Strategic Cyber Security Awareness Program Development Training Course



19 - 23 Oct 2026

Boston

7500 € (Per Person)

Ref: #CYB8464_88546

Course Introduction / Overview:

In today's hyper-connected digital landscape, the human element remains the most critical variable in an organization's cyber defense strategy. Technical safeguards are essential, but a well-informed and security-conscious workforce is the ultimate deterrent against sophisticated threats. This course moves beyond basic employee training to empower managers with the strategic skills needed to design, implement, and sustain a robust cyber security awareness program. We delve into the principles of creating a resilient security culture, a concept expertly detailed by Dr. Lance Hayden in his influential book, "People-Centric Security: Transforming Your Enterprise Security Culture". Participants will learn to transform security from a compliance checklist into an ingrained organizational value. At BIG BEN Training Center, we provide a comprehensive framework for building a program that not only educates but also engages employees, effectively turning your team into your strongest security asset. This training equips leaders to measure program effectiveness, demonstrate return on investment, and continuously adapt to the evolving threat landscape, ensuring long-term organizational resilience against cyber-attacks.

Target Audience / This training course is suitable for:

- Managers and Team Leaders across all departments.
- Information Technology (IT) and Information Security (IS) Managers.
- Human Resources (HR) Managers and Training Coordinators.
- Compliance, Risk, and Audit Professionals.
- Project Managers and Department Heads.
- Executives and Senior Leaders responsible for organizational risk.
- Anyone tasked with developing or overseeing a security awareness initiative.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Pharmaceutical sectors.
- Technology and Telecommunications.
- Government and Public Sector Agencies.
- Retail and E-commerce.
- Energy and Utilities.
- Education and Research Institutions.
- Manufacturing and Industrial sectors.

Target Organizations Departments:

- Information Technology and Security.
- Human Resources and Corporate Training.
- Operations and Business Units.
- Legal, Risk Management, and Compliance.
- Internal Audit and Governance.
- Executive and Senior Management.
- Project Management Office (PMO).
- Customer Service and Support.

Course Offerings:

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

- Design a comprehensive, strategic cyber security awareness program from the ground up.
- Conduct a thorough needs analysis to identify specific organizational vulnerabilities and training gaps.
- Develop engaging and relevant training content tailored to different employee roles.
- Implement effective phishing simulation campaigns and social engineering awareness exercises.
- Establish key performance indicators (KPIs) to measure program effectiveness and ROI.
- Foster a proactive and positive security culture within their teams and the wider organization.
- Create and enforce clear security policies and procedures.
- Communicate security concepts effectively to a non-technical audience.
- Integrate security awareness into the employee lifecycle, from onboarding to offboarding.
- Lead incident response communication and post-incident awareness reinforcement.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, practical, and highly interactive, ensuring that participants can immediately apply their learning in a real-world context. We move beyond traditional lecture-based formats to a hands-on, workshop-style environment. The course heavily utilizes case studies of recent, high-profile security breaches, allowing participants to deconstruct attack vectors and identify the human factors involved. A significant portion of the training is dedicated to collaborative group activities, where attendees will work in teams to design mock awareness campaigns, draft security policies, and develop incident response communication plans. Role-playing scenarios will simulate challenging situations, such as managing an employee who has fallen for a phishing scam or presenting a business case for security investment to senior leadership. Throughout the course, there will be continuous opportunities for peer review and constructive feedback, facilitated by our expert instructors. This blended approach of theoretical knowledge, practical application, and collaborative problem-solving ensures a deep and lasting understanding of how to build and manage an effective security awareness program.

Course Agenda (Course Units):

Unit One: Foundations of a Modern Security Awareness Program

- The Evolving Threat Landscape and the Human Factor.
- The Psychology of Social Engineering and Human Error.
- Defining Security Culture vs. Security Awareness.
- Key Principles of Adult Learning and Behavioral Change.
- Legal, Regulatory, and Compliance Drivers for Awareness Training.
- The Manager's Crucial Role in Championing Cyber Security.
- Aligning the Awareness Program with Business Objectives.

Unit Two: Strategic Program Design and Development

- Conducting a Training Needs Analysis and Risk Assessment.
- Setting SMART Objectives and Defining Success Metrics.
- Developing a Program Charter and Securing Leadership Buy-in.
- Content Strategy: Building a Curriculum for Different Audiences.
- Choosing the Right Delivery Methods (eLearning, Workshops, Gamification).
- Budgeting and Resource Allocation for Your Program.
- Creating a Multi-Year Program Roadmap.

Unit Three: Core Content and Engagement Tactics

- Mastering Phishing and Spear Phishing Defense Training.
- Recognizing and Reporting Social Engineering Tactics.
- Safe Internet and Email Usage Policies.
- Data Protection, Classification, and Secure Handling.
- Password and Authentication Best Practices.
- Mobile and Remote Work Security (BYOD).
- Physical Security Awareness and Clean Desk Policies.

Unit Four: Implementation and Cultivating a Security Culture

- Developing a Comprehensive Program Launch and Communication Plan.
- Building a Security Champions Network to Drive Engagement.
- Integrating Security Awareness into Employee Onboarding and Offboarding.
- Techniques for Making Security Training Engaging and Memorable.
- Leveraging Storytelling to Illustrate Security Concepts.
- Providing Positive Reinforcement and Recognition.
- Handling Policy Violations and Teachable Moments.

Unit Five: Measurement, Metrics, and Continuous Improvement

- Establishing Key Performance Indicators (KPIs) for Program Success.
- Measuring Behavioral Change and Reduction in Human-Related Risk.
- Calculating the Return on Investment (ROI) of Your Program.
- Utilizing Phishing Simulation Results for Targeted Training.
- Gathering and Analyzing Feedback through Surveys and Focus Groups.
- Reporting Program Status and Success to Senior Leadership.
- Adapting the Program to New Threats and Evolving Business Needs.

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:

Beyond compliance, how can a manager transform a security awareness program from a mandatory chore into a genuine, self-sustaining cultural value within their team?

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

This course distinguishes itself by focusing squarely on the strategic and leadership aspects of cyber security awareness, specifically tailored for managers. While many courses teach employees how to spot a phishing email, our program teaches managers how to build the entire system that fosters such vigilance. We move beyond the "what" of security topics to the "how" of program design, cultural transformation, and performance measurement. The curriculum is built on the premise that a successful program is not just an IT initiative but a core business function that requires leadership, communication, and strategic planning. Participants will not just learn about security threats; they will engage in hands-on workshops to draft policies, design communication campaigns, and calculate the return on investment for their initiatives. Unlike generic, one-size-fits-all training, this course emphasizes a people-centric approach, empowering managers to become effective security leaders who can inspire genuine behavioral change and cultivate a resilient security culture that endures long after the training is complete.