Last Updated: 16 January 2026

OPEN ENROLLMENT PROGRAM

Jointly organized by ASBM and AICB

AICB 8 CPD HOURS

ASIASchool of Business in collaboration with MIT Sloan Management

Iclif Executive Education Center

PERSONAL INFORMATION SECURITY MANAGEMENT:
PROTECTING YOURSELF & YOUR ORGANIZATION

HRDCORP CLAIMABLE

PROGRAM DETAILS

FACULTY	DATE/TIME	FEE*	VENUE
Atif Ahmad Sean Maynard Michael Lim	16 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

Designed specifically for board directors and C-suite executives, this one-day program equips participants with the practical knowledge and strategic frameworks needed to protect themselves and their organizations from evolving cyber threats. Whether you serve on the board or lead the organization, you will gain comprehensive understanding of why executives are targeted, how attackers operate, and what specific actions you must take to secure your personal digital life in ways that strengthen organizational resilience.

Through immersive case-based learning, participants will develop confidence in implementing personal security measures while understanding their role in leading organizational security culture. You will learn to recognize sophisticated social engineering tactics, implement essential technical controls like MFA and password management, secure home networks and personal devices, and develop operational security practices for travel and remote work.

The program emphasizes the critical connection between personal cybersecurity practices and fiduciary duties. Board members serving on multiple companies could potentially create a "human supply chain" whereby one successful cyberattack could result in extensive access and opportunity at multiple organizations. Your personal security is not just about self-protection – it is about fulfilling your governance responsibilities and setting the standard for organizational culture.

Delivered by distinguished cybersecurity experts with extensive experience advising Malaysian boards and government agencies, this program provides actionable guidance grounded in Malaysian regulatory requirements and real incidents affecting Malaysian organizations.

Learning Outcomes

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

- Recognize why executives are high-value targets and understand specific threat vectors
- Implement fundamental personal security controls (MFA, password management, device security)
- Apply information lifecycle thinking to personal and organizational information management
- Develop operational security (OpSec) practices for daily activities, travel, and remote work
- Lead organizational security culture through personal example and visible commitment
- Execute immediate response protocols when targeted or compromised
- Create actionable personal security plans with immediate, short-term, and ongoing measures

Who Will Benefit?

- Board of Directors
- Business Leaders
- C-Suite Executives
- Anyone who might find this program helpful

Program Outline

Session 1: Opening Case Scenario - The Executive Compromised

- Immersive whaling attack: CFO receives WhatsApp from "CEO" requesting transfer
- Initial response discussion: What red flags exist and what would you do in real-time?
- Personal device vulnerabilities and how authority dynamics disable critical thinking
- Setting the stage for understanding executive-targeted attacks and their devastating potential

Session 2: The Executive as High-Value Target

- Why you're in the crosshairs: access to strategic decisions, financial authority, and the "human supply chain" effect
- Cyber incidents in Malaysia: impersonation and fraud
- The aggregation effect: how LinkedIn profiles, social media, and public appearances become attacker intelligence
- Immediate response protocols: the critical first 30 minutes that determine fund recovery success

Session 3: Personal Security Fundamentals – Your First Line of Defence

- Understanding information as dynamic asset: storage, circulation, and transmission vulnerabilities
- Classification frameworks: bridging personal and organizational information across multiple board roles
- Handling protocols: from board materials on personal devices to secure disposal and cloud storage settings
- Passwords, devices and networks security: encryption, biometric authentication, and securing the vulnerable home network
- Software updates and backup strategies: closing exploitable gaps and building ransomware resilience

Session 4: Advanced Personal Protection Strategies

- Operational Security (OpSec) methodology: identifying what about you is valuable and where you are exposed
- Social media and digital footprint audit: limiting travel plans, family details, and strategic information exposure
- Communication security: verification protocols that save millions without insulting colleagues
- Home network and IoT threats: how Internet-connected pianos and smart devices create corporate vulnerabilities

Session 5: Case Revisited – Strategic Personal Security Planning

- Application of verification protocols and OpSec principles to opening scenario
- Group development of personal action plans: immediate (MFA, password manager), short-term (home network audit), ongoing
- Individual commitment cards: specific actions participants pledge to implement within defined timeframes
- Final debrief: personal cybersecurity excellence as organizational leadership imperative and fiduciary responsibility

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
in collaboration with MIT Sloan Management
Iclif Executive Education Center

AACSB ACCREDITED

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

Personal Information Security Management – Protecting Yourself & Your Organization