Iranian criminals suspected in Navy shipbuilder cyber attack and extortion attempt

By Exclusive by political reporter Jane Norman

Published: 2018-11-12 · Archived: 2026-04-05 17:02:13 UTC

Iranian hackers are believed to be responsible for a cyber security breach and extortion attempt on Australia's biggest defence exporter.

Key points:

- Ship designs were accessed in the cyber attack on Austal
- Not known whether the hackers worked for the Iranian Government or not
- An Iranian-based hack attack on Australian universities took place this year

Perth-based shipbuilder Austal earlier this month revealed an "unknown offender" had hacked into its computer systems, accessing staff email addresses and phone numbers as well as ship drawings and designs.

Some of the information was then offered for sale on the dark web in an apparent extortion attempt.

The ABC can reveal the Australian Cyber Security Centre (ACSC) has determined the attack was most likely carried out by Iranian hackers.

The head of the ACSC, Alastair MacGibbon, would not confirm the nationality but said the hackers failed to steal sensitive information.

"We don't like anyone breaking into any type of business, particularly defence contractors, but I can say that nothing of national security significance was taken," he said.

Mr MacGibbon likened the attack to a "ram-raid", suggesting the hackers stole as much information as they could until they were detected and shut out.

"The fact that this material was put on the dark web to sell to the highest bidder would have to suggest it's a criminal matter," he said.

It is unclear whether the group was linked to the Iranian Government, but the breach was detected in mid-October, around the time Prime Minister Scott Morrison announced Australia would review its support for the Iran nuclear deal.

However, Mr MacGibbon played down any link, saying it did not appear the breach was in response to any Government announcement.

A spokesperson for the Iranian Embassy in Canberra strongly denied his country was responsible, adding Iran "had high respect for Australia".

According to the US intelligence community, Iran is a leading cyberspace adversary, along with China, Russia and North Korea.

"Russia, Iran, and North Korea are testing more aggressive cyberattacks that pose growing threats to the United States and US partners," a 2018 threat report presented to Congress in the US says.

The head of the Australian Strategic Policy Institute's International Cyber Policy Centre, Fergus Hanson, said while China offered the greatest cyber threat to Australia, Iran was opportunistic and known for its retaliatory attacks.

"Iran is less frequently mentioned in the Australian media but it certainly has a sophisticated capability and in international terms it's one of the major threat actors in this space," he said.

Growing threat from Iranian cyberattacks

Earlier this year, dozens of Australian universities were targeted by an Iran-based "spear-phishing campaign" as part of an attempt to steal intellectual property and academic research.

But that is the only publicly acknowledged Iranian cyberattack on an Australian institution.

Mr Hanson said if an Iranian group was responsible for the Austal breach, it was likely to be used by the country's defence industry.

> "Several of Iran's rivals have bought ships from Austal … so there would be an incentive for Iran to have a better understanding of those ships' capabilities,"

he said.

"And if Iran's looking to build ships, stealing those designs would also be handy."

Austal has built ships for the Australian Navy for more than a decade, but with shipyards in the US and the Philippines, it has become a major global player.

According to its website, the shipbuilder has designed and built more than 300 vessels for more than 54 countries including Oman, Kuwait, Yemen and Saudi Arabia.

Sources have told the ABC that Austal notified the Australian Stock Exchange (ASX) only after the breach and theft were made public on Twitter.

The Federal Government has recently started attributing cyberattacks to the countries responsible and Mr Hanson said that should continue.

"If you do have evidence that a country is targeting you then, in most cases, it makes a lot of sense to attribute and impose costs on countries that do undertake major cyberattacks," he said.

