WORKSHOP CONTENT OUTLINE

Incident Response and Cyber Threat Intelligence: A Workshop for Leaders Working on Malaysia's Cyber Crime Response

Prepared for PDRM reference, ahead of the 18 May 2026 workshop in Kuala Lumpur

Date	18 May 2026
Venue	Majestic Hotel, Kuala Lumpur
Duration	One day, 9:00 am to 5:15 pm
Participants	30 pax. CSAM members, senior police officers, and regulators associated with the CCFC initiative
Delivered by	Melbourne Security Associates, on behalf of the University of Melbourne research team, whose work was sponsored by the Australian Government (DFAT[1]) and supported by NACSA

Workshop orientation

Malaysia is building a national capability for responding to cyber-enabled crime, with the Cyber Crime Fusion Centre as its anchor institution. The leaders in the room on 18 May are among those who will shape, oversee, or work alongside that capability as it develops.

This workshop is designed for the leadership and middle management tier of that audience. It provides a working understanding of two capabilities that sit at the heart of any modern cyber defence posture: cybersecurity incident response, and cyber threat intelligence. Both are drawn from the Australian and Malaysian empirical research the University of Melbourne team has conducted over the past five years, including current fieldwork funded by the Australian Government through the Cyber and Critical Tech Cooperation Program.

The day is built around a single immersive scenario that frames the content at the start and is revisited at the end. Participants engage with the scenario cold, then work through seven substantive modules, then return to the scenario to identify what they would do differently. The format is experiential by design: each module combines concise input with structured discussion, so participants spend the day thinking, arguing, and comparing their own practice against what the research shows.

Scope

The material is grounded in organisational and strategic incident response and cyber threat intelligence practice. It draws on how Australian and Malaysian organisations respond to cyber incidents and how they operate intelligence functions. It does not cover law enforcement investigation workflows or fraud investigation procedures, which sit with specialist agencies.

[1] Australian Department of Foreign Affairs & Trade

Day at a glance

9:00 – 9:30	Opening Case Scenario
9:30 – 10:15	Module 1: Introduction to Cybersecurity
10:15 – 11:00	Module 2: The Threat Landscape
11:00 – 11:15	Break
11:15 – 12:15	Module 3: Introduction to Cyber Incident Response
12:15 – 1:00	Module 4: Cyber Crime in Malaysia
1:00 – 2:00	Lunch
2:00 – 3:00	Module 5: The Practice of Cyber Incident Response in Organizations
3:00 – 4:00	Module 6: The Practice of Cyber Threat Intelligence in Organizations
4:00 – 4:15	Break
4:15 – 5:15	Module 7: Case Revisited, Learnings, and Close

Module detail

MODULE 0 OPENING CASE SCENARIO

Lead: *Professor Atif Ahmad*

Participants are immersed in an unfolding cyber-enabled crime incident affecting a Malaysian organisation. Working in small groups, they discuss how they would recognise, interpret, and respond to what is happening in front of them. No frameworks, no prompts. The purpose is to surface the instincts and assumptions participants bring into the room, which the rest of the day will test and refine.

How it runs:

Scenario narration at the front of the room, followed by table discussion of initial decisions and information needs. Participants are given an incident briefing sheet they keep for the day and return to in Module 7.

Content covers:

- An immersive incident narrative reflecting the kinds of cyber-enabled crime affecting Malaysian organisations
- Facilitated group discussion surfacing initial decisions and information needs
- Identification of the governance and operational questions the rest of the day will address

MODULE 1 INTRODUCTION TO CYBERSECURITY

Lead: *Professor Atif Ahmad*

Foundational scene-setting for the day. What cybersecurity means as a discipline at enterprise level, why it has moved from a technical concern to a strategic one, and how the language and concepts used across the rest of the day fit together. This module establishes the shared vocabulary and mental model the room will use through to the close of the day.

How it runs:

Concise input from the front, followed by a short paired exercise in which participants translate the core cyber concepts into the language of their own organisation.

