Empower Results®

# Build Cyber Resilience

A cyber security crisis can strike a company at any time – malicious insiders, organised hacking groups and state-sponsored adversaries persistently try to breach computer networks and systems all over the world. It only takes one successful attack to devastate a company's financial performance, brand, and reputation.

An effectively implemented cyber incident response plan is fundamental to an organisation's ability to handle a cyber incident and reduce the risk of resultant reputation and brand damage. It is increasingly important that companies test the plan and response team with training exercises or simulations. Aon provides solutions to assist organisations in building their cyber resilience.

## Cyber Incident Readiness Assessment

Our workshop is designed to evaluate an organisation's response capabilities during a crisis situation. It brings together key stakeholders from all relevant business functions to discuss:

- Cyber incident readiness, planning and testing;
- A high-level review of the company's current incident response plan;
- Integration of cyber incident response plans into business continuity and crisis management plans;
- Organisational and third-party security awareness management; and
- Engagement with response support panels.

Following the workshop, Aon will present an analysis of the organisation's current capabilities and provide recommendations for developing and maintaining an evolved incident response process. You can choose to build or adapt their response plan based on templates we provide, or engage Aon to provide an cyber incident response planning service to develop the plan.

## Cyber Threat Simulation

Testing the incident response plan is key. Aon takes key stakeholders from your organisation through a cyber scenario to observe how the organisation handles the situation. The goal of the simulation is to test for flaws in the response plan and improve response capabilities.

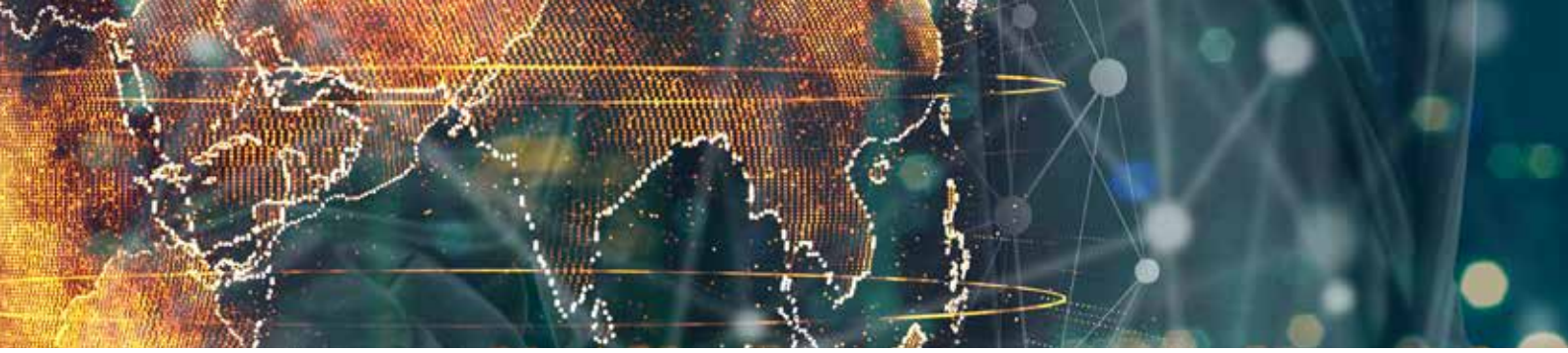
The simulation is run in a workshop format with the stakeholders at a table (or via conferencing facilities as required). The stakeholders will be briefed in advance on the exercise and their roles but they will not be fully aware of the scenario. This service includes:

- Development of a tailored exercise plan outlining objectives, methodology, scope, stakeholders, communications, reporting, performance criteria;
- Development of an exercise scenario, run sheet, supporting tools;
- Initial participant briefings;
- Facilitation of a 2-3 hour cyber scenario exercise; and
- Provision of post exercise report and recommendations.

Following the threat simulation exercise, Aon will debrief those involved in the exercise including senior executive and board members if desired, which will allow for modifications to be made to the plan based on the lessons learned.

***Your actions in the first 24 hours after discovering a data breach are often critical to the success of your response.***

– Office of the Australian Information Commissioner



## Aon Cyber Risk Solutions

Aon's dedicated cyber risk consultants and brokers provide a cyber resilience solutions framework to help identify, quantify, mitigate & manage and transfer the cyber risks that are relevant to your organisation.


If you would like Aon to facilitate one of these cyber services for your organisation, please contact us today.

## Contacts:

**Michael Parrant**

*Cyber Insurance Practice Leader*
**t** +61 2 9211 3485
**e** michael.j.parrant@aon.com

**aon.com.au/cyber**

FSG0068 0918

Empower Results®