LOCAL GOVERNMENT

Sector Overview

More than ever, local government entities are prime targets for cyber-attacks as they deliver essential services far beyond the outdated 'three R's' concept of local councils ('rates, roads, and rubbish'). Significant variation in council delivery infrastructure in Australia now exists beyond the three R's to include property services, water and sewage services, health services, and facilities supply and management.

Like the rest of Australia's economy and society, local governments are undergoing a digital transformation of their organisations and operations. The transformation accelerated in response to a shift to virtual service delivery as a result of the Covid-19 pandemic and resulted in a new wave of cyber threats that must be understood.

Local governments are attractive cyber targets for trusted insiders, cyber criminals, and nation-state actors because they collect and store significant volumes of sensitive personal, commercial, and operational information about their ratepayers, local businesses, local government employees, and interactions with State and Federal governments. They are often also custodians of other types of valuable data (Geographic mapping, local regulatory data etc.).

The potential impacts of a cyber-attack on a local government include but are not limited to:

- financial, reputational, and legal damage
- disruption of critical services/operations
- data loss

Australia has 537 local governments/councils, according to the Australian Local Government Association (ALGA), with regional, rural, or remote councils representing roughly 55% of ALGA members. The Brisbane City Council is the largest, serving 1.25 million residents.

Local governments are significant employers, with approximately 200,000 people directly employed or roughly 10% of Australia's entire public sector workforce. These figures demonstrate that cyber-attacks against this sector may potentially have large direct impacts and significant spill-over effects.

If cyber-attack trends in other economically advanced democratic nations are a reliable indicator of what can be expected in Australia in future, the trends are concerning. There has been a significant increase in cyber-attacks in the United States against US State and Local governments. In 2021 at least 2,323 local governments, government-run schools, and healthcare providers suffered ransomware attacks. As a result of this spike in attacks, the US Federal Government passed the State and *Local Government Cyber Security Act* (S. 2520) to establish a formal framework for the ongoing partnership between CISA and the Multi-State Information Sharing and Analysis Centre (MS-ISAC) to enable SLTT governments (state, local, tribal, and territorial) to improve cyber threat intelligence sharing.

Closer to home, the increasing local government attacks include but are not limited to:

- In August 2021, a Victorian local council suffered a cyber-attack that forced it to disable many online services, including online payments, its 'ePlanning' system, and its call centre for over two weeks and had to operate under 'manual processes' during this time.
- In December 2021, a city council in South Australia was hit by a ransomware attack that resulted in the encryption of its servers, which consequently caused substantial service disruption.
- In April 2022, a NSW council suffered a ransomware attack on water infrastructure remote monitoring systems that it managed, which forced the council to use manual processes to manage its infrastructure. A wide range of business operations was also impacted, including council minutes, employee financial data, and systems responsible for monitoring water quality and levels. During the initial response, the incident forced council technology staff to work 40–80 hours of overtime a week.

Key Cyber Challenges and Issues:

- Ransomware and other cyber extortion threats, which have risen dramatically in 2021, pose a severe threat to local governments
- The government is Australia's third most frequently impacted sector by cyber extortion.
- Accidental exposure by employees or contractors is the most frequent cause of data breaches in the public sector. Additionally, local governments are being actively targeted by foreign governments to gather intelligence and interfere in local politics. Some of these actors assess local governments as "weak links" in Australia's national security.
- The most likely type of cyber-attack local governments may experience is business email compromise (BEC) which has the potential to result in significant financial damage.
- Phishing is the most common method threat actors use to obtain initial network access
- Local governments urgently need to implement programs for employee training and awareness of cyber security threats.

Most local government entities won't have the capability to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their local government assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

Published: 1st February 2023