
AI-Enabled Cyber Threats, Resilience and Executive Response Training Course

10 – 14 October 2027
Kuala Lumpur





AI-Enabled Cyber Threats, Resilience and Executive Response Training Course

Ref: 256_19173 **Date:** 10 – 14 October 2027 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

AI-enabled cyber threats, resilience and executive response is the subject of this one-week training course for non-technical senior leaders at managerial to strategic level, ending in an executive cyber resilience playbook. Attackers now use AI to impersonate colleagues and scale fraud, while organisations adopt AI systems that add new failure points. The approach moves from threat and exposure, through resilience design and AI system risk, to crisis decisions and a rehearsed response. Mars Training Centre UK delivers this programme in AI-enabled cyber threats and resilience.

The Business Case

Cyber incidents are decided in the first hours, and the people deciding are rarely technical. Leaders who understand how AI changes attack methods, which services cannot stop and who may authorise recovery steps can act faster, communicate consistently and protect the services that customers and regulators care about most.

- Service Disruption Duration: Shortens as recovery priorities and decision rights are agreed before an incident.
- Exposure to Impersonation Fraud: Falls as verification rules and awareness measures address AI-generated deception.
- Board Oversight Quality: Improves as leaders ask for evidence on resilience instead of general assurances.

Principles and Evidence Base

- ISO/IEC 27001: Its information security management requirements frame the risk and control questions leaders ask in Sessions 1 and 2.
- ISO 22301: Its business continuity management requirements shape the impact analysis and recovery priorities in Session 3.
- NIST Cybersecurity Framework: Its Identify, Protect, Detect, Respond and Recover functions organise the crisis and recovery work in Sessions 4 and 5.
- ISO/IEC 42001: Its AI management system requirements guide the oversight of AI systems in Session 2.



Intended Participants

- Directors accountable for services that must keep running during a cyber incident.
- Executives who sit on crisis or incident committees and approve recovery decisions.
- Heads of function who depend on technology but do not manage it.
- Board advisers who challenge management on cyber and AI risk.

The programme serves banking, energy, healthcare, government and telecommunications organisations.

Learning Outcomes

1. Participants will be able to evaluate how AI changes the methods, speed and reach of cyber attacks on their organisation.
2. Participants will be able to diagnose exposure created by the organisation's own use of AI systems and suppliers.
3. Participants will be able to construct impact tolerances and recovery priorities for critical services.
4. Participants will be able to prioritise protective measures by business impact rather than technical detail.
5. Participants will be able to justify crisis decisions, including communication and recovery trade-offs, under time pressure.
6. Participants will be able to design an executive cyber resilience playbook with named decision owners.

Programme Structure

Day 1: AI-Enabled Cyber Threats for Non-Technical Leaders

How does AI change who attacks, how and how fast?

- Attack Lifecycle in Plain Terms
- AI-Generated Phishing, Voice and Video Impersonation
- Ransomware and Extortion Business Models
- Threat Briefing Format for Executives
- Case Review of Two Sector Incidents

Day 2: Exposure and AI System Risk

Where is the organisation exposed, including through its own AI use?

- Critical Asset and Service Exposure Map
- ISO/IEC 27001 Risk and Control Questions for Leaders
- Supplier and Cloud Dependency Review
- AI System Misuse, Data Leakage and Model Manipulation
- ISO/IEC 42001 Oversight Checklist for AI Tools



Day 3: Operational Resilience Design

Which services must not fail, and how long can they be down?

- Business Impact Analysis Under ISO 22301
- Impact Tolerance Statements
- Recovery Priority and Dependency Sequencing
- Backup, Recovery and Manual Workaround Options
- Resilience Investment Trade-Off Table

Day 4: Crisis Leadership and Response Decisions

Who decides what in the first hours of a cyber crisis?

- NIST Respond and Recover Functions for Executives
- Crisis Team Roles and Decision Rights
- Ransom, Disclosure and Shutdown Decision Framework
- Stakeholder and Media Communication Plan
- Timed Incident Simulation

Day 5: Applying AI-Enabled Cyber Threats Resilience to a Playbook

Is the playbook ready to be adopted and rehearsed?

- Applying the Session 1 Threat Briefing to a Chosen Organisation
- Applying Session 2 Exposure Findings to Priority Services
- Testing Session 3 Tolerances Against the Simulation Outcome
- Assigning Decision Owners and Escalation Triggers
- Completing the Executive Cyber Resilience Playbook

Methodology

The programme is built around scenario simulation and case analysis. Participants work through a staged incident in a mixed leadership team, making decisions with partial information, then review what the choices cost. No programming or technical tools are used.

- Suggested activity: Judging a suspected voice-clone payment request and setting a verification rule.
- Suggested activity: Ranking critical services and agreeing tolerances in a role-played committee.
- Suggested activity: Briefing a mock board on an incident after the first twelve hours.



Capstone Output

Each participant completes an executive cyber resilience playbook for one organisation or business unit. It contains a threat briefing, an exposure map, impact tolerances, recovery priorities, decision rights, communication holding statements and escalation triggers. It is used to brief the executive team and to run the first rehearsal.

Frequently Asked Questions

Is AI-enabled cyber threats training suitable for leaders without a technical background?

Yes. AI-enabled cyber threats training is built for non-technical directors and executives. It assumes responsibility for services or decisions, not security or programming experience.

Which standards do AI-enabled cyber threats and resilience in this programme rest on?

AI-enabled cyber threats and resilience work rests on ISO/IEC 27001, ISO 22301, the NIST Cybersecurity Framework and ISO/IEC 42001 for AI systems.

How is the playbook from AI-enabled cyber threats and resilience training used at work?

You use the playbook to brief the executive team, assign decision owners and rehearse the response. It also gives boards a clear basis for questioning management on resilience.