HIGH POINT CENTER

# course : Cyber Security for Non-IT Professionals

| | | | |
|---|---|---|---|
| **City :** | Amsterdam | **Hotel :** | Hotel Okura Amsterdam |
| **Start Date :** | 2025-10-27 | **End Date :** | 2025-10-31 |
| **Duration :** | 1 Week | **Price :** | 5950 $ |

HIGH POINT CENTER

## Course Overview

This 5-day program provides participants with the essential knowledge and practical skills to navigate the dynamic field of cybersecurity. The course establishes a solid foundation in key concepts, principles, and industry standards, while offering hands-on exposure to technical, physical, and managerial controls that underpin a strong security posture.
Through real-world case studies and interactive exercises, participants will explore threat actors, attack vectors, malware, and high-profile cyber incidents. In addition, the course covers technical domains such as authorization, authentication, encryption, and network security fundamentals. Finally, participants will engage in a practical incident response exercise to understand the full lifecycle of cyber incident management and strengthen organizational resilience.

## Course Objectives

By the end of this course, participants will be able to:
Explain key cybersecurity concepts, terminologies, and industry standards.
Apply technical, physical, and managerial controls to establish a comprehensive security posture.
Identify cyber threats, analyze threat actors' motivations and capabilities, and recognize common attack vectors.
Understand malware types and examine real-world case studies.
Describe core technical aspects, including authorization, authentication, encryption, and network security fundamentals.
Evaluate business impacts, design business continuity plans, and develop disaster recovery strategies.
Apply the incident response lifecycle in a simulated practical exercise.

## Target Audience

This course is designed for professionals who:
Work in or aspire to work with cybersecurity or IT functions.
Require a comprehensive overview of cybersecurity to support their role.
Need to understand the impact of cybersecurity on organizational resilience and risk management.

## Methodology

Interactive presentations
Group discussions and collaborative learning
Individual research tasks
Practical, scenario-based exercises

## Course Outline

1. Fundamentals of Cybersecurity
Core security concepts and definitions
Cybersecurity standards and frameworks
Compliance and regulatory requirements
Case studies of high-profile cyber attacks
2. Security Controls
Technical controls: encryption, access management, network defense
Physical controls: facility and infrastructure protection
Administrative controls: governance, policies, and procedures
3. Understanding Cyber Threats
Threat actors: profiles, motivations, and capabilities
Common attack vectors and exploitation methods
Introduction to malware and its variants
4. Core Technical Aspects
Authorization and authentication mechanisms
Principles of encryption and data protection
Network security fundamentals
Security in cloud computing environments
5. Incident Management and Resilience
Incident response concepts and lifecycle
Business continuity management (BCM)
Disaster recovery (DR) planning and strategies
Practical tabletop incident response exercise

## Certificates

On successful completion of this training course, HighPoint Certificate will be awarded to the delegates.
Continuing Professional Education credits (CPE): In accordance with the standards of the National Registry of CPE Sponsors, one CPE credit is granted per 50 minutes of attendance.