Risks of Cryptocurrency for Local Government

Neil Hartley
3 May 2018

What do cryptocurrency miners and driverless mining trucks have in common?

The answer is they both use powerful computers to earn money for someone else. What is not so funny about this new form of global block-chain currency is that someone else could use your facilities to do their own mining, to their personal benefit and at your local government's expense!

By way of a 'real and current example', Federal police officers recently executed a search warrant at the Bureau of Meteorology Collins Street headquarters in Melbourne, where two employees were being investigated for allegedly running an elaborate operation involving the use of the bureau's powerful computers to 'mine' cryptocurrencies.

Who are the cryptocurrency miners?

Cryptocurrency mining used to be undertaken by very clever coders who solved complex algorithms for cryptocurrency rewards. Now, it is mined by average computer literate people who simply buy the necessary software off the Web. They, of course, ideally need powerful computers and a good supply of electricity to undertake that task. They now often form cooperative groups to compete against similar groups for those rewards.

What are the risks for local governments?

So far with this relatively new 'currency', we see two obvious risks for local government. First, a hacker breaks into your computer system and uses your hardware to mine cryptocurrency for themselves; second, someone breaks into your electricity supply to feed their own computers to mine cryptocurrency. Your IT staff are the best people to manage the first situation; your building maintenance staff or rangers are the best people to manage the risk in the second situation. One example of this is where a hacker redirects a power supply to a remote location, which is rarely checked.

What can your local government do about these risks?

This issue of cryptocurrency is a real and current risk, so it would be best to take some prompt action at your local government to satisfy yourself that everything reasonably possible is being done to protect yourself and your local government.

Some tips on what to do:

- Your IT team could undertake a test to ensure that no unauthorised access has been gained, nor unauthorised programmes have been operated. They could conduct a review of remote access arrangements to ensure no breaches have occurred;

- Your Finance Team could review power usage for every individual account, to ascertain if there had been any unusual increases in power consumption from those locations.

You might also list the matter on a future Audit & Risk agenda for further discussion as there will no doubt be unique situations that relate to your individual local government beyond the above two more obvious examples.

It does appear that there are large sums of money at stake here, so do not underestimate the ingenuity of those few in our community that wish to take advantage of this 'easy source of crypto-cash.

Key Recommendations

- Your IT team can monitor access and programmes
- Your Finance team can look for spikes in power usage
- You can put this topic on the Audit & Risk agenda for discussion

Contact

For more information please contact:

Neil Hartley
Governance Consultant
T +61 8 9200 4900
E nhartley@civiclegal.com.au