



**INNOCYBER Innovation HUB**

Digital transformation, Cyber & IoT

# < **CYBERSECURITY** > **EXECUTIVE PROGRAM**

## **2<sup>nd</sup> Edition**

**Starting date:**

**April 13<sup>th</sup>, 2023**

Scientific Coordination

Professor

António Casimiro

Executive Coordination

Professor

Telmo Vieira



**Ciências**  
**ULisboa**



**PREMIVALOR Consulting**  
*Your Value Partner*



## >Objectives and scope

- > To provide an overall comprehension of the risks and challenges on organizations resulting from an increasingly digital economy concerning cybersecurity.
- > To provide insights from leading experts of the industry, regulators and reference academics concerning the implications of cybersecurity risks in terms of the organizations' Business, Governance and Compliance.
- > This program aims to be the best international cybersecurity short/medium term course for executives and decision makers in Europe.





## > To whom this course is addressed

- > Members of the **Management Board** of companies/organizations from the private and public sectors
- > Members of the **Supervisory Board** of companies/organizations from the private and public sectors
- > Members of the **Management Board** and the **Supervisory Board** of **Banks, Fintechs, and Insurance companies**
- > **Directors and Decision makers** of organizations on the areas/committees of **Internal Control and Risk, Internal Audit, Inspection, Compliance and Legal**
- > **Armed forces** decision makers
- > **Law enforcement** decision makers
- > **Certified Public Accountants/Statutory Auditors** (Revisores Oficiais de Contas)
- > **Lawyers** on decision making positions



## > Format

- > The course will have an **Hybrid format** (the first class and the last 2 classes will be in person @ Faculdade de Ciências da Universidade de Lisboa + the remaining classes will be held online)
- > Starting date: **April 13<sup>th</sup>, 2023**
- > 30 hours (12 modules)
- > **Tuesdays and Thursdays**, from 16:30 to 17:50 and 18:00 to 19:20
- > **Certificate** to be issued by Faculdade de Ciências da Universidade de Lisboa (FCUL) after the completion of the course





## > Program

- > MODULE 1: Macro perspective on cybersecurity
- > MODULE 2: Introduction to cyber security concepts
- > MODULE 3: Operational Technology Security (OT)
- > MODULE 4: Protection of assets and detection of attacks
- > MODULE 5: Funding Programmes for the Cybersecurity Economy
- > MODULE 6: Identification of assets and risk concepts



## > Program

- > MODULE 7: Reaction and Recovery
- > MODULE 8: Cybersecurity Law
- > MODULE 9: Cybercrime
- MODULE 10:
  - Economic Evaluation of Cybersecurity Investments
  - Cybersecurity risks and challenges on Banking and Fintech sectors
- > MODULE 11: Asymmetric Threats - Cyber Threats
- > MODULE 12: Case studies and Tabletop exercise





# > MODULE 1

## Macro perspective on cybersecurity (3h)

- > The strategic perspective of Cybersecurity at national level - Resilience, sovereignty, and Leadership
- > What the C level needs to ask to assess the organization's cybersecurity level
- > Major challenges for organizations and citizens
- > New technologies leveraged by the pandemic
- > The need for a common knowledge concerning cybersecurity
- > EU Cybersecurity Strategy and its relationship with the National Cyberspace Security Strategy
- > EU Cybersecurity Certification. What is due to occur in Portugal and the impact in the economy
- > Cybersecurity incidents in Portugal – The National Cybersecurity Observatory
- > Operational Capability to prevent, deter and respond
- > New strategic initiatives
- > Self-evaluation Quiz

### > Instructor

**Contra-Almirante António Gameiro Marques**

General Director

Gabinete Nacional de Segurança (GNS)





## > MODULE 2

### Introduction to cyber security concepts (3h)

- > Cyber Security definition
- > Importance of security at different layers (from physical to information)
- > Fundamental information security properties: confidentiality, integrity, availability
- > Types of vulnerabilities
- > Types of attacks
- > Motivations of attackers
- > Phases of an attack
- > Attack-Vulnerability-Intrusion (AVI) model
- > NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
- > Self-evaluation Quiz

### > Instructor

**Eng. José Alegria**

CISO, Head of CyberSecurity & Privacy (DCY)

