

LEADERSHIP TRAINING

Cybersecurity And Digital Trust For Leaders

Delivered through a customized Cyber World Lab for executives, this experience harnesses state-of-the-art tools and methodologies in collaboration with a leading cybersecurity partner - CyberS3c.

A woman's profile is shown in a light, ethereal style, overlaid with vibrant digital data visualizations. These include colorful streaks of light in shades of blue, purple, and yellow, along with numerous small, glowing dots and circular patterns, suggesting a high-tech or cyber environment. The background is a soft, out-of-focus grey.

As AI expands opportunities, it also magnifies risks – making preemptive security essential for enterprise cyber defense. This program equips forward-thinking leaders to move beyond IT silos and embed intelligent, proactive cybersecurity into the very fabric of their organizational vision.

The Leadership Gap

To steer their organizations safely through digital transformation, leaders must understand the cyber implications of new technologies. Without a foundational level of cyber literacy, executives risk:

- ⦿ Being unable to ask the right questions of technical teams
- ⦿ Falling short in prioritizing and mitigating key risks
- ⦿ Struggling to lead effectively during crisis events
- ⦿ Preventing the development of a resilient culture that prioritizes safety.

THIS PROGRAM BRIDGES THE GAP – ARMING LEADERS WITH THE TOOLS, AND CONFIDENCE TO PROTECT WHAT MATTERS MOST: THEIR REPUTATION, RESILIENCE, AND RELATIONSHIPS.



Why Choose This Program?

Embrace a Holistic Approach

KEY HIGHLIGHTS

Foundational Knowledge

Gain a solid understanding of cybersecurity essentials to make confident, informed decisions.

Leadership Development

Learn how to plan, prioritize, and lead security initiatives with clarity and impact.

Master the Five Cs

Change, Compliance, Cost, Continuity, and Coverage – to build resilient security postures that empower enterprises of every size to thrive in the face of cyber threats.

Engaging Learning Experience

Take part in hands-on labs, Cyber42 simulation games, and collaborative team exercises to build business resilience through incident response and management

Expert Instructors

Learn directly from seasoned cybersecurity professionals with real-world experience.

**LEAD WITH
CONFIDENCE.
INSPIRE TRUST.**

SAFEGUARD THE FUTURE.

PROGRAM OVERVIEW

This six-week executive program is more than a course; it's a transformative experience designed to empower decision-makers across sectors with the insight, confidence, and tools to lead cybersecurity from the front.

2 Sessions

PER WEEK

(6 weeks | Hybrid)

2 Hours

PER SESSION

Objectives

- 🕒 **Understand** the evolving cyber threat landscape and its implications for business.
- 🕒 **Learn** how leadership can foster a security-first mindset across the organization.



WHO SHOULD ATTEND?

This program is designed for a wide range of business leaders – from micro and startup founders to executives in small and medium-sized enterprises (SMEs) and large corporations. It is tailored to benefit both C-level leaders with strong IT expertise and executives with limited technical backgrounds.

- ⦿ **Understand** how to align cybersecurity initiatives with overall organizational objectives.
- ⦿ Differentiate between proactive and reactive cybersecurity management strategies and explore how security failures often stem from the interplay of multiple factors rather than isolated technical flaws.
- ⦿ **Explore the key components of a successful cybersecurity strategy** – balancing governance, human behavior, and technological adaptability.
- ⦿ Examine the **socio-technical framework**, encompassing structure, people, technology, and tasks, to build a holistic approach to cybersecurity.
- ⦿ Analyze successful **case studies and established frameworks** to apply best practices in real-world scenarios.


- ⦿ Identify vulnerabilities and develop proactive **strategies for mitigation**.
- ⦿ Apply knowledge through interactive, **scenario-based decision-making exercises**.
- ⦿ Overview of **major frameworks** (e.g., NIST, ISO 27001, CIS Controls)
- ⦿ **Mapping threats** to critical assets and business processes

Week 1 February 23rd and 27th, 2026

Cybersecurity as a Business Imperative

Week 2 March 2nd and 6th, 2026

Building the Cybersecurity Framework

- 
- ⦿ Develop strategies for **responding to cyber threats**.
 - ⦿ Make informed decisions by correctly assessing risks, **and estimating probabilities and impacts of incidents**.
 - ⦿ Build resilience through business continuity **planning**.
 - ⦿ Engage in **hands-on exercises**, such as mock phishing attempts.

- ⦿ Integrating CSIRT (Computer Security Incident Response Team) and CISO-as-a-Service into risk management to enable faster recovery and build sustainable trust in the business.
- ⦿ Raising the new cibersecurity directives (NIS2) that expand the cybersecurity scope for more sectors , medium and large entities, public administration, critical digital services, and supply chaing obligations.

Week 3 March 9th and 13th, 2026

Identifying and Managing Risks

Week 4 March 16th and 20th, 2026

Incident Response and Recovery



- ⦿ Tackle behavioural challenges using insights from **Daniel Kahneman, Nudge Theory**, and other behavioral science frameworks.
- ⦿ Explore **Gartner's governance structures** that promote shared accountability across departments.
- ⦿ Understand the socio-technical **concept of feedback loops** – how human errors and security gaps can drive continuous improvement in governance and risk management.
- ⦿ Empower employees by raising awareness of how their daily actions impact organizational security, and encourage leadership to model and prioritize secure behavior.
- ⦿ Discover how **collaboration between IT and HR** can play a critical role in identifying and mitigating insider threats.

