Cybersecurity Executive Program

➢ Objectives and scope of the course

To provide an overall comprehension of the **risks** and **challenges** on organizations resulting from an increasingly digital economy concerning cybersecurity leveraged in terms of speed and deepness by the COVID-19 pandemic.

To provide insights from the leading experts of the industry 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, Fintech,** and **Insurance companies**
- **Decision makers** of organizations on the areas/**committees** of **Internal Control and Risk, Internal Audit, Inspection**, and **Compliance and Legal**
- **Armed forces** decision makers
- **Law enforcement** decision makers
- **Chartered accountants/Statutory Auditors** (Revisores Oficiais de Contas)
- **Lawyers** on decision making positions

➢ Classes format

Online + in presence last class (optional)

➢ Mentored classes

25 hours (9 classes/modules)

➢ Starting dates:

March 29th, 2022 (1st cohort)

➢ Days/hours

Tuesdays and Thursdays from:

16:30 – 17:50 (1 hour + 20 minutes)

18:00 – 19:20 (1 hour + 20 minutes)

➢ Course program

MODULE 1- Macro perspective on cybersecurity (3h) – Contra-Almirante (*Rear Admiral*) António Gameiro Marques – General Director of Gabinete Nacional de Segurança (GNS)

- 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

MODULE 2 - Introduction to cyber security concepts (3h) – Eng. José Alegria (Altice) - Chief Information Security Officer at Altice Portugal

- 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

MODULE 3 - Identification of assets and risk concepts (3h) – Prof.ª Ana Respício (Faculdade Ciências da Universidade de Lisboa)

- Resources
- Information flows and dependencies
- Security policies and responsibilities
- Risk identification
- Risk assessment

- Risk analysis
- Risk management
- Control strategies
- Cost-benefit analysis in InfoSec
- Self-evaluation Quiz

MODULE 4 - Protection of assets and detection of attacks (3h) – Eng. Paulo Moniz (EDP) - Information Security and IT Risk at EDP - Energias de Portugal

- 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

MODULE 5 - Reaction and Recovery (3h) – Eng. Marcelo Rodrigues (PWC) / Eng. Pedro Miguel Santinhos (Director PWC)

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

MODULE 6 - Cybersecurity Law (3h) -Dra. Magda Cocco (VdA- Vieira de Almeida & Associados, Soc de Advogados)

- The importance of the legal dimension
- Main legal concepts
- 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

MODULE 7 - Economic Evaluation of Cybersecurity Investments (Prof. Telmo Vieira – Managing Partner PremiValor Consulting / *Certified Public Accountant* - ROC) - (1,5 horas)

Cybersecurity Due Diligence in a Mergers & Acquisitions (M&A) process

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

- Self-evaluation Quiz

Cybersecurity risks and challenges on Banking and Fintech sectors (Eng. Luís Carlos Gonçalves – Head of Cybersecurity, IT Risk and Compliance at Bank of Portugal) - (1,5 horas)

- Major trends and Cybersecurity concerns in the financial sector
- 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

MODULE 8 – Asymmetric Threats - Cyber Threats (2,0 hours) – Tenente-coronel André Castro (Portuguese Air Force)

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

MODULE 9 - Case studies and Tabletop exercise (2,0 hours) – Contra-Almirante (*Rear Admiral*) António Gameiro Marques – General Director of Gabinete Nacional de Segurança (GNS)

- 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

QUIZ - Final self-evaluation quiz on learned topics (50 minutes) – one week later after the last module.

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.

➢ Course Professors/lecturers short Bio

António Gameiro Marques (Contra-Almirante (*Rear Admiral*) – General Director of Gabinete Nacional de Segurança (GNS))

Rear Admiral António Gameiro Marques joined the Naval Academy in 1976 and completed a degree in Naval Military Sciences in 1981.

From the 1st of September 2016 he is the Director General of the National Security Authority (GNS), which includes de National Cybersecurity Center in its structure.

Eng. José Alegria ***(CISO, Head of CyberSecurity & Privacy (DCY), Altice Portugal)***

Chief Security Officer at Altice Portugal.

Worldwide coordinator of the CyberWatch Program at the Altice Group.

Member of European Cybercrime Center (EC3) Advisory Group on Communication Providers at EUROPOL.

Over 15 years of experience in the application of advanced software technology to cyber intelligence and cybersecurity.

Prof.ª Ana Respício ***(Assistant Professor at the Informatics Department of the Faculty of Science of the University of Lisbon)***

Ana Respício (female) is an Assistant Professor at the Informatics Department of the Faculty of Science of the University of Lisbon where, currently, she is vice-head of department. She is an integrated researcher of the LASIGE research lab. She holds a PhD in Statistics and Operations Research (U. Lisbon, 2003). She has published more than 70 refereed scientific papers and her research interests include decision support (theory and technologies), optimization, cybersecurity risk management, information security, IoT, AAL, and simulation. She has participated in several R&D

projects, funded by the European Commission, by National scientific agencies, and cooperation with industry projects, namely project DOIT – Decentralization and Optimization of IoT aware business processes, in the area of optimization of sensors' networks, and H2020 project DiSIEM, in the area of Information Security and Big Data.

She is Associate Editor of the Journal of Decision Systems and member of the editorial board of IDT Journal and IJIDS. She is vice-chair of the IFIP Working Group 8.3: Decision Support since 2014 and is a member of the Euro Working Group in DSS.

