

**OPEN ENROLLMENT
PROGRAM**



Iclif Executive Education Center

CYBER RESILIENCE AND COMPLIANCE



PROGRAM DETAILS

FACULTY	DATE/TIME	FEE*	VENUE
Atif Ahmad Sean Maynard Michael Lim	15 April 2026 9.00AM - 5.00PM	RM3,500 USD875	Asia School of Business

Note: *

- Excludes Sales & Service Tax (8%)
- Fee excludes accommodation at ASB Residential for outstation/ overseas participants but can be arranged at additional cost.
- USD Pricing is indicative pricing. All fees are invoiced in Malaysian Ringgit (RM). USD amounts are shown for reference only and will vary based on the prevailing exchange rate at the time of payment.

Program Overview

As organizations face increasingly sophisticated cyber threats, cybersecurity has evolved from a technical issue to a critical boardroom priority.

The program is designed specifically for board directors and senior management who need to elevate their cybersecurity governance capabilities. It will equip participants with the strategic understanding and governance frameworks needed to oversee cybersecurity risks in the Malaysian context more effectively. Participants will gain comprehensive insight into Malaysia's cybersecurity ecosystem and regulatory requirements under the Cybersecurity Act 2024, with clear guidance on directors' and senior management legal obligations and personal liability considerations.

Through immersive case-based learning, interactive role plays, peer discussions, and practical application exercises, participants will develop the confidence to set clear roles and responsibilities, embed cybersecurity in risk management frameworks, and fulfill governance and management responsibilities during active cyber incidents. The program concludes by revisiting the opening scenario, allowing participants to apply governance principles to real-world situations.

Delivered by distinguished cybersecurity experts with extensive experience advising corporate boards and government agencies, this program bridges the gap between technical complexity and strategic oversight - empowering directors and management to govern with confidence in an increasingly interconnected world.

Learning Outcomes

At the end of the program, participants will be able to:

- Explain the Malaysian cybersecurity ecosystem and governance structure
- Identify legal obligations under the Cybersecurity Act 2024
- Apply strategic frameworks for cybersecurity oversight
- Develop appropriate questions to evaluate cybersecurity risk
- Discuss board and management responsibilities during cyber incidents
- Discuss how to apply governance practices that create organizational cyber resilience

Who Will Benefit?

- Board of Directors
- Board Risk Committee Members
- Senior Management
- Anyone who might find this program helpful

Program Outline

Session 1: Opening Case Scenario & Interactive Discussion

- Immersive scenario describing a cyber incident affecting a Malaysian critical infrastructure organization
- Individual reflection on governance challenges
- *Small Group Role Play*: Board Director-CEO-CIO crisis discussions
- *Plenary Discussion*: What are your key cybersecurity challenges?

Session 2: Malaysian Cybersecurity Ecosystem & Cybersecurity Act 2024

- Case studies of Cybersecurity in Malaysia
- Overview of Malaysia's Cyber Agencies and Regulatory bodies (NACSA, NSC etc.)
- Code of Practice implications for critical infrastructure
- Directors' duties and personal liability
- Compliance timeline and enforcement mechanisms
- *Interactive Discussion*: Which external bodies do you contact during a cyber incident?
- *Expert Panel Q&A*: Implications of Malaysia's laws and regulation on the Organizational Leadership

Session 3: Strategic Cybersecurity Governance

- Setting clear roles and responsibilities (Board, Executive Leadership vs Management)
- Embedding cybersecurity in risk management frameworks
- Key questions directors and executives should be asking
- *Interactive Discussion*: In your last board meeting, what was the most technical term in the cybersecurity report? How did you handle it?
- *Role Play*: Bridging the Communications Gap between Cybersecurity Teams and Board Leadership
- *Leadership Application Exercise*: Developing questions for your management team and board

Session 4: Cyber Crisis Management for Directors and Executives

- *Readiness*: Planning and preparedness at board and executive levels
- *Response*: Board and executive roles during active incidents
- *Recovery and remediation* in the Malaysian context
- *Interactive Discussion*: Who in your organization has authority to pay a ransom, shut down operations, or publicly disclose a breach? Did the board explicitly delegate these authorities?
- *Expert Panel Q&A*: Crisis management and governance decision-making

Session 5: Case Revisited - Applying Governance Principles

- Application of learned principles to opening case scenario
- *Small Group Workshop*: Developing Key Questions for your Management Team
- *Implementation Planning*: Personal commitments and next steps
- *Closing Reflection*: What changes at your next board or leadership meeting?

Faculty



Prof Atif Ahmad is Professor of cybersecurity practice at the University of Melbourne and Deputy Director of the Academic Centre of Cyber Security Excellence. With over 20 years of teaching experience in cybersecurity at undergraduate and postgraduate levels, he has been appointed as Subject Matter Expert for Malaysia's National Cyber Security Strategy 2025-30. His areas of expertise include cyber defence capability, threat intelligence, incident response, and security risk management.

