Cybersecurity
CENTRE OF EXCELLENCE

Cybersecurity Leadership Masterclass: Leading Organisational Resilience

The Cybersecurity Leadership Masterclass is designed as an interdisciplinary course, focusing on management strategies, organisational governance, the technical elements that underpin the Cybersecurity discipline, security technologies, national policy and legislation, and standards, The course incorporates elements relevant to creating a culture of cybersecurity awareness and resilience and focuses on the developing relevant strategic responses to the security challenges posed to organisations in an increasingly complex digitally transforming environment.

The course is structured into nine targeted modules, each designed to progressively build upon the previous one, ensuring participants develop a cohesive and practical Cybersecurity strategy tailored to their organisation's needs. The course has a strong practical element, that complements the theoretical learnings, and course participants will complete elements of an organisational strategy document, for which a template is provided - each module builds on the template

The Cybersecurity Leadership Masterclass program emphasizes the critical role of senior management and leadership in effectively managing cybersecurity threats and achieving organizational objectives related to information protection. Designed specifically for senior managers, CISOs, and executive leaders, the course delivers strategic insights into cybersecurity management within an organizational context. Participants will gain a comprehensive understanding of risk management, audit, governance structures, and compliance requirements, and explore how regulations influence legal responsibilities and liabilities.

Additionally, the program highlights the importance of robust continuity and disaster recovery planning, addresses economic considerations relevant to cybersecurity investments, and provides strategic guidance on building high-performing cybersecurity teams and leading effectively within complex cyber threat environments.

Course Objectives:

- Participants will be able to develop a comprehensive cybersecurity strategy aligned with organizational goals.
- Participants will understand the key principles of cybersecurity governance and how to implement them.

Module Breakdown

Module 1: Foundations of Cybersecurity Strategy

This foundational module introduces participants to the core concepts that underpin the Cybersecurity domain including definitions, the evolving threat landscape, current trends, attack vectors, and emerging threats. It proceeds to align Cybersecurity with the business objectives and underscores the importance of identifying organisational, vision, mission, goals and priorities.

Module 2: Cybersecurity Governance and Strategic Leadership

- Participants will learn the leadership skills necessary to champion and drive cybersecurity initiatives.
- Participants will gain knowledge and skills to build cybersecurity resilience within an organization.

Duration

9 weeks (excluding orientation)

Language

English

Effort

6-8 hours per week

One introductory online lecture per module, followed by one week of self-paced online learning per module

Building upon the foundations, this module delves into the strategic leadership responsibilities essential for effective cybersecurity governance.

Module 3: Cybersecurity Risk Management

Participants will explore high-level principles and frameworks for cybersecurity risk management. Risk management fundamentals: identifying, assessing, and mitigating cybersecurity risks

Module 4: Legislative and Regulatory Compliance

This module addresses the legal and regulatory environment that shapes cybersecurity strategy. Participants will gain strategic insights into relevant cybersecurity regulations and the importance of proactive compliance management.

Module 5: Technical Elements of Cybersecurity

This module provides senior leaders with a broad strategic perspective on essential cybersecurity concepts such as Defense-in-Depth and Zero Trust Architecture. It provides and overview of the tools and technologies deployed in the cybersecurity domain.

Module 6: Critical Information Infrastructure Protection

For those concerned with national security or essential services, this module focuses on the specific strategic considerations for protecting critical information infrastructure.

Module 7: Incident Response, Continuity, and Crisis Management

Participants will learn to strategically manage cybersecurity incidents, focusing on effective response planning, crisis management, business continuity, and recovery strategies.

Module 8: Building Effective Cybersecurity Teams and Organizational Culture

This module addresses the strategic aspects of building effective cybersecurity teams and fostering an organizational culture that prioritizes cybersecurity awareness and continuous improvement.

Module 9: Developing the Cybersecurity Strategy

This module focuses on strategically planning for and executing measures that enable an organization to withstand, recover from, and adapt to cyber disruptions, a crucial element of a robust cybersecurity strategy.