Transferring cyber risk

Local Government

Cyber risk has become a leading issue for many councils in a technology-dependent world, as most have a reliance on computing systems and networks critical to operations. New exposures have emerged in the management of personal data and the consequences of losing corporate information. Experience shows that no system is impenetrable, and even top-notch, state-of-the-art cyber security is vulnerable. In an increasingly punitive legal and regulatory environment, and in the face of more frequent contractual insurance requirements specifying cyber liability, forward-thinking councils are taking proactive steps to explore and transfer cyber risk.

When should councils be concerned about their risk exposure?

Councils should be concerned about cyber risk if they:

- Gather, maintain, disseminate or store private information
- Have a high degree of dependency on electronic processes or computer networks
- Engage vendors, independent contractors or additional service providers
- Are required to comply with PCI Security Standards/Plastic Card Security statutes
- Operate a website and subsequently face publishing exposures
- Are conscious of protecting their reputation and avoiding a loss in community and consumer confidence.

What risks are unique to local government?

- Increasing dependence on electronic information assets to conduct business activities
- Frequent need for unlimited access to citizens' personally identifiable information for various government purposes
- Significant obligation to clients to maintain confidentiality for ethical as well as regulatory obligations
- Primary target due to 'hactivists' trying to access government related data bases
- Increased vulnerability to breaches caused by negligent or malicious employees, as well as disgruntled citizens
- Obligations to preserve evidence in case of litigation, increases the level of exposures in the event of network outages and breaches.

Why are standard insurance policies not enough?

While existing forms sometimes carry a level of coverage, they were not intended to cover many risks associated with an increasingly digital world. Typical forms respond as follows:

- General Liability: covers bodily injury and property damage, not economic loss
- Professional Indemnity: covers economic damages resulting from a failure of defined services only, and may contain exclusions for data and privacy breaches
- Property Insurance: covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are viruses and hackers
- Crime: covers employees and generally only money, securities and tangible property. No coverage for third party property such as customer/client data

What is the scope of today's cyber coverage?

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

How can councils transfer cyber risk?

- Some exposures can be transferred contractually if outsourcing services. Insurance solutions exist if the vendor will not take responsibility
- The marketplace is evolving to provide services solutions, including loss control resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response
- Many insurers provide cyber coverage on a primary basis (breach response coverage offering varies based on insurer and policy structure)
- Numerous additional insurers are available for consideration of excess limits.

Further information

Paul Crapper
National Head of Local Government
03 9211 3313
paul.crapper@aon.com

Brett Parnell
Client Executive - Cyber
03 9211 3488
brett.parnell@aon.com

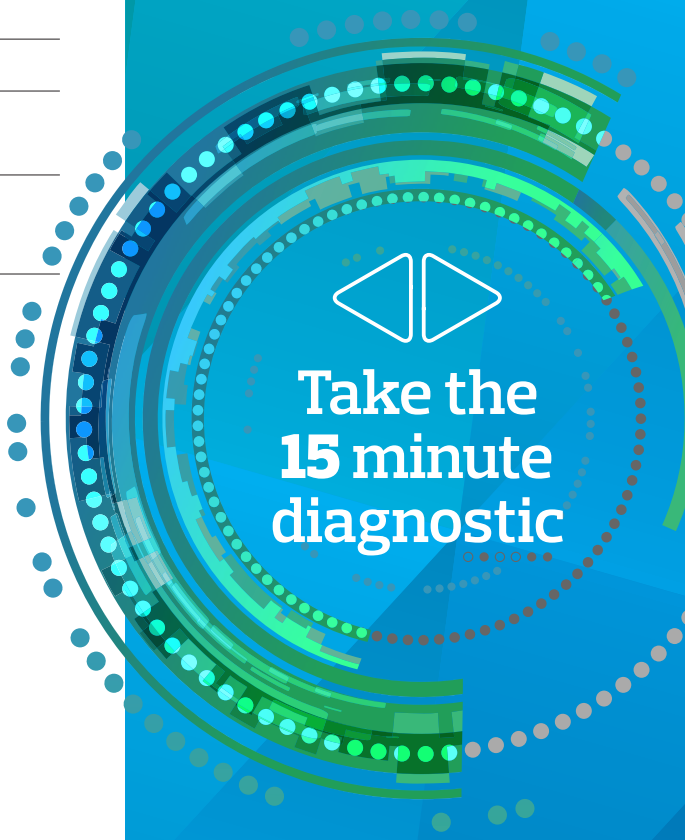
aon.com.au

Risk. Reinsurance. Human Resources.

COM0265A 1115

STARTING YOUR CYBER RISK TRANSFER STRATEGY

Aon's Cyber Risk Diagnostic Tool will help you identify the key internal and external factors that may affect your level of exposure to cyber risks. It will also give you real insight into the relevant cyber risk drivers, and provide you with practical guidance on a governance framework that you can put in place as part of an effective cyber risk management strategy.



aoncyberdiagnostic.com

Aon
Empower Results®