PROTECT MALAYSIA2026

LEADERSHIP SERIES
MASTERCLASS

POWERED BY
PURPLE DOOR

HRDC CLAIMABLE

CYBER CRISIS LEADERSHIP IN THE AGE OF AI

AI IS ACCELERATING CYBER THREATS

WHAT ONCE TOOK DAYS
NOW HAPPENS IN **MINUTES**

IS YOUR ORGANISATION READY?

30 JULY 2026
W HOTELS, KUALA LUMPUR

A One-Day Executive Masterclass
for Industry and Regulatory Leaders

Professor Dr Atif Ahmad
Director
Melbourne Security Associates

FEATURING GUEST SPEAKER

Dato' Dr Michael Lim
Director
Melbourne Security Associates

www.protect.com.my
hello@protect.com.my
training@protect.com.my
For booking, please contact
HOTLINE +6010 944 9228 | +6017 752 1389 | +6017 686 9286

CYBER CRISIS LEADERSHIP
IN THE AGE OF AI

A One-Day Executive Masterclass for Industry and Regulatory Leaders

Artificial intelligence is reshaping the cyber threat landscape at unprecedented speed. New attack classes are emerging, threat actors are scaling operations with AI and crisis decisions that once unfolded over days must now be made within minutes.

Today's leaders face information overload, fragmented intelligence and governance frameworks not built for the realities of AI driven cyber risk.

Designed for senior executives, regulators and decision makers, this masterclass equips leaders to govern, respond and lead confidently through high impact cyber crises in an increasingly volatile digital environment.

As Malaysia advances its national agenda on AI, cybersecurity and digital resilience, the focus is no longer awareness. It is execution.

Built around a live immersive cyber crisis simulation, participants will navigate the full lifecycle of a modern AI enabled incident, from operational disruption and executive escalation to regulatory scrutiny, media pressure and strategic recovery decisions.

More than a masterclass, this is an executive leadership simulation designed to strengthen judgement, crisis governance and organisational resilience in the age of AI.

> "Sarawak started the national conversation. Kuala Lumpur now operationalises it, translating strategy into leadership readiness, institutional capability and real-world crisis response."

WHO SHOULD ATTEND

Board Members | Chief Executive Officers (CEOs) | Chief Information Officers (CIOs) | Chief Information Security Officers (CISOs) | Risk and Governance Leaders | Regulators and Policy Makers | Legal Counsel and Compliance Leaders | Government-Linked Company (GLC) Executives | Critical Infrastructure Operators | AI Governance and Responsible AI Teams | Public Sector Digital Transformation Leaders

STRATEGIC LEADERSHIP OUTCOMES

A clear understanding of how AI is reshaping the threat landscape and the conditions under which senior leaders make decisions during a crisis.

Strategic frameworks for cyber oversight that hold up when the adversary has AI capability

Familiarity with obligations of the Cybersecurity Act 2024 and Personal Data Protection Act 2024 and an informed view of where the Malaysian government is at on AI.

A practical understanding of how leadership decision-making is likely to change as AI compresses attack speed and degrades the conditions for situation awareness.

A short personal action plan and a peer network of senior leaders from across Malaysia's critical sectors.

HOW THIS MASTERCLASS DIFFERS

This is not a conventional cybersecurity masterclass. Designed for senior leaders and decision makers, the programme moves beyond theory into a sustained live cyber crisis simulation where leadership judgement, governance and response are tested in real time.

The masterclass takes a practical and candid approach to AI governance, focusing not only on what is known, but also on the uncertainties organisations must now prepare to lead through.

PROGRAM DELIVERY

DELIVERED BY	Melbourne Security Associates in partnership with Purple Door
FACILITATORS	**Professor Atif Ahmad** and **Dato' Dr Michael Lim** (former Deputy Head of Computer Crime, Royal Malaysia Police)
FORMAT	Interactive executive masterclass with case-based learning and certificate of completion. Recommended 20 to 30 senior leaders from Malaysia's government, regulators, GLCs, critical infrastructure, financial services and academia.

