Cyber Incident Readiness Assessment & Threat Simulation Solution

Empower Results®

A cybersecurity 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.

Planning your response

In October 2015, the Australian Government released a draft consultation paper, *Guide to developing a data breach response plan*, which included the following key observations:

- "Your actions in the first 24 hours after discovering a data breach are often critical to the success of your response"; and
- "You should create and test your plan before a data breach occurs".

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.

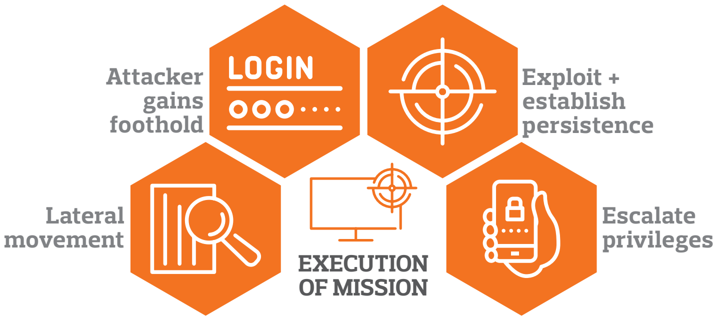
Cyber Incident Readiness Assessment

Aon's Cyber Incident Response Readiness service is designed to evaluate an organisation's response capabilities during a crisis situation. This exercise commences with a workshop involving 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.
- Effectiveness of cyber insurance in assisting with Incident Response activities

Aon will present our analysis of the organisation's current capabilities and will provide recommendations for developing and maintaining an evolved incident response process.

The organisation can then choose to build or adapt their response plan based on templates provided by Aon, or engage Aon to provide an Incident Response Planning Service to develop the plan.



Cyber Threat Simulation – table-top exercise

Once the Cyber Incident Response Plan is complete, it needs to be tested. Aon offers a Cyber Threat Simulation Solution whereby we present a cyber scenario to all the key response stakeholders and 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 and potentially with other supporting functions present via conferencing facilities.

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.

Once the Threat Simulation session is complete, Aon will debrief those involved in the exercise and senior executive and board members if desired, which will allow for modifications to be made to the plan based on the lessons learned.

Other cyber solutions

Aon also offers the following services:

Incident Response Plan & Process Development

Once a Cyber Incident Readiness Assessment is complete, we can work with stakeholders to develop and document a detailed and effective Cyber Incident Response Plan.

Cyber Security Assessments

Aon can facilitate engagements to analyse organisational cyber risks and can include services such as penetration testing and security architecture assessments.

Cyber Risk Profiling

We can provide an incident scenario definition workshop, quantification of financial risk and insurance gap analysis.

Aon's capabilities

With the largest team of dedicated cyber risk consultants and brokers exclusively engaged in delivering a range of cyber assessment, mitigation, transfer, and response solutions for our clients, Aon is uniquely positioned to assist organisations to improve their overall cyber risk profile and readiness.

These capabilities include:

- More than **610** dedicated cyber professionals across Asia-Pacific, the US, Canada, London, EMEA, Bermuda;
- Over **150** cyber analytics projects;
- Over **500** cyber claims handled by Aon since 2012; and
- **13** of **15** the largest global cyber breaches managed by Aon since June 2016.

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

aon.com.au/cyber

Contacts:

Fergus Brooks

Cyber Risk Practice Leader
T +61 2 9253 7835
E fergus.brooks@aon.com

Michael Parrant

Cyber Insurance Practice Leader
T +61 3 9211 3485
E michael.j.parrant@aon.com

Empower Results®