12 OCTOBER 2021

Cyber insurance driving ransomware threat, says CSCRC

While cyber insurance can play a positive role in uplifting cyber security, the payment of ransoms by insurers should be banned, according to a new Cyber Security Cooperative Research Centre (CSCRC) policy paper.

Underwritten or oversold? How cyber insurance can hinder (or help) cyber security in Australia, argues the practice of insurers including ransom payments as part of cyber insurance policies is unintentionally feeding the ransomware epidemic and potentially leading to organisations becoming lax about cyber security.

CSCRC CEO Rachael Falk (co-author), said cyber insurance was not a cyber security silver bullet and should be viewed as part of an organisation's holistic cyber security strategy.

"This policy paper explores a number of issues related to cyber insurance, with a focus on how it can hinder and help cyber security uplift across the Australian economy," Ms Falk said.

"We believe the payment of ransoms by insurers is helping drive the illicit ransomware trade – what is vital when it comes to ransomware and cyber insurance is that we start to starve out the cyber criminals and break the payment chain by stopping insurers paying the ransom."

Other concerns raised in the paper include the lack of clarity regarding inclusions and exclusions in Australian cyber insurance policies, which could leave insured businesses ineligible to claim, and the sweeping 'step-in' powers insurers wield in the event of a cyber event, which in effect could make them shadow directors.

Despite the pitfalls, however, Ms Falk said cyber insurance could play a positive role in uplifting cyber security.

"There are really practical steps insurers can take to drive cyber security uplift in Australia as part of their cyber insurance offerings," Ms Falk said. "They are in a position to set minimum cyber security standards for coverage. They can work with other organisations like telecommunications providers to offer 'bundled' cyber security products as part of policies. And they could help drive regulatory compliance by refusing to cover costs associated with an unreported breach."

The policy paper makes four key recommendations related to: the payment of ransom or extortion payments by insurers; clarity regarding the management of cyber insurance underwriting risk and clear articulation of what is and is not covered by cyber insurance; the development of a Cyber Security Checklist for SMEs by insurers; and opportunities for insurers to partner with other service providers to offer 'bundled packages' for cyber security uplift.

For more information contact:
Anne-Louise Brown, Director of Corporate Affairs and Policy
P: 0468 934 453
E: anne.louise@cybersecuritycrc.org.au