SPEAKER PROFILES

PROFESSOR DR ATIF AHMAD

Director
Melbourne Security Associates

Dr Atif Ahmad is a Director of Melbourne Security Associates and a full professor of cybersecurity at a leading Australian university. He holds a PhD from the University of Melbourne and has 25 years of expertise in cyber strategy, incident response, threat intelligence, and intellectual property protection. He is a Subject Matter Expert appointed by Malaysia's National Security Council to the National Cyber Security Strategy 2025-30, and has trained more than 300 industry leaders and senior public servants including Directors of CNII institutions.

DATO' DR MICHAEL LIM

Director
Melbourne Security Associates

Dato' Dr Michael Lim is a Director of Melbourne Security Associates and a former Deputy Commissioner of Police with the Royal Malaysia Police, where he served as Deputy Head of Computer Crime and played a key role in strengthening Malaysia's national cybercrime investigation capabilities. He brings extensive experience in law enforcement leadership and digital forensics, contributing significantly to Malaysia's cyber policing and digital security landscape. He holds a PhD from the University of Melbourne, and brings a rare combination of operational policing experience and academic depth, bridging frontline cybercrime enforcement with strategic insight into emerging digital threats.

DAY 1 Cyber Crisis Leadership in the Age of AI

A full day executive masterclass comprising six interconnected parts driven by one continuous live cyber crisis simulation. Designed to strengthen leadership judgement, crisis response and decision making in the age of AI.

09:00am	09:15am	**OPENING AND WELCOME** Program framing, introductions, opening from the host. Why a masterclass on AI and cyber leadership matters now.
09:15am	10:30am	**PART 1	OPENING CASE SCENARIO** Immersive case scenario set in a Malaysian critical infrastructure organisation. The threat actor is using AI: synthetic media of a senior executive, automated reconnaissance, and AI-generated social engineering at scale. The defender is not. The organisation has hours, not days, before the situation deteriorates. Participants work through their first-hour response as directors and executives, followed by table discussion and plenary debrief.
10:30am	10:45am	**BREAK**
10:45am	11:45am	**PART 2	STRATEGIC APPROACH TO CYBERSECURITY** Presentation (45 min): how to think about cyber from a strategic perspective. Balancing assets, threats, risks, and controls. Identifying the crown jewels: digital platforms, sensitive information, trade secrets, and trust assets. Activity (15 min): identifying your organisation's crown jewels and the controls currently protecting them.
11:45am	12:45pm	**PART 3	THREAT ACTORS SUPERCHARGED BY AI** Presentation (45 min): how AI is changing the capability of threat actors. Synthetic media and executive impersonation. AI-generated phishing at industrial scale. Automated reconnaissance and attack tooling. The collapse of traditional indicators of compromise. Why the threat landscape of 2026 is materially different from that of 2023. Activity (15 min): each table identifies the AI-enabled threat scenario most plausible against their own organisation in the next twelve months.
12:45pm	01:45pm	**LUNCH**
01:45pm	02:45pm	**PART 4	MALAYSIAN CONTEXT** Cases of cyber attacks in Malaysia and their regulatory aftermath. The national governance structure under the Cybersecurity Act 2024 and the Personal Data Protection Act 2024. The role of NACSA, the Department of Personal Data Protection, and law enforcement during a cyber incident. A short closing segment on where the Malaysian government is at on AI governance and the work currently in progress. Activity (15 min): brief self-assessment of your organisation's exposure under CSA 2024 and PDPA 2024 obligations.
02:45pm	03:00pm	**BREAK**
03:00pm	04:15pm	**PART 5	CRISIS LEADERSHIP WHEN SITUATION AWARENESS COLLAPSES** On the cyber incident lifecycle from a leadership perspective: detection, containment, eradication, recovery, learning. How threat intelligence should flow into incident decision-making. In-depth case of an exemplar financial institution showing intelligence-led crisis response. Closing segment: anticipating how AI will change crisis dynamics, including the compression of decision windows when the adversary has AI capability and the defender does not.
04:15pm	05:00pm	**PART 6	CASE REVISITED AND ACTION PLANNING** Return to the opening case with the day's frameworks now in hand. Facilitated table discussion. Each participant develops a short personal action plan: three things to take back to their organisation on Monday.
05:00pm	05:15pm	**CLOSING** Synthesis of the day, certificate presentation, and closing remarks.