Cyber risk:
the reality of the risk

It is a daily occurrence that media headlines focus on topical data breaches or cyber security. The impact of a cyber event can be extremely significant – practically, legally, reputationally, and financially.

System shutdowns, cyber extortion attempts and the urgent need to restore systems and internal/ client data are all examples of consequences that can have a profound effect on the brand of an organisation, and its ability to retain customers and revenue.

Cyber criminals are working on new techniques to penetrate the security of organisations to misappropriate funds, cause damage, access sensitive data, and steal intellectual property. The deployment of malware and malicious software has rocketed by 400% since 2012. Organisations that operate critical infrastructure and industrial control systems are being targeted, resulting in destruction to systems and operations technology, property damage and considerable business disruption.

Cyber risks may affect directors' duties and disclosure requirements

ASIC has recently released a Cyber Resilience Health Check Paper signalling that it is taking a more active interest in cyber risk management. The reports highlights that Board and senior management are accountable for taking a robust approach to cyber resilience.

- ASIC regulated entities will be required to review and update cyber risk management practices.
- ASIC suggests an organisation consider the purchase of cyber insurance as an appropriate business decision based on a company's risk profile.
- If you are a Corporation or ASX listed, a cyber event may affect your disclosure requirements including information contained in a prospectus, annual directors' reports and continuous disclosure obligations.

Legislative changes means increased responsibilities

- Mandatory breach notification laws passed both houses of federal parliament in February 2017 with a minimum effective date of 22 February 2018
- Greater accountability in the collection and management of personal information
- Increased power of the Privacy Commissioner to conduct audits and issue enforceable undertakings, backed by a penalty regime (maximum of $340,000 for individuals and $1.7 million for organisations).

Are you sure you're already covered for cyber risks?

While conventional insurance products may provide elements of cyber cover, gaps exist. Conventional insurances were not designed to the meet the evolving nature of certain cyber exposures. Where policies are ambiguous, it is likely a cyber claim will be resisted by insurers.

The average time between initial data breach to detection is 210 days. Most victim organisations (64%) take over 90 days to detect intrusions, and 5% take 3 or more years to identify the criminal activity.

For more information, contact:

Fergus Brooks
National Practice Leader,
Cyber Risk
t: +61 2 9253 7835
fergus.brooks@aon.com

Solution: Aon cyber risk transfer strategy

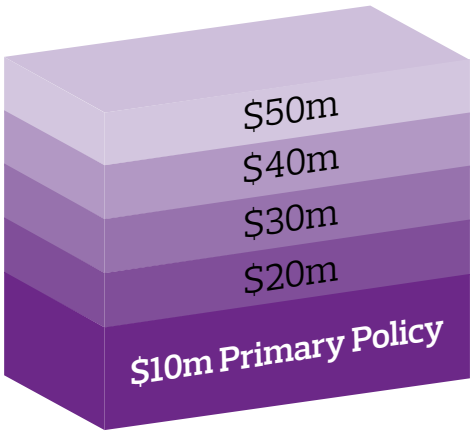
Cyber insurance provides comprehensive cover for first and third party exposures in relation to any cyber or privacy event that impacts your business. It provides your business with a structured crisis response plan to mitigate further loss and assists with returning to 'business as usual'.

What is covered?

First party	Third party
• Business interruption (loss of income and extra expenses) • Costs to restore/recreate data • Notification costs & credit monitoring services including identity theft management • Forensic and accounting investigation expenses • Cyber extortion costs • Crisis communication/ public relations costs • Legal costs assisting with privacy notification/ compliance response	• Defamation claims • Infringement of privacy and intellectual property claims • Claims arising from network security failures • Claims as a result dissemination of confidential information or damage to third-party systems • Legal defence costs • Privacy breach regulatory proceedings and investigations • Fines & penalties

Starting your cyber risk transfer strategy

Based upon our benchmarking data, our knowledge of your organisation and your industry sector, we are able to help you build a cyber risk transfer solution.



Take the test

Review your cyber risk exposures with our Cyber Diagnostic Tool:

aoncyberdiagnostic.com

Risk. Reinsurance. Human Resources.

Empower Results®

FSG0011I 0517