FACT SHEET

Cyber Security

August 2018

The fast moving nature of cyber security risk is a constant threat to local government. The types of risks that could be relevant to your council include:

- Negligent or malicious acts of employees
- Targeted attacks, theft and destruction of data by criminal hackers
- Accidental damage and distribution of data
- System malfunction
- Loss of data stored by Third Party providers
- System infection through malicious email campaigns
- Cyber extortion or ransomware
- Denial of service attacks
- Stolen and lost devices

In accordance with the Australian Government's release of Australia's Cyber Security Strategy in May 2016, Local Government entities are able to access resources, seek advice and report incidents to the Australian Cyber Security Centre (ACSC). The organisation responsible to provide this on behalf of the ACSC is the Australian Signals Directorate (ASD).

ASD provides free resources on how to protect your network. This includes an Information Security Manual providing governance requirements for the security of government ICT Systems. ASD also maintains an Evaluated Products List (EPL) of ICT security products evaluated for use in Australian and New Zealand government agencies.

All cyber incidents should be reported to ASD to both assist the response and enable ASD to continue building an intelligence picture of the ever changing threat environment. NSW LG entities as agencies that hold tax file numbers (TFNs) have additional obligations under the Notifiable Data Breaches (NDB) scheme to notify if a TFN data breach is 'likely to result in serious harm' to any individual.

RESOURCES

The following is a list of links to useful resources available from ACSC and ASD that will assist councils fulfil their responsibilities to protect its ICT Network:

- Australia's Cyber Security Strategy
- To understand the threat faced by Council: ACSC 2017 Threat Report: ACSC 2017 Threat Report
- To create governance on the security of your Council ICT Network: ACSC Information Security Manual
- To access evaluated products to protect your Council ICT Network: ASD Evaluated Products List
- To implement strategies to mitigate cyber security attacks on your Council ICT Network: ASD Strategies to Mitigate Cyber Security Incidents
- To find an ASD accredited person to evaluate your Council network: IRAP Assessors
- To report a cyber security incident: Cyber Security Incident Report Form

- To notify a TFN data breach: IPC NSW Public Sector Agencies and Notifiable Data Breaches

Viewing a printed version of this Fact Sheet?
You can find the above links at statewidemutual.com.au/factsheetlinks

HOW CAN STATEWIDE MUTUAL HELP?

Statistically there is a high likelihood of Council suffering a breach or an incident. As such, Statewide Mutual's cyber cover addresses this and provides post-breach assistance through Zurich's DigitalResolve solution. This solution provides Members with access to a dedicated and experienced breach response team to manage any cyber incident from initial notification through to resolution. The solution includes:

- The first notification of a loss is phoned in to a dedicated phone number available 24 hours a day, 365 days a year (Call: 1800 ZCYBER).
- All notifications are assigned an Incident Manager who will provide support from start to finish.

HOW DOES DIGITALRESOLVE WORK?

- ✓ Contact Zurich DigitalResolve whenever an incident occurs, 24/7, 365 days a year.
- ✓ Dedicated Incident Manager appointed immediately.
- ✓ IT forensic experts appointed (if required) to locate and act to resolve the event and report to the Incident Manager.
- ✓ Incident Manager consults with you and appoints other experts as required, such as lawyers and PR consultants.
- ✓ Regular discussions between your business and all parties to agree best approach to resolve the incident.
- ✓ Other experts appointed where necessary, for example notification and credit monitoring specialists.
- ✓ Comprehensive summary document issued at service conclusion.

FOR FURTHER ASSISTANCE

Contact your Regional Risk Manager or Account Manager for additional information and help upon request.

To confirm if your Council has access to Zurich's DigitalResolve solution speak with your Account Manager.