A concerted cyber security attack has impacted ICT businesses and their customers worldwide, including in Australia, a situation described as being a "catalytic event" for local companies.

In a video news release posted on YouTube on Friday (21 December), Alastair MacGibbon — who heads up the Australian Cyber Security Centre (ACSC) — said that this event should be a major wake-up call as to the risks associated with the theft of commercial assets.

"The threat is real," Mr MacGibbon said.

"This needs to be seen as a catalytic event to drive change in our cyber security posture, to protect not just against this particular threat actor and the activity we have exposed, but against a whole range of threat actors and activities as yet unknown.

"This is a great reminder to the companies that use managed service providers as their outsourced IT providers that there are things they must do to ensure the security of their own operations and their customers."

Mr MacGibbon said that this applies not just to anyone directly impacted by this breach, but for all companies to minimise the risk of a serious breach in the future.

"This should be a point of inflection in the Australian economy to lift as many systems as we can… to look much more holistically at seeing the responsibility we all have, as businesses or as governments, to protect the systems that we use," he said.

"There's an old saying that you can outsource services but you can't outsource risk, so if I was a company or an organisation buying in a service provided by an MSP (a managed service provider), I can outsource that to them, but I don't outsource my risk.

"If we've learnt nothing over the past couple of years, it's that your own organisation in and of itself can't be secure, unless those that provide services to you and interact with you are also secure."

According to Mr MacGibbon, a very integrated approach between the private and public sectors to boosting cyber protections and addressing risks "can dramatically improve the security of Australian connected systems", which he said is "good for our economy and it's good for our society".

What actually happened?

Cyber.gov.au said that a "concerted campaign to steal commercial secrets from the customers of MSPs" had comprised IT service providers around the world, including in Australia.

It did not state which, or how many, companies have been impacted.

"A number of MSPs that provide services in Australia are known to have been compromised. It is possible that other MSPs have also been affected. The compromise is significant and ongoing, and at this stage, it is difficult to assess the full extent of damage to Australian organisations," it said.

“We have no evidence to suggest that individuals or the general public have been specifically targeted. However, the campaign has targeted commercial secrets, which will affect Australia’s competitiveness.”

Why is this incident so noteworthy?

The significance of this particular cyber attack is that it specifically targeted managed service providers, rather than companies or government departments directly. That meant that a much larger number of organisations have potentially been exposed.

“Managed service providers… essentially [run] the computer systems for some of the best-known companies in Australia and, frankly, a lot of government services too,” Mr MacGibbon said.

That makes them a critical part of the country’s “security apparatus”.

“The message today is while we can help individual organisations, collectively it is our responsibility to take action,” he said.

“We’ve got a huge amount of information on cyber.gov.au for managed service providers, for customers of managed service providers, for small businesses that are very unlikely to be affected by this event but it is an opportunity for them to take action, and obviously programs for boards on what questions they should be asking right through to information packs to try to explain the type of event we’re talking about today.”

What should customers of these service providers do?

All customers that rely on outsourced IT providers should contact those providers for an update on whether they have been breached or are still investigated whether they have been targeted, and if so, what impact it has had, according to cyber.gov.au.

“To start the conversation, consider asking the following questions,” the site said.

“1. Have you run the published indicators of compromise and tools against your network and ICT systems?

“2. Has my IT system been compromised? If so:

- What specific data and systems are known to be affected?
- What was the indication that there was an incident?
- Date and time of the incident?
- Is the incident ongoing?
- What actions is your MSP taking to investigate and remediate?
- Has this incident been reported anywhere?”

It added that any business that becomes aware itself of a breach of customer or employee data should immediately contact their service provider. Businesses should also be aware that they may also need to take action under the Notifiable Data Breaches Scheme.

The ACSC has set up a dedicated web page on the MSP global hack with more information for businesses that may have been impacted.