# 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.

## 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).

## For more information, contact:

NFP Team
1800 123 266
au.nfp@aon.com

## Decoding the technical terms:

**Malware:** short for malicious software and refers to any software used to disrupt computer or mobile operations

**Ransomware:** is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid.

**Worm:** a self-replicating malware computer program designed to spread to other computers

**Exploit:** a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware

**Digital currency:** an internet-based form of currency which enables instant, borderless and anonymous transactions

AON
Empower Results®

## **Solution:** Aon Cyber insurance

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?

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

## 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.

ourcommunity.com.au
Where not-for-profits go for help

PREFERRED SUPPLIER TO AUSTRALIAN NOT-FOR-PROFITS
ourcommunity.com.au

AON
Empower Results®

AFF0750AR 0218