Cyber Resilience in the Financial Services Sector Training Course



30 Nov - 04 Dec 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #BI6961_176702

Course Introduction / Overview:

The financial services sector operates at the heart of the global economy, making it a prime target for sophisticated cyber-attacks that threaten not just individual institutions but systemic stability. This intensive training course is meticulously designed to move beyond traditional cybersecurity measures, focusing instead on building comprehensive cyber resilience. As articulated by security expert Ross Anderson in his seminal work, "Security Engineering: A Guide to Building Dependable Distributed Systems," true security is about creating systems that are not just hard to break, but that behave gracefully when they do. This principle is the cornerstone of our curriculum. Participants will explore the intricate threat landscape unique to finance, from state-sponsored actors to insider threats, and learn to develop proactive, adaptive, and robust defense strategies. BIG BEN Training Center has structured this program to equip professionals with the strategic foresight and practical skills needed to protect critical financial infrastructure, manage regulatory complexities, and lead their organizations through crisis with minimal disruption. This course provides a holistic framework for embedding resilience into the fabric of an organization's culture, technology, and operations, ensuring long-term viability in an era of persistent cyber threats.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs) and security leadership.
- IT Security Managers and Analysts.
- Risk Management Professionals.
- Compliance and Audit Officers.
- Financial Operations Managers.
- Business Continuity and Disaster Recovery Planners.
- IT Architects and System Administrators in financial institutions.
- Regulatory and policy-making professionals in the financial sector.

Target Sectors and Industries:

- Commercial and retail banking.
- Investment banking and asset management.
- Insurance and reinsurance companies.
- Financial technology (FinTech) and payment processing firms.
- Credit unions and cooperative banks.
- Securities and commodities trading firms.
- Government financial regulatory bodies and central banks.
- Private equity and venture capital firms.

Target Organizations Departments:

- Information Technology and Cybersecurity.
- Risk Management and Corporate Governance.
- Compliance and Legal.
- Internal Audit.
- Operations and Business Units.
- Treasury and Finance.
- Crisis Management and Corporate Communications.

Course Offerings:

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

- Develop and implement a strategic cyber resilience framework tailored to the financial sector.
- Analyze the specific threat landscape and attack vectors targeting financial institutions.
- Master regulatory compliance requirements such as FFIEC, NYDFS, and GDPR within a cybersecurity context.
- Conduct comprehensive cybersecurity risk assessments and manage third-party vendor risk effectively.
- Design and execute robust incident response and recovery plans to minimize operational impact.
- Integrate threat intelligence into a proactive defense strategy.
- Evaluate and secure emerging technologies like cloud computing and blockchain in a financial context.
- Foster a strong, security-aware culture throughout the organization.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum engagement and practical application, recognizing that cyber resilience is built through experience, not just theory. This course employs a blended learning approach that combines expert-led instruction with highly interactive sessions. Participants will delve into real-world case studies of major financial sector breaches, dissecting the attack chains, the institutional response, and the lessons learned. A significant portion of the training is dedicated to collaborative workshops and group exercises, where attendees will work together to develop risk matrices, draft incident response communications, and simulate board-level crisis meetings. These activities are designed to foster critical thinking and strategic decision-making under pressure. The course also features simulation exercises that model realistic cyber-attack scenarios, allowing participants to apply their new skills in a controlled, safe environment. Continuous feedback from the instructor and peers is a core component, ensuring that participants can refine their understanding and approach throughout the five-day program. Our goal is to create a dynamic learning environment that transforms knowledge into actionable capability.

Course Agenda (Course Units):

Unit One: Foundations of Financial Cyber Resilience

- The Evolving Threat Landscape in Financial Services.
- Distinguishing Between Cybersecurity and Cyber Resilience.
- Core Principles of a Cyber Resilience Framework.
- Key Regulatory and Compliance Mandates (FFIEC, NYDFS, PRA, MAS).
- Understanding Systemic Risk and Financial Stability Implications.
- The Role of Governance, Risk, and Compliance (GRC) in Resilience.
- Case Study Analysis of a Major Financial Institution Breach.

Unit Two: Strategic Risk Management and Governance

- Developing a Cyber Risk Appetite Statement.
- Advanced Cybersecurity Risk Assessment Methodologies.
- Third-Party and Supply Chain Risk Management.
- Building an Effective Cybersecurity Governance Structure.
- The Role of the Board of Directors and Senior Management.
- Integrating Cyber Resilience into Enterprise Risk Management (ERM).
- Metrics and Key Risk Indicators (KRIs) for Measuring Resilience.

Unit Three: Proactive Defense and Threat Intelligence

- Building a Proactive Threat Hunting Capability.
- Leveraging Financial Services Threat Intelligence Sharing (FS-ISAC).
- Implementing Advanced Threat Detection and Analytics.
- Security Orchestration, Automation, and Response (SOAR).
- Vulnerability Management and Penetration Testing Strategies.
- Protecting Critical Functions and Crown Jewel Assets.
- Threat Modeling for Financial Applications and Systems.

Unit Four: Incident Response and Crisis Management

- Developing a Financial Sector-Specific Incident Response Plan.
- Leading and Managing a Security Operations Center (SOC).
- Digital Forensics and Investigation in a Regulated Environment.
- Crisis Communication Strategies for Stakeholders and Regulators.
- Business Continuity and Disaster Recovery Integration.
- Conducting Effective Tabletop Exercises and Simulations.
- Post-Incident Review and Continuous Improvement.

Unit Five: Future-Proofing Financial Services Security

- Securing Cloud Adoption and Multi-Cloud Environments.
- Cyber Resilience for FinTech and Digital Transformation.
- Security Considerations for Blockchain and Digital Assets.
- Leveraging Artificial Intelligence and Machine Learning in Defense.
- Building a Human Firewall through Security Awareness and Culture.
- The Future of Cyber Warfare and its Impact on Finance.
- Developing a Personal Action Plan for Implementing Course Concepts.

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:

As financial systems become increasingly interconnected with non-financial sectors, how can a firm's cyber resilience strategy adapt to manage systemic risks that originate outside its traditional regulatory perimeter?

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

This training course distinguishes itself by moving beyond generic cybersecurity principles to offer a specialized, strategic immersion into the unique ecosystem of the financial services industry. Unlike programs that focus solely on technical tools or broad best practices, our curriculum is built around the specific regulatory pressures, sophisticated threat actors, and systemic risks inherent to banking, insurance, and investment management. We emphasize the development of strategic foresight, enabling participants to build resilience frameworks that are not only compliant but also adaptive and forward-looking. The course content is deeply rooted in practical application, utilizing case studies drawn directly from financial sector breaches and regulatory enforcement actions. This provides a level of contextual relevance that is often missing in other training. Furthermore, the focus is less on managing technology and more on leading people and processes through high-stakes crises. Participants will learn to navigate the complex interplay between technology, business operations, legal obligations, and reputational management, equipping them with the holistic leadership skills necessary to champion cyber resilience at the highest levels of their organizations.