Prior to his academic career, Prof Ahmad worked as a consultant for WorleyParsons and Pinkerton, where he conducted cyber-risk assessments for critical infrastructure and evaluated compliance with ISO security standards. Throughout his career, he has secured over AUD6 million in research funding and published more than 103 peer-reviewed papers that have been cited more than 5,000 times. His research employs social science methods to understand and improve organizational cybersecurity practices, with a focus on developing models that enhance cyber incident response capabilities.

Prof Ahmad has led numerous international teams developing cyber resilience across Southeast Asia, assisting major banks and telecommunications companies to develop their cyber defence capabilities. His ethnographic studies of Australia's leading cyber practices have resulted in several models that improved 'best practice' for cyber operations teams, particularly at leading critical infrastructure organizations in Australia and Malaysia. These insights drive his agenda for capacity building in South-East Asia.

Prof Ahmad has developed numerous industry-centered curricula for cybersecurity management and created award-winning educational films that have won 17 international awards. He regularly delivers masterclasses for Australian foreign aid programs to Malaysia and India, and received the Faculty Teaching & Learning Engagement Award in 2021. He serves as Associate Editor for the prestigious journal *Computers & Security* and has significantly contributed to improving the cyber resilience of organizations across the Asia-Pacific region.



Dato' Dr. Michael Lim is a Retired Deputy Commissioner of the Royal Malaysia Police with over 37 years of experience in security operations. Currently serving as a Senior Lecturer at Enforcement, Leadership and Management University and Visiting Lecturer at the Centre for Cyber Security, University Kebangsaan Malaysia, he brings extensive practical expertise in cybersecurity, protective security, and intelligence operations to the program.

Dr Lim completed his PhD in Information Security (Cybersecurity Culture and Practice) from the University of Melbourne, augmented by a Master of Business Administration from Charles Sturt University, Australia, and a Master of Computer Science from University Putra Malaysia. His career in the Royal Malaysia Police included high-profile roles such as Deputy Director of Cyber Crime (2024-2025), Assistant Director of Protective Security (2023-2024), and Assistant Director of Intelligence Technical (2020-2023).

Throughout his distinguished career, Dr. Lim managed portfolios including Computer Crime and Human Trafficking. His professional certifications include Certified Identity Access Manager (CIAM) and Certified Security Culture Practitioner (CSCP). As a research consultant, he is currently involved in projects with the University of Melbourne on cyber incident response capability and cyber leadership in Malaysia.

Dr Lim has presented at numerous conferences on cybersecurity, AI, and the intersection of cybersecurity and mental health. As an adjunct lecturer at several Malaysian universities, he teaches in Master of Protective Security Management, Master of Law Enforcement, and Bachelor of Computer Science programs. His research on organizational security culture has been published in international conferences, including the Pacific Asia Conference on Information Systems and the Australian Information Security Management Conference. Dr. Lim brings a unique blend of practical law enforcement experience, academic knowledge, and regional cybersecurity expertise to the program.

Faculty



Professor Sean Maynard is Associate Dean (Academic) at the Faculty of Engineering and IT and Professor in the School of Computing and Information Systems at the University of Melbourne. With 29 years of experience at the University, he has been appointed a Subject Matter Expert for the Malaysia Security Strategy (2025-2030) by the Malaysian Security Council. His areas of expertise include cybersecurity management, business analytics, organizational security culture, and information security governance.

Prof Maynard has a PhD in Information Systems from the University of Melbourne, supplemented by a Master of Computing and Bachelor of Computing Honours from Monash University. Throughout his career, he has secured over AUD2.39 million in research grants and published 106 peer-reviewed papers with more than 4,079 citations. His research bridges the gap between academia and real-world application, focusing on how organizations can adapt to the evolving cybersecurity threat landscape.

Professor Maynard serves on the editorial board of Computers & Security and has held leadership positions in academic conferences, including as Program Chair for the Australasian Conference on Information Systems (2022).

Prof Maynard has led significant curriculum redesign initiatives and received the FEIT Teaching & Learning Engagement Award in 2021 for his case-based learning approaches to cybersecurity education. He has contributed to five Department of Foreign Affairs and Trade (DFAT) grants since 2022 for research in Malaysia, focusing on developing the nation's cyber response capability, cyber resilience, and strategic thinking in cybersecurity.



Asia School of Business (DU046(W))

Iclif Executive Education Center

ASB Academic, No 11, Jalan Dato' Onn, 50480 Kuala Lumpur

Email: ExecEd@asb.edu.my

exec.asb.edu.my



[asbiclif](#)



[@asb.iclif](#)



[asbiclif](#)



[asb iclif](#)

SCAN ME



[Cyber Resilience and Compliance](#)