Week 5 March 23rd and 27th, 2026

Fostering a Cybersecurity Culture

- ⦿ **Leverage** emerging **technologies** in a responsible and secure manner.
- ⦿ Ensure the sustainability of cybersecurity initiatives through strong policy and **governance**, using **Gartner's strategic roadmap** as a guide.

PROGRAM DETAILS

Format

Hybrid format that combines online learning with in-person sessions, ensuring a flexible experience geared toward maximizing impact and networking.

Certificate

Receive a prestigious e-certificate upon completion.

Support

Dedicated Learning Manager for personalized guidance.

Enables real-time interaction with faculty and global peers.

Week 6 March 30th and April 6th, 2026*

The Sustainability of Digital Trust

*Due to the public holiday, the class originally scheduled for April 3rd will be held on April 6th.



WHAT SETS THIS PROGRAM APART?

Weekly Modules, Powerful Impact

Each week, you'll engage in 4 hours of immersive learning—combining high-impact modules with experiential sessions. Through simulations, role-playing, and collaborative exercises, theory comes alive. You'll confront realistic challenges, develop solutions, and practice the kind of decision-making that defines great leaders.

Real-World Learning, Real-World Leaders

You won't just learn about cybersecurity—you'll learn how to lead it. With exclusive sessions led by top industry experts, including thought leaders like Dr. Gurpreet Dhillon, you'll gain strategic insight into topics such as organizational risk, leadership transition vulnerabilities, and building a culture of security that lasts.

Industry collaboration and cutting-edge tools

Throughout the program, you'll gain hands-on exposure to emerging technologies, frameworks, and strategies through expert-led webinars, interactive labs, and curated content.

This isn't just about staying informed – it's about staying ahead.

WHAT MAKES US DIFFERENT?

Interactive Team Labs

Participants will transform knowledge into action through dynamic team labs and immersive case studies. These hands-on sessions are designed to deepen understanding, strengthen collaboration, and apply learning in real-world scenarios. By the end of the program, you will have built a framework of managerial protocols and a personalized playbook with clear, actionable steps to foster a cyber-aware culture across your organization.

Networking Opportunities

Connect with peers from diverse sectors to exchange insights and experiences.

Personalised mentorship

One-hour mentorship session with a senior leader from your sector. Choose from a select group of CEOs and executives, across industries, on the list below.



EMANUEL SOARES
Principal Cybersecurity Engineer of Critical Software



GURPREET DHILLON
John Becker Dean, College of Business Administration
Professor of Management , Information Systems and Quantitative Analysis



SÉRGIO SILVA
CEO and Co-Founder of CyberS3c



SARA DOS SANTOS FERNANDES
Head of Division at the Operational Center for Information Security (COSI)



JOSÉ COSTA
CSO and Board Member of Critical Software

Take The First Step Toward Securing Your Future

Make Cybersecurity Everyone's Responsibility

Globally recognized scholar in cybersecurity and information systems. Dr. Dhillon is the John Becker Dean of the College of Business Administration at the University of Nebraska Omaha, where he also holds a joint appointment as Professor of Management and Professor of Information Systems and Quantitative Analysis. He has published more than 100 peer-reviewed journal articles in leading academic outlets, including FT50 journals, and is the author of over a dozen books on cybersecurity, IT governance, and organizational ethics. His expert commentary has been featured in The Wall Street Journal, New York Times, USA Today, Business Week, CNN, NBC News, NPR, and TEDx. Dr. Dhillon has advised national governments and Fortune 500 firms on cybersecurity strategy and ethical security leadership.

Gurpreet Dhillon

John Becker Dean, College of Business Administration
Professor of Management; Professor of Information Systems and Quantitative Analysis
University of Nebraska Omaha, USA

Computer engineer, scientist, and ethical hacker, currently serving as a cybersecurity professor and assistant researcher at NOVA IMS, Universidade Nova de Lisboa. He holds a Ph.D. in Information Management with a specialization in Information Security, Privacy, and Identity Protection. Dr. Alhelaly has over 30 years of experience in cybersecurity engineering and consulting across academic, governmental, and corporate sectors. He is the designer of the Applied Cybersecurity Program at NOVA IMS, spanning undergraduate, master's, and postgraduate levels. His research focuses on applied cybersecurity, Zero Trust architectures, and human-centered privacy technologies. Dr. Alhelaly leads the Cybersecurity for Executives program and collaborates internationally on AI governance, privacy-by-design, and secure digital transformation.

Yasser Al Helaly

Assistant Researcher & Cybersecurity Professor at NOVA IMS



Partnership



"CYBERS3C® is a 100% Portuguese Cybersecurity company, offering consulting, auditing, and operational training services in the field of Offensive Security. With all systems located within national territory and technology developed in Portugal, we aim to equip national organizations with the capacity to be resilient against Cyberattacks"

Calendar

February 23rd, 27th, March 2nd, 6th, 9th, 13th, 16th, 20th, 23rd, 27th, 30th, April 6th.

Training schedule

6:30 PM to 8:30 PM

Tuition fee

Discounts available for groups of three or more participants. Includes NOVA IMS Certificate.

2,990 €

(VAT exempt under Article 9 of the VAT Code)



Renata Barateiro
Marketing and Admissions Coordinator for Executive Training
+351 213 828 619
executive@novaims.unl.pt