ALTICE Portugal







## > **MODULE 3**

### Operational Technology Security (OT) (3h)

- > Cybersecurity OT Overview - Industry 4.0
- > OT & IIoT Technology Architecture:
  - > Industrial Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Industrial Control Systems (ICS), Industrial Internet of Things (IIoT), Cyber-Physical System (CPS)
- > Differences between IT and OT
  - > Industrial Cyber Kill Chain, MITRE ATT&CK
- > Cybersecurity Architecture in Industrial Systems:
  - > Defense in Depth concept and Purdue Model, Industrial security standards ISA 62443
- > Standards and good practices in Industrial systems:
  - > NIST CSF, NIST 800-82, IEC 62443
- > Critical Infrastructures and Essential Services (EU Regulations):
  - > EU Critical Infrastructures regulations, EU NIS2 directive
- > IT-OT Convergence. Industrial SOC's
- > Protection of OT & Mitigation measures:
  - > Cyber OT Technology trends, OT Services and Procedures
- > Self-evaluation Quiz

### > Instructor

**Prof. Eng. Javier Jarauta Sánchez**

Head of Cybersecurity Strategic Demand Generation

SIA / Minsait

Coordinator of the Master in Cybersecurity at Universidade Pontifícia de Comillas  
ICAI-ICADE in Madrid





## > MODULE 4

### Protection of assets and detection of attacks (3h)

- > Access control (Authentication, Authorization, Accounting)
- > Network protection (SSL/TLS, VPNs)
- > Infrastructure protection (Firewalls, IPS, Antivirus)
- > Information protection (backups, DLP tools)
- > Penetration testing
- > Personnel training
- > Intelligence gathering systems / OSINT
- > Vulnerability scanners
- > Event gathering and monitoring systems (Syslog, NIDS, HIDS)
- > Event correlation (SIEMs)
- > Self-evaluation Quiz

### > Instructor

**Eng. Paulo Moniz**

Information Security and IT Risk Director

EDP - Energias de Portugal







## > **MODULE 5**

### Funding Programmes for the Cybersecurity Economy (1,5h)

- > The European Strategy for the Digital de Decade
- > Cybersecurity Policy Context in Europe
- > The EU Cybersecurity Market – The road to a Strategic Autonomy
- > The Digital and Horizon Europe Programmes and the European Cybersecurity Competence Centre
- > European Funding for Cybersecurity - A practical approach
- > Self-evaluation Quiz

#### > Instructor

**Dr. Marco Barros Lourenço**

Head of Research and Innovation

European Union Agency for Cybersecurity  
(ENISA)





## > **MODULE 6**

Identification of assets and risk concepts (1,5 h)

- > Information flows and dependencies
- > Risk identification
- > Risk assessment
- > Risk analysis
- > Risk management
- > Self-evaluation Quiz

### > Instructor

**Prof.<sup>a</sup> Ana Respício**

Assistant Professor of Informatics

Faculty of Science of the University of Lisbon







## > MODULE 7

### Reaction and Recovery (3h)

- > Response plans (legal frameworks)
- > Incident management
- > Analysis of incident impacts
- > Contingency plans
- > Disaster recovery
- > Business continuity
- > Image recovery and communication
- > Self-evaluation Quiz

### > Instructors

**Eng. Marcelo Rodrigues**

Cybersecurity & Privacy Director

PwC Portugal



**Eng. Pedro Santinhos**

Risk Assurance Director

PwC Portugal





## > **MODULE 8**

### Cybersecurity Law (1,5h)

- > The importance of the legal dimension
- > Cybersecurity legal and regulatory framework - main trends
- > The legal impacts of a cyber incident
- > A strategic approach to cybersecurity regulatory framework (general and sector-specific legislation)
- > Self-evaluation Quiz

### > Instructor

**Dra. Magda Cocco**

Head of Practice of Information,  
Communication & Technology

VdA - Vieira de Almeida







## > **MODULE 9**

Cybercrime (1,5 hours)

- > Modus Operandi and terminology of the main cybercrimes
- > Incident and Crime: practical aspects of legislation
- > From the preparation to the mitigation of cyber-incident: the legal action
- > Self-evaluation Quiz

### > Instructor

**Dr. Rogério Bravo**

Chief Inspector of UNC3T - National Unit for  
Combating Cybercrime and Technological Crime  
Portuguese Judiciary Police (PJ)





