RISK INSIGHT

Cyber ready: Protecting local council reputation

Preparing for mandatory data breach notification legislation

Australia's local councils rightly put a premium on their reputation, but a lack of awareness of cyber security risk places councils in extreme jeopardy of compromising their good standing through a cyber-attack, especially after mandatory breach reporting comes into effect.

Local councils hold a wealth of their community's data including credit card information, health related data, ratepayer information and business and development proposals, and are prime targets for cyber-attacks.

The global and local landscape

In the UK, the BBC reported that the City of Edinburgh Council had more than 13,000 email addresses stolen from its database in 2015. The breach happened when the council's website service provider was targeted by hackers.

The council reported the incident to the UK Information Commissioner and the UK Government's Computer Emergency Response Team and had to warn those affected by the breach of the potential for increased spam and phishing attempts.

Also in the UK, Lincolnshire County Council was held to ransom by a cyber-attack, the BBC reported in January 2016.

An email was opened that triggered a zero-day (previously unknown by cyber security providers) malware attack and the council was asked to pay a ransom and had to close down its systems as a precautionary measure. Staff were forced to resort to pen and paper while the council's 458 servers and 70 terabytes of data were scanned.

In Australia there have been a number of well publicised attacks on government agencies including the NSW Department of Resources and Energy which warded off an attack on its Maitland office in December 2015 and the Bureau of Meteorology suffered a major and very expensive cyber strike in early 2015 that could have compromised other Federal Government systems.

It is understood that there have been several significant cyber-attacks on councils here in Australia which have not been publicly disclosed, where councils have had to respond quickly to the risk in order to maintain their operations and minimise the risk of sensitive community information being released into the public domain.

Reputational risk and more

In the wake of these attacks and others the Federal Government launched its $230 million Cyber Security Strategy report in March 2016.

Meanwhile, the Australian Cyber Security Centre (ACSC) didn't mince words on digital security dangers in its latest threat report. The ACSC, whose partner agencies include the Australian Crime Commission, the Australian Federal Police, ASIO, the Australian Signals Directorate and CERT Australia, said the cyber threat to this country is "undeniable, unrelenting and continues to grow".

The report said Australia 'must be vigilant and proactive in its approach to cyber security.'

'Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this.'

While the country's local councils value their financial sustainability and stability dearly, cyber risk, which could seriously undermine that stability, is an underrated threat.

According to Aon's latest Australian Local Government Risk Report the top 10 risk concerns for local government listed financial sustainability and stability as the number one concern, and threats to infrastructure as number two.

While cyber risk did not feature as an area of concern in the list, it can clearly be linked to financial sustainability and stability, infrastructure and reputation - all risks that did make the top 10 in Aon's report. Nationally, just 54 percent of councils have a cyber risk policy, according to Aon's report, although NSW councils lead substantially on awareness in this crucial area, with 86 percent of councils surveyed having a cyber policy.

The lack of a cyber risk policy leaves councils vulnerable to an increasingly punitive regulatory environment, particularly legislation under the Privacy Act.

In the future, the risk to reputation is expected to rise, especially with the introduction of Federal government mandatory data breach legislation, which is likely in late 2016. The expected legislation will require that organisations immediately disclose to a customer or constituent when their personal information has been breached. Given this is not already law in Australia; it is difficult to get a full understanding of the reputational damage that follows an organisation when it advises its customer that their personal information is in the hands of a hacker.

Understanding Council's cyber risk profile

Paul Crapper, Aon Australia's National Head of Local Government says cyber risk is dawning as an area of concern with several Australian councils recently enquiring about getting help with cyber risk in discussions about insurance.

'Some councils already understand cyber risk and the potential effect on their community, reputation and operations if a breach occurs, some are interested and want to have a look at it, while others think it's irrelevant which is fascinating given the level and complexity of information they hold.'

Mr Crapper believes councils need to become more commercial in their thinking both in tendering competitively for their insurance and risk assessment needs and in responding to ever increasing cyber dangers.

'Part of being more commercial in the changing business landscape that local government is exposed to is being more cognisant of things like cyber,' he says.

Mr Crapper believes the imminent mandatory data breach notification legislation makes it imperative for councils to examine their cyber risk profile.

'If you are running a business and your business is council and you have never thought about having robust cyber coverage in the past, then you are about to get a very rude awakening because if you breach privacy under the new legislation you will have a major problem.'

Mr Crapper says councils need to fully reflect on the level of sensitive, private community data they hold and the reputational consequences of a breach.

'The ratepayer information and the credit card details used for paying things like pet fees and rates is only part of it. Then there's all the immunisation records of children and the health and address records associated with aged care and disability services. There's council fine and infringement information also – do people want that getting out there?'

Councils may believe they are covered for cyber risk under their professional indemnity policies but that may only cover damage done after the fact, not the cost of responding to the breach such as communicating the breach to those affected, legal fees as a result of potential legal action and fines associated with breaching privacy laws.

AON
Empower Results®

Cyber ready with Aon

Aon is developing new digital security services for the Australian market including risk assessment experts that can come in and carry out a cyber health check, the results of which can direct the form of policy coverage. Cyber health checks were referenced in the Federal government's new cyber security package. Aon also offers a free cyber risk diagnostic desktop tool that is available to councils to assess their potential level of exposure.

'These will help councils anticipate cyber risk and mitigate cyber risk,' says Mr Crapper.

Aon is also developing policies that cover what Fergus Brooks, Aon National Practice Leader, Cyber Risk calls the 'post breach world.'

'When an insured feels they may have had a cyber-incident, the response team will fly in and start fixing the problem', says Mr Brooks.

This would see the insurer's cyber coverage panels include crisis management companies, forensics companies, public relations firms and law firms with 'breach coaches' that can lead a council through the legal minefield surrounding a breach.

'The whole world is about to change,' says Mr Brooks of the Australian cyber policy market.

Find out more

For more information, contact Paul Crapper, National Head of Local Government, on 03 9211 3313 or paul.crapper@aon.com.

connect-aon.com.au