Report on the meeting with the Shire of Cranbrook's IT Provider, Ramped Technology (Garry Hamersley) in Albany Wednesday 6th April 2022 attended by Linda Gray, Chief Executive Officer and Diana Marsh, Manager of Finance and Administration.

The meeting with Ramped Technology in Albany gave us a better understanding of the role they play with the Shire of Cranbrook on two fronts; firstly, in terms of keeping the Shire running smoothly IT wise, and ensuring upgrades are made so that core functions can be met. Secondly, Ramped Technology is obviously a crucial partner in our business continuity and disaster recovery plans.

The war in Ukraine is a war on two fronts; on the battle ground and through cyber crime. Last year the malware that went into Ukraine spread around the world and eventually ended up in Australia. There were 14,000 cyber security incidents reported to the Australian Cyber Security Centre last year, and of that number local government was in the top five for ransomware. Losses are estimated to be $85 million in Australia with an increase in the last year of 54%.

One of the important areas that have not been defined by local government policies or procedures is who is responsible for what regarding cyber security. Whilst the IT provider would normally do system backups and monitoring, it is the new responsibility of the local government to capture these controls and measures in documents now required by the Office of the Auditor General's audit. These are the result of the unsatisfactory results of their auditing of fifteen local governments in 2021.

The documents and processes required to be in place are:

- Cyber security policies
- Processes to identify, understand and address relevant cyber security risk (*and includes an understanding of the level of risk appetite by the shire)*
- Controls
- Education (*If staff are not aware of current risks such as malware and ransomware then the importance of not clicking on links is lost)*
- Technical controls to detect and prevent phishing emails
- Processes to identify and address vulnerabilities affecting their internal and external IT infrastructure
- Cyber security incident response plan
- Updated business continuity plan
- Disaster recovery plan
- Technical controls to detect, alert and prevent cyber intrusions

We also need to provide awareness raising programs to continually educate staff and elected officers on cyber security risks. The required documents and improved processes would focus on the prevention of intrusions and will be communicated to Council through the Audit and Risk Committee. A quick response to any incident through staff's familiarisation of the Shire's incident response plan is important as often criminals take time to go through the stages of an attack. They use different groups for each stage and sell the next stage in a marketplace on the Dark Web. The Local Government Professionals Leadership Summit was very informative on how organised cyber criminals are within their "industry".

Ramped Technology provided us with the required information at the meeting which allowed us to assess the risks and they followed up with quotations on some of the improvements we could implement. Unfortunately, an increase in funding is in line with the increased threat. We will continue to research the level of protection provided now and the potential impact on our 2022/2023 Budget.

Linda Gray
Chief Executive Officer
SHIRE OF CRANBROOK

Shire of Cranbrook
Great Southern's Finest