15th July 2021

Open letter in response to Strengthening Australia's cyber security regulations and incentives.

The cybersecurity industry's response to the ongoing and increasing threats posed by ransomware criminals is a challenge that cannot be dealt with using conventional thinking. Those who are most skilled at thwarting and responding to these threats are also those who profit from it. It's my opinion that this responsive model must change.

It is my view that we need to do three things to solve the ransomware problem:

1. Criminalise the payments of ransoms resulting from ransomware attacks.
2. Provide legal flexibility for organisations impacted by ransomware attacks.
3. Require a minimum level of cybersecurity readiness by organisations requiring legal flexibility.

The only way to break the business model of ransomware criminals is to ensure no payment can be made. Those organisations who pay the ransom are validating the criminal's business model. If an organisation cannot pay a ransom, the criminals have no means of income - no working model.

Organisations falling victim to ransomware attacks (regardless of their ability to pay the ransomware) may incur legal penalties, and therefore require an avenue to legal exemption or alternative renegotiations in good faith.

Organisations who reach a level of cybersecurity readiness would a) be prepared for a cyber threat, and b) be more likely to qualify for appropriate cyber insurance including for losses relating to ransomware attacks.

With these three components, I believe the threat of ransomware and other attacks are reduced, the criminals will need to alter their business model or be out of business, and organisations will improve as a result.

An open discussion regarding these points will prompt change in the attitudes of organisations towards cybersecurity readiness.

Andrew Galdes

AGIX

andrew.galdes@agix.com.au | *https://agix.com.au*