Developing a Proactive Cybersecurity Strategy

How to safeguard enterprise systems and digital assets from evolving cyber threats

Focus on: The Manager ☑ The Specialist ☑ Spotlight Programme □ Hands-on Skills □

Course Overview

This 5-day course is designed for Business Leaders and CISOs to develop a proactive cybersecurity strategy that aligns with business goals and safeguards enterprise systems against evolving threats. Participants will gain a deep understanding of the cyber threat landscape, risk management frameworks, and regulatory compliance, while learning how to create and implement a robust cybersecurity strategy. The course combines strategic insights with hands-on activities, including incident response planning, crisis management simulations, and cybersecurity strategy development. By the end of the course, participants will be equipped to lead their organisations in strengthening cybersecurity resilience, ensuring business continuity, and responding effectively to cyber incidents.

Course Objectives		This Course is Ideal For:	
1	Develop a proactive cybersecurity strategy aligned with business goals and digital transformation initiatives.	✓	Chief Information Security Officers (CISOs) responsible for leading and implementing cybersecurity strategies.
2	Strengthen cyber risk management and ensure compliance with key regulations and governance frameworks.	✓	Chief Information Officers (CIOs) overseeing the alignment of cybersecurity with business goals and technology integration.
3	Enhance incident response and crisis leadership capabilities to maintain business continuity during cyber incidents.	✓	Senior IT & Security Executives shaping overall security policies and risk management strategies.
4	Foster a security-first culture by addressing human factors and ensuring cybersecurity awareness at all levels.	✓	Risk & Compliance Officers ensuring regulatory compliance and mitigating cybersecurity risks.
5	Measure and improve cybersecurity maturity using KPIs, executive reporting, and real-world simulations.		

Course Content

Day	Theme	Coverage
1	The Business Impact of Cybersecurity	Session 1: The Evolving Cyber Threat Landscape • Key cybersecurity threats impacting enterprises (ransomware, APTs, supply chain attacks) • How cyber incidents affect business operations, reputation, and revenue • Cybersecurity trends: AI-driven threats, regulatory shifts, and geopolitical risks Session 2: Cyber Risk from an Executive Perspective

		• The role of business leaders and CISOs in cybersecurity governance • Regulatory compliance (GDPR, NIS2, SEC Cyber Disclosure, ISO 27001)
2	Building a Proactive Cybersecurity Strategy	Session 1: Proactive Cybersecurity Measures • Technological interventions (identify and access) and monitoring (IDS) • Human generated threats (insider, social engineering) and their mitigation Session 2: Aligning Cybersecurity with Business Objectives • Developing a risk-based cybersecurity strategy • Cybersecurity as a business enabler (protecting growth, M&A, digital transformation) • Budgeting for cybersecurity: Balancing cost, risk, and ROI
3	Cyber Incident & Crisis Management	Session 1: Developing an Incident Response Strategy • Key components of an Incident Response Plan (IRP) • Understanding cyber insurance: pros, cons, and cost considerations • Legal, compliance, and PR response to cyber incidents Session 2: Cyber Crisis Management Simulation • Executive response to a major cyber attack • Handling crisis communications (internal teams, customers, regulators)
4	Cybersecurity Leadership & Organisational Resilience	Session 1: Strengthening Organisational Cyber Resilience • Managing insider threats and third-party security risks • Strategies for board-level cybersecurity reporting and KPIs • Business continuity planning and disaster recovery Session 2: Creating a Security-Aware Corporate Culture • The human factor: Executive strategies for security awareness training • Managing the relationship between CISOs, CIOs, and the board security-first cultures
5	Cybersecurity Strategy Execution & Final Planning	Session 1: Developing a Comprehensive Cybersecurity Action Plan • Prioritising cybersecurity initiatives based on risk, resources, and business goals • Addressing emerging threats and adapting your strategy over time Session 2: Executive Strategy Peer Review

		• Identifying areas of improvement and potential gaps in cybersecurity strategy • Defining success metrics for ongoing evaluation and refinement

Course Assessment	Certification
Participants will be assessed on:	Upon successful completion of the course, participants will receive a **Certificate of Successful Completion**, along with a **Transcript of Marks** showing the performance by grade in each element of assessment and overall.
Participation in sessions	
Completion of exercises & case studies	
Performance in assessments	

Course Instructor

The speaker for this programme is an International Expert and Professor of Cyber Security at a leading UK university. He is also a Member of the UK Government's Cyber Security Advisory Board. The speaker has extensive expertise in Cyber Security and Artificial Intelligence and is widely published in this field.