Content covers:

- What cybersecurity actually protects: assets, information, trade secrets, digital platforms
- The shift from a technology problem to a strategic and enterprise-wide problem
- The tension between business, technology, and leadership perspectives on cyber risk
- The core concepts the rest of the day will draw on: assets, threats, risks, controls

MODULE 2 THE THREAT LANDSCAPE

Lead: *Professor Atif Ahmad*

A structured view of who is conducting cyber-enabled crime, why, and how. The module covers threat actor typologies, motivations, capabilities, and the way organised criminal enterprises have professionalised over the past decade. It deliberately prepares the ground for the afternoon's cyber threat intelligence content by surfacing the questions leaders need to be able to ask about the threats they face.

How it runs:

Input on threat actor typologies, followed by a table exercise in which participants map the threat actors most relevant to their own sector and surface the assumptions driving their choices.

Content covers:

- Threat actor typologies relevant to Malaysian organisations and the wider region
- How threat actor capability has shifted: organised, persistent, commercially motivated, geographically distributed
- The link between understanding threats and making resource decisions
- Foundational questions leaders should be asking about their threat environment, revisited in the afternoon through the CTI research findings

MODULE 3 INTRODUCTION TO CYBER INCIDENT RESPONSE

Lead: *Professor Atif Ahmad*

The conceptual foundation for incident response. What an incident response capability actually consists of, how the standard lifecycle is meant to work, and why real incidents tend to stress that lifecycle in predictable ways. The module sets up the afternoon's Module 5, where the practice of incident response in real organisations is examined in depth.

How it runs:

Input on the incident response lifecycle grounded in short case snapshots, followed by a table exercise in which participants walk a sample incident through the lifecycle and identify the decision points that matter most from a leadership perspective.

Content covers:

- What incident response is and what it is not
- The standard incident response lifecycle: preparation, detection, containment, eradication, recovery, lessons learned
- Where incident response typically fails under pressure
- The three-layer response structure: security operations, security leadership, executive and board
- The questions leaders should be asking about their own incident response readiness

MODULE 4 CYBER CRIME IN MALAYSIA

Lead: *Dato' Dr Michael Lim*

Michael draws on thirty-seven years of service in the Royal Malaysia Police, including his time as Deputy Director of Cyber Crime, to ground the morning's frameworks in the Malaysian operational reality. He uses scams as illustrative case material: not as a curriculum on fraud investigation, but as the lens through which the audience can see how cyber-enabled crime actually moves through Malaysian organisations, law enforcement, and regulatory bodies. This is the module where international frameworks meet the local picture.

How it runs:

Storytelling-led session structured around illustrative scam cases from Michael's time at PDRM, followed by a facilitated Q and A in which participants probe the cases against their own working assumptions.

Content covers:

- How cyber-enabled crime presents itself on the ground in Malaysia
- Inter-agency coordination during active incidents: how it works, where it breaks down, where national-level coordination makes the difference
- Stories from the field that illustrate the gaps between policy intent and operational reality
- Reflections on the cultural, institutional, and practical conditions that shape how national cyber capability takes hold in Malaysia

MODULE 5 THE PRACTICE OF CYBER INCIDENT RESPONSE IN ORGANIZATIONS

Lead: *Professor Atif Ahmad, with Professor Sean Maynard*

The first of the afternoon's two empirical modules. This session moves beyond the lifecycle presented in Module 3 and into how incident response actually plays out inside real organisations. Drawing on the University of Melbourne research team's in-depth case studies of high-maturity and low-maturity organisations in Australia and Malaysia, the module surfaces what distinguishes effective response from ineffective response, and why the differences matter at enterprise scale.

How it runs:

Comparative case walkthrough contrasting a high-maturity organisation with a low-maturity counterpart across the maturity model dimensions, followed by a table exercise in which participants locate their own organisations on the maturity spectrum.

