AI-Themed Cyber Incident Response Exercise

Assess your organisation's posture, policies and procedures against the next generation of AI-enabled attacks.

AI is reshaping the cyber security landscape

Attackers are using AI to accelerate reconnaissance, craft more convincing social engineering, and scale intrusion attempts – while defenders are still working out how AI changes detection, response and recovery.

How are we postured against AI-driven threats?

What impact is AI having on our threat landscape?

How do we prepare – what do we need to change?

How would your organization respond to an AI-driven attack?

A facilitated, scenario-based tabletop exercise puts your organisation through a realistic AI-accelerated attack to pressure-test decision-making, escalation paths and recovery arrangements.

- Validate your policies and procedures against plausible AI-enabled attack paths, not hypothetical worst cases.
- Surface gaps in governance, escalation and cross-team coordination before a real incident occurs.
- Ground response planning in real-world case studies.
- Benefit from experienced practitioners who bring current threat intelligence into the room.

Our approach

01 We build realistic AI scenarios

Our scenarios are grounded in real-world incidents and evolving attacker techniques. We draw on live threat intelligence and lessons from actual breaches to make sure the exercise reflects what AI-enabled attacks look like today, not a hypothetical future.

02 We align the scenario to your specific network, technology stack and organisation

No two organisations face the same risk profile, so we tailor the scenario to your environment – your netfork architecture, technology stack, and the threats most relevant to your sector. This ensures the exercise tests decisions your team would actually need to make, not a generic script.

03 We deliver in an engaging, discussion-based format, with advice and support from subject matter experts

The exercise is facilitated as an interactive discussion rather than a lecture, encouraging your team to think through decisions in real time. Experienced subject matter experts are on hand throughout to share practical insight, answer questions, and guide the conversation toward actionable takeaways.

Organisational benefits:

- A clear, evidence-based answer to your Board and executive's questions on AI-related posture and risks.
- A practical view of where AI is changing your threat landscape.
- A prioritised set of actions to close gaps in policy, process and capability.

Why CyberCX?

CyberCX's Cyber Capability, Education and Training (CCET) practice delivers industry-leading education and training. Our experts bring deep knowledge of the Australian and New Zealand threat landscape, giving you clear, practical advice on AI-related cyber risks. Every engagement is shaped around your organisation, sector and region, so what you get is relevant and ready to use. We run sessions that work equally well for executives and operational staff, helping your people anticipate threats, build resilience and stay a step ahead.

About CyberCX

CyberCX unites our country's most trusted experts in delivering an unparallel, comprehensive end-to-end portfolio of cyber security and cloud services across Australia and New Zealand.

Contact us to find out how CyberCX can boost the cyber security skills of your entire organisation.

cybercx.com.au **1300 031 274**

CyberCX
Part of Accenture

Securing our communities