ASIAN INSTITUTE OF MANAGEMENT

FT EXECUTIVE EDUCATION 2025 RANKING

Cyber Security Executive Leadership

Navigate tomorrow's security landscape

Overview

Amidst the dynamic realm of digital transformation and burgeoning technologies, growth opportunities are vast. Yet, alongside progress, intricate cybersecurity risks demand proactive leadership. Unleash your potential amidst this flux through "Cyber Sentry Leadership: Navigating Tomorrow’s Security Landscape.” Exclusively crafted for executives and senior management, this course empowers you to champion your organization's digital voyage. Dive into the fluid cyber landscape, grasp strategic risk management, and forge resilient incident response strategies. Via immersive simulations, real-world cases, and rigorous assessments, you'll emerge poised to navigate evolving cybersecurity.

Elevate your leadership, pioneer the digital frontier, and harness opportunities. Enroll now in "Cyber Sentry Leadership" to amplify your skills, drive success, and protect digital assets. Your transformative journey commences here.

Objectives

The course aims to achieve the following key objectives:

- **Comprehensive Understanding:** Develop an in-depth comprehension of the dynamic cybersecurity landscape, from emerging threats to evolving risks.
- **Strategic Risk Management:** Acquire skills to identify, assess, and mitigate cyber risks strategically, safeguarding critical assets.
- **Effective Incident Response:** Craft robust incident response plans to minimize disruptions and ensure swift recovery from cyber incidents.
- **Framework Application:** Learn to implement and manage cybersecurity frameworks, aligning organizations with industry best practices.
- **Empowered Leadership:** Elevate leadership capabilities by mastering cybersecurity, fostering a vigilant organizational culture

Program Learning Content

Day

- Course Overview and Introduction to cybersecurity landscape and importance

Day 2

- Emerging Attack Surface and Attack Vectors Attackers
- Cyber Kill Chain

Day 3

- Defense Strategies for IT Including Principles of Cyber defense
- Case Study - HBR

Day 4

- Case Study - HBR

Day 5

- Managing cyber risk in OT and Critical Information Infrastructures

Day 6

- Threat Modelling

Day 7

- Cyber Risk Management, GRC and Guidelines and Framework

Day 8

- Incident Response Planning
- Assumed Breach

Day 9

- Simulation Game - HBR

Day 10

- Security Education
- Training and Awareness, Cyber Capabilities Development – Skill and Competencies required

Day 1: Understand the course structure, objectives, and the importance of cybersecurity in modern business.

Day 2: Explore the attack surface, attack vectors, and different attackers and their potential impact on organizations. Understand the use of Cyber Kill Chain

Day 3: Gain insights into the principles of cyber defense, focusing on safeguarding critical assets and maintaining operational continuity.

Day 4: Dissect a real-life incident and its aftermath. Explore the intricacies of handling a Cyber-attack, drawing insights from strategic decisions made by the organization's leadership. Analyze the practical implications of incident response and apply lessons learned to bolster your organizational preparedness.

Day 5: Explore safeguarding Operational Technology and Critical Information Infrastructures, mitigating cyber risks for uninterrupted operations in an interconnected landscape.

Day 6: Learn the fundamental concepts of threat modeling. Understand its role in identifying potential vulnerabilities and assessing security risks within software systems. Explore various threat modeling methodologies and their applications.

Day 7: Learn to identify, assess, and prioritize cyber risks strategically to protect critical assets.

Day 8: Develop comprehensive incident response plans to minimize disruptions and ensure business continuity in the face of cyber incidents.

Day 9: Immerse in a Harvard Business Review simulation, "IT Management Simulation - Cyber Attack," experiencing real-world cyber challenges. Make strategic decisions to manage a simulated cyber-attack, honing your incident response skills in a risk-free environment.

Day 10: Develop strategies to foster a security-conscious workforce through comprehensive education and training, enabling employees to proactively identify and mitigate cyber risks.

Explore the essential skills and competencies necessary for effective cybersecurity leadership, preparing individuals and organizations to navigate evolving threats with confidence

What will you learn

Upon completing this course, participants will:

- Recognize and analyze the latest threat vectors and cyber risks facing modern organizations.

- Strategically manage and mitigate cyber risks, ensuring long-term organizational security.

- Develop and implement effective incident response plans for rapid recovery and minimal disruption.

- Apply cybersecurity frameworks to enhance organizational security posture and compliance.

- Lead confidently in cybersecurity matters, and fostering a proactive culture of vigilance and readiness

Program Faculty

Philip Kwa

Clinical Professor
Asian Institute of Management

With over two decades of diverse global experience spanning corporate and entrepreneurial landscapes, Philip has demonstrated exceptional versatility in roles ranging from CEO and CFO to Sales and Marketing Head and Strategic Consulting Director. Currently, he serves as the Incoming Academic Program Director for the Master in Cybersecurity program at the prestigious Asian Institute of management.

