FUJITSU

Crisis simulation

Tabletop exercises to prepare your team to efficiently manage a cyber attack

Organisations that regularly test their crisis response plans are able to recover faster, communicate more effectively, and maintain business continuity when it matters most.

Our tabletop exercises are structured, interactive sessions that simulate real-world cyber incidents. These exercises engage your organisations key stakeholders - IT, security, legal, communications, and executive leadership, in a controlled environment to test and refine your organisation's incident response capabilities.

- Understand threat landscape
- Refine policies and procedures
- Evaluate tools and tech
- Be prepared with confidence
- Improve collaboration
- Streamline your operations

Empower

Empower teams to act decisively under pressure.

Uncover

Uncover gaps in processes, tools, and communication.

Engage

Engage leadership and staff in proactive cyber defence.

Practice

Practice interactions with regulators and refine strategies.

What's involved?

Our facilitators guide your team through realistic simulations, prompting critical thinking and cross-functional collaboration. Each exercise is an opportunity to refine your incident response plans, communication protocols, and decision-making processes.

Preparation and planning

We tailor scenarios to your organisation's threat landscape, aligning with your current incident response plan and business priorities.

Live simulation

A 2-4 hour session involving realistic injects and evolving threats. Participants respond in real-time, revealing strengths and gaps in coordination, decision-making, and technical readiness.

Organisational recovery

Focus on holistic recovery strategies from a significant breach.

Crisis simulation report

Our experts conduct a post-exercise review, providing insights and actionable improvements to enhance response efforts.

FAQs

What's covered?

- Simulated breach scenarios with evolving injects and cross-functional engagement.

Who should attend?

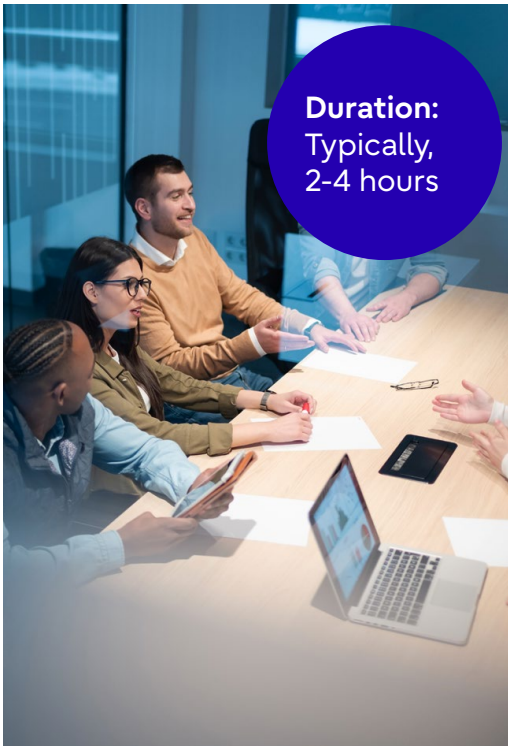
- We recommend including at least one representative from each key area of your response team, such as legal, comms, and IT. Sessions are designed for groups of 5–20 participants.

Do we need to prepare anything in advance?

- We'll provide a short pre-session briefing. No extensive preparation is needed, but it's helpful if participants are familiar with your organisation's incident response plan.

Where are the sessions held?

- Our facilitator/s come to you (Australia or New Zealand). We also offer remote sessions if preferred.



How prepared is your organisation for a cyber crisis?

Get in touch

Fujitsu Cyber

www.fujitsu.com/au/services/security

www.fujitsu.com/nz/services/security