Evolving Role of Leadership in Cybersecurity Governance.
- Understanding the Business Impact of Modern Cyber Threats.
- Key Cybersecurity Frameworks (NIST, ISO 27001) for Strategic Oversight.
- Defining and Communicating Cyber Risk Appetite to the Board.
- Threat Intelligence for Strategic Decision-Making.
- The Intersection of Corporate Strategy and Cyber Strategy.
- Analyzing State-Sponsored Threats and Corporate Espionage.

Unit Two: Building a Strategically Resilient Organization

- Developing a Top-Down Cybersecurity Culture.
- The CISO, the CEO, and the Board, a Strategic Partnership.
- Crafting and Implementing Effective Cybersecurity Policies.
- Integrating Security into the Digital Transformation Lifecycle.
- Building a Human Firewall, Training and Awareness Programs for the Entire Workforce.
- Key Performance Indicators (KPIs) and Metrics for a Board-Level Dashboard.
- Supply Chain and Third-Party Risk Management (TPRM) Strategies.

Unit Three: Financial, Legal, and Regulatory Imperatives

- The Economics of Cybersecurity, Budgeting and Proving ROI.
- Navigating the Global Landscape of Data Privacy Regulations (GDPR, CCPA).
- Directors' and Officers' Liability in the Context of a Cyber Breach.
- The Role and Strategy of Cyber Insurance.
- Cybersecurity Considerations in Mergers and Acquisitions (M&A).
- Reporting Requirements for Publicly Traded Companies.
- Managing Relationships with Regulators and Law Enforcement.

Unit Four: Leadership in Times of Crisis

- Anatomy of a Cyber Crisis, from Detection to Resolution.
- Developing a Business-Focused Incident Response Plan.
- The Leader's Role During a High-Stakes Cyber Incident.
- Mastering Crisis Communication with Stakeholders, Media, and Employees.
- Business Continuity and Disaster Recovery Planning.
- Leading Post-Breach Remediation and Recovery Efforts.
- Conducting Effective Post-Mortem Analyses to Foster Improvement.

Unit Five: Future-Proofing the Organization's Security Posture

- Emerging Threats, AI, Quantum Computing, and IoT Security.
- Implementing a Zero Trust Architecture from a Strategic Perspective.
- The Future of Cybersecurity Talent Management and Retention.
- Building Public-Private Partnerships for Enhanced Security.
- Ethical Considerations in Cybersecurity and Data Usage.
- Fostering a Culture of Continuous Security Improvement and Adaptation.
- The Final Challenge, A Comprehensive Executive Crisis Simulation.

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 state-sponsored cyber-attacks and AI-driven threats, how can a leader balance aggressive innovation with the non-negotiable need for robust cyber defense?

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

This course distinguishes itself by being exclusively tailored for the strategic mindset of senior executives and board members, deliberately avoiding deeply technical jargon and implementation details. Unlike many cybersecurity courses that focus on the "how" for IT professionals, our curriculum is centered on the "why" and "what" for business leaders. The core emphasis is on governance, risk, financial implications, and leadership during a crisis, treating cybersecurity as a fundamental business enabler rather than a technological problem. A key differentiator is our extensive use of sophisticated, real-time crisis simulations that replicate the intense pressure and complex decision-making environment of a major cyber-attack. This experiential learning is complemented by case studies of boardroom responses to iconic breaches, providing unparalleled insight into successful and unsuccessful leadership strategies. Furthermore, the program fosters a unique peer-learning environment, allowing senior leaders from diverse industries to benchmark strategies and build a valuable professional network. The focus is not on tools, but on the strategic frameworks and leadership acumen required to build a truly resilient organization.