His expertise encompasses Cyber Security Training, Risk Assessment, Governance, Business Process Transformation, Factory Automation, and Entrepreneurship. Philip's career trajectory has taken him across various countries including the USA, China, Thailand, Indonesia, Hong Kong, Japan, and Korea, where he spearheaded intricate IT projects and strategic initiatives in Supply Chain and Business Strategy.

Formally educated with an MBA from the University of Hull, a Diploma in Directorship from SMU-SID, a Post Graduate Diploma in Knowledge Engineering from USS-ISS, and a Bachelor of Commerce from the University of Western Australia, Philip further solidifies his credentials with professional certifications such as CISM, PMP, and Practitioner Certificate in Data Processing, along with Certified Accountant status.

Beyond his professional accomplishments, Philip is deeply committed to community service, having founded the Info security Chapter of Singapore Computer Society, and being actively involved in organizations like Tech Talent Assembly and ACE Singapore. His leadership as Audit Chair and Deputy General Treasurer reflects his dedication to shaping a resilient and thriving PMET workforce and entrepreneurial ecosystem.

Jeffrey Ian C. Dy

Adjunct Faculty
Asian Institute of Management

Jeffrey Ian C. Dy has over 20 years of experience in technology and information security leadership across the public and private sectors. As Undersecretary at DICT, he oversees Infostructure Management, Cybersecurity, ICT Literacy and Competency Development, and the Government Emergency Communications System, while co-chairing the National Cybersecurity Inter-Agency Council and serving on key government committees.

He was the principal author of the National Cybersecurity Plan 2023–2028 (Executive Order 58) and led the expansion of the National Computer Emergency Response Team, the National Security Operations Center, and the National Fiber Backbone, as well as the approval of the World Bank-backed Philippine Digital Infrastructure Project. In addition to being an Adjunct Faculty of the Asian Institute of Management, he also lectures on Information Security at the Philippine Military Academy, National Defense College, and the Foreign Service Institute

Key Benefits

Key benefits that participants can gain from this course:

- **Strategic Cyber Vigilance:** Develop a heightened awareness of the ever-evolving cybersecurity landscape, enabling you to proactively identify and address emerging threats before they impact your organization.

- **Informed Decision-Making**: Acquire the knowledge to make well-informed strategic decisions regarding cybersecurity, minimizing risks, and optimizing resource allocation for maximum protection.

- **Resilient Incident Response:** Gain the skills to design and execute effective incident response plans, minimizing downtime and ensuring a swift return to normal operations in the event of a cyber incident.

- **Leadership Empowerment:** Elevate your leadership capabilities by understanding and effectively communicating cybersecurity strategies to your team, fostering a culture of vigilance and preparedness.

- **Competitive Advantage:** By mastering cybersecurity frameworks and best practices, you'll enhance your organization's security posture, bolstering customer trust and positioning your business as a secure and resilient industry leader.

Who Should Attend

Executives, Senior Management, Directors, and Leaders across industries who understand the strategic significance of cybersecurity in the modern business landscape. This course is tailored to those seeking to enhance their leadership acumen in safeguarding digital assets and ensuring business continuity.

Program Fee

PHP 50,000 or USD 900*

*Final USD amount may vary based on
the exchange rate at the time of payment.

Interested in early bird or group discounts?

Group enrollment spiel: Get 5% off the program fee for group of 3 to 6 pax
and 10% for group of 7 pax and above.

Earning a Postgraduate Certificate and Postgraduate Diploma

AIM SEELL offers Postgraduate Stackable Certificate Courses in various areas of concentration and discipline, which build an individual's qualifications and distinguish their professional value. It enables professionals to develop their proficiency in diverse areas of concentration in a personalized and more manageable manner. By successfully completing SEELL's programs, credentials can be earned over time, stacked towards earning a Postgraduate Certificate in an area of their choice, and ultimately, a Postgraduate Diploma in Management. This leads to more career opportunities, advancement, and potentially high-paying jobs.

Earning Credentials

Alumni Status will be Granted upon completion of the program

Upon completion of the program, the participant will earn **two (2)** unit, which can be credited toward the following:

- Postgraduate Certificate in Data Privacy and Cybersecurity
  Postgraduate Diploma in Management

*Postgraduate Certificate requires 5 units earned within 2 years
*Postgraduate Diploma requires 20 units earned within 3 years

For guidance on other eligible programs for Postgraduate Certificates and designing your learning journey with SEELL, please email us at SEELL@aim.edu or visit our website at https://aim.edu/executive-education/