## > MODULE 10

### a. Economic Evaluation of Cybersecurity Investments (1,5 h)

#### > The economic Evaluation of Cybersecurity Investments:

- > The financial model
- > Key assumptions
- > Key economic and financial indicators (KPI):
  - > ALE - Annual Loss Expectancy
  - > ROSI - Return on Security Investment
  - > NPV - Net Present Value
  - > IRR - Internal Rate of Return
  - > NPV.E - Economic Net Present Value
  - > IRR.E - Economic Internal Rate of Return
- > Concept of externalities on cybersecurity

#### > Self-evaluation Quiz

### > Instructor

**Prof. Telmo Vieira**

Managing Partner

PremiValor Consulting

Certified Public Accountant / Statutory Auditor (CPA)







## > MODULE 10

### b. Cybersecurity risks and challenges on Banking and Fintech sector (1,5h)

- > Major trends and Cybersecurity concerns in the financial sector, namely in the Banking industry
- > Cooperation, Proactivity and Systemic Approaches to Cyber Threats
- > Cybersecurity Governance: Engaging the Executive Boards
- > Narrowing the Cyber Language GAP between Operational/ Tactical and Executive Boards
- > Self-evaluation Quiz

### > Instructor

**Eng. Pedro Martins da Silva**  
Head Of Unit - Cybersecurity  
Banco de Portugal





## > **MODULE 11**

### Asymmetric Threats - Cyber Threats (3h)

- > Asymmetric conflicts;
- > Cyber war;
- > Asymmetric threats;
- > Asymmetric cyber attacks;
- > Asymmetric cyber attacks - examples:
  - > Syrian Electronic Army
    - > DDOS
  - > Stuxnet
  - > Estonia
  - > Ukrainian elections
- > Cost vs impact;
- > Who is the enemy;
- > Who is the target;
- > Vectors;
- > What to do;
- > Attack strength;
- > Case study;
- > Self-evaluation quiz.

#### > Instructor

**Major José Ferreira**  
Cyber Defense Head  
Portuguese Air Force







## > MODULE 12

### Case studies and Tabletop exercise (3h)

- > Target and MAERSK case studies – to be first discussed by students and then in class with the professor/lecturer as a way to cement the knowledge obtained throughout the course
- > Tabletop exercise to stimulate leaders in the decision associated with a crisis originating in cyberspace
- > Final remarks on the program

### > Instructor

**Contra-Almirante António Gameiro Marques**

General Director

Gabinete Nacional de Segurança (GNS)



> **NOTE:** The tabletop exercise is a meeting to discuss a simulated emergency. Participants review and discuss the actions they would take in a specific emergency, testing their emergency plan in an informal, low-stress environment. Tabletop exercise is intended to clarify roles and responsibilities and to identify additional mitigation and preparedness needs. The exercise should result in action plans for continued improvement of the emergency plan.



## > Pricing

> **1.475 € \***

> Discounts (non-cumulative):

> **Early bird: 15%** for participants that register until January 31<sup>st</sup>, 2023

> **Early bird: 10%** for participants that register between February 1<sup>st</sup>, 2023 and February 28<sup>th</sup>, 2023

> **20%** for INNCYBER INNOVATION HUB partner companies/organizations and individual participants from universities and research centers

> **20%** for companies that participate in the course with 2 or more members

### **LIMITED SPOTS AVAILABLE**

Having into account the characteristics of the course contents and the positions occupied by the lecturers of the program, candidates are subject to curriculum evaluation and a “*Fit & Proper*” process before participation approval on the course.

\* 23% VAT to be added (if applicable)





# INNCYBER Innovation HUB

Digital transformation, Cyber & IoT



**Ciências**  
**ULisboa**

For additional information, please feel free to contact us:

[www.inncyberinnovationhub.com](http://www.inncyberinnovationhub.com)

Rita Vasconcelos (Director) - [rita.vasconcelos@premivalor.com](mailto:rita.vasconcelos@premivalor.com) | +351 913 247 778 (WhatsApp)

André Barata - [andre.barata@premivalor.com](mailto:andre.barata@premivalor.com) | +351 913 247 837 (WhatsApp)

Office Phone: +351 217 820 316

We are available to book a conference call for further clarification on the platforms:

- Zoom
- Google Meet
- MS TEAMS

Avenida 5 de Outubro n.º 75, 7.º piso

1050-049 Lisboa | PORTUGAL