She is member of the Portuguese Technical Commission for standardization under the ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection (CT163).

Eng. Paulo Moniz ***(Information Security and IT Risk at EDP - Energias de Portugal)***

With 25 years of experience in the world of information technology is in charge of Information Security and IT Risk department at EDP.

He has a degree in Electrical and Computer Engineering from Instituto Superior Técnico and has completed successfully a post-degree in Information Systems (POSI) in the same institution. He also has an MSc in Information Security from Carnegie Mellon University and an MSc in Information Security from the Faculty of Science, University of Lisbon. Later on also successful completed a Master in Business Administration (MBA) from AESE Lisbon Business School.

He has assumed several important participations in the cybersecurity area, highlighting participations at the National level, as a member of the Cyber Committee of AFCEA Portugal (Armed Forces Communications and Electronics Association), member of the Board of Directors of CIIWA (Competitive Intel and Information Warfare Association) and collaboration as a teacher and researcher by IDN (National Defense Institute). Internationally, he is part of the “Systems of Cyber Resilience - Electricity” group at the World Economic Forum and is also responsible for the EDP Group's participation in European H2020 projects in the area of cybersecurity.

Dra. Magda Cocco (Partner, Vieira de Almeida)

Partner| Head of Practice of Information, Communication & Technology, and Partner in charge of the Aerospace sector at VdA.

Magda has provided expert advice to companies, and public entities across different industries on Data economy and cybersecurity-related matters, assisted several entities in governance and strategic matters in these fields, coordinated compliance programs and assisted public and private entities in connection with cybersecurity threats. Magda has also been involved in innovative technological projects with implications in these areas and in defining various countries' legal policies and frameworks.

She is a lecturer at several Universities, teaching subjects related to data, technologies, electronic communications, space and satellites and cybersecurity.

In 2016, Magda was nominated for the Financial Times' Legal Innovator of the Year award, along with the top ten most innovative European lawyers.

Eng. Marcelo Ferreira Rodrigues (Director PWC - Risk Assurance Services | Cybersecurity & Privacy)

Marcelo is a Risk Assurance Director in PwC. He has 15 years of experience in Information Systems Audits, security administration, pentesting, programming and information system audits in the government, industry and financial sector.

Marcelo has a degree in Computer Science by University of Oporto, and as main certifications has CISA - "Certified Information Systems Auditor" and CISM – "Certified Information Security Manager".

He has participated in several projects for organizations of which we highlight the following:

- Responsible for executing and coordinating several pentesting projects at PwC. Experience in black-box and white-box approach, with
- projects executed in a wide range of sectors (Industry, Services, Financial Services).
- Responsible for multiple cloud migration projects.
- Firewall Policy and Software Procurement - Execution of firewall rules analysis and maintenance for a complex set of firewalls
- Responsible for network and systems monitoring implementation, using open source software.
- Responsible for security hardening projects, for servers and network devices
- Information Technology Audits, including security audit validations, for a wide range of clients in multiple sectors (Automotive, Paper
- Industry, Energy, Water, Food, Insurance, …)

Tenente-coronel André Castro (Portuguese Air Force)

Tenente-coronel André Castro began his assignment in the CIS Directorate of the Air Force in February 2018 as the Cyber Defense Chief. Before this assignment he was stationed in the Air Force Academy as CIS Chief and previously in the Combined Air Operations Centre 10 (CAOC10) for 11 years as the INFOSYS and INFOSEC Officer for NATO Networks. Previously, he was the senior systems administrator for the Military and Technical Centre Network in Ota (CFMTFA) for three years.

He has a Masters from Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa in Computer Science.

Eng. Pedro Miguel Santinhos (Director PWC)

With a degree in Computer and Computer Engineering from Instituto Superior Técnico, he has more than a decade of career at the multinational PwC and is currently Director in the area of Risk Assurance Services with project management functions in the areas of auditing systems and information technologies, data analysis, forensic auditing and business continuity.

Additionally, between 2014 and 2016 he was responsible for the IT internal audit activities of the Jerónimo Martins Group and is currently a visiting professor at the Autónoma Academy (professor at the Lisboa Atlântico MBA) and at the OROC (Order of Chartered Accountants).

Prof. Telmo Francisco Vieira

Managing Partner, PremiValor Consulting,

Prof. at ISEG-Lisbon University on Management department for the areas of Mergers, Acquisitions & Restructuring at the Master in Finance and Advanced Auditing at the Master of Accounting.

Co-Founder of INNCYBER INNOVATION HUB

Certified Public Accountant - CPA / Statutory Auditor registered at OROC and CMVM

President of the Supervisory Board of a Bank.

Mentor and investor in Startups on the areas of health, cybersecurity, energy, smart cities and AI.

Eng. Luís Carlos Gonçalves (Head of Cybersecurity, IT risk and Compliance at Bank of Portugal)

Luis holds a PhD degree in Information and Computer Science and specializes in Nacional and International Defense Law. In such role serves as an invited professor in several universities and executive education programs. As an Executive Advisor, is a member of several European Advisory Boards, and works close with executive boards focusing on Strategic and Executive Governance. As subject matter expert works closely with European Agencies and Think Thanks. Currently serves as Head of Cybersecurity, IT Risk and Compliance at the Central Bank of Portugal.