Content covers:

- What mature incident response actually looks like in practice, versus what is written in plans
- Organisational situation awareness: how effective organisations perceive, comprehend, and project during a cyber crisis
- Comparative insights from exemplar Australian and Malaysian financial institutions
- A maturity model for incident response and the dimensions that carry the most weight
- The behavioural and structural patterns that distinguish defence-driven from compliance-driven organisations

MODULE 6 THE PRACTICE OF CYBER THREAT INTELLIGENCE IN ORGANIZATIONS

Lead: *Professor Atif Ahmad, with Professor Sean Maynard*

The second empirical module of the afternoon. This session presents what cyber threat intelligence looks like as a practised capability inside real organisations, drawing on the University of Melbourne team's multi-year research program. It covers findings from two in-depth Australian bank case studies, and shares emerging observations from the Malaysian fieldwork currently underway under the Cyber and Critical Tech Cooperation Program. Framed as research in progress, it invites the room into a genuine discussion about what the findings suggest.

How it runs:

Input on the CTI lifecycle anchored in the Australian case findings, with the Malaysian observations presented as a research-in-progress update. Followed by a table exercise in which participants locate their own organisations on the CTI practice continuum.

Content covers:

- What cyber threat intelligence is, and what it is not
- The CTI lifecycle: direction, collection, processing, analysis, dissemination
- Findings from two in-depth Australian case studies, published in Computers and Security
- The distinction between CTI that informs decisions and CTI that sits in reports
- Emerging observations from the Malaysian fieldwork, presented as research in progress
- Implications for how a mature national-scale CTI function might position, resource, and evaluate itself

MODULE 7 CASE REVISITED, LEARNINGS, AND CLOSE

Lead: *Professor Atif Ahmad, with Professor Sean Maynard and Dato' Dr Michael Lim*

The day closes by returning to the opening scenario. Participants re-enter the same incident they discussed cold at 9:00 am, now equipped with the incident response and cyber threat intelligence frameworks covered during the day. Small groups work through the scenario again, then the full room reconvenes for a facilitated debrief led jointly by the three faculty members. The purpose is to make the shift in thinking visible to the participants themselves, and to surface the learnings each participant takes back into their role.

How it runs:

The opening scenario is re-injected at the point it was paused in the morning. Participants rework it in small groups and then reconvene for a full-room debrief, with each faculty member contributing a closing reflection that draws the threads of the day together.

Content covers:

- Re-engagement with the opening scenario using frameworks introduced during the day
- Small-group working session followed by full-room debrief
- Joint faculty reflection: what the day surfaced, where the capability gaps appear to sit, what needs sustained attention
- Close and next steps

Faculty

The workshop is delivered by three faculty members, each bringing a distinct contribution to the day.

Professor Atif Ahmad	Full Professor of Cybersecurity at the University of Melbourne, Deputy Director of the Academic Centre of Cyber Security Excellence, and founding director of Melbourne Security Associates. Subject Matter Expert to NACSA for Malaysia's National Cyber Security Strategy 2025–30. Lead investigator on the current DFAT-funded research into cyber threat intelligence practice in Malaysian organisations. Anchors the cybersecurity, threat, and incident response content across the morning, and leads the afternoon's empirical research modules.
Professor Sean Maynard	Professor at the University of Melbourne, co-investigator on the incident response and cyber threat intelligence research program, and a specialist in cybersecurity governance and strategic decision-making. Co-presents the empirical practice modules in the afternoon.
Dato' Dr Michael Lim	Thirty-seven years with the Royal Malaysia Police, including service as Deputy Director of Cyber Crime from 2024 to 2025. PhD in Information Security from the University of Melbourne. Visiting Lecturer at UKM. Leads Module 4 on the Malaysian operational reality and joins the closing module.

A note on the research base

The incident response and cyber threat intelligence content presented during the day draws on a decade of published research in Computers and Security, the European Journal of Information Systems, Decision Support Systems, the International Journal of Information Management, and the Journal of the Association for Information Science and Technology. The Malaysian material is from fieldwork currently underway in partnership with the International Islamic University Malaysia, funded by the Australian Government's Cyber and Critical Tech Cooperation Program.

The material has been selected for its relevance to the work participants do. The intention is that everyone in the room leaves with a working understanding of what mature incident response and cyber threat intelligence look like in practice, and a sharper sense of the questions worth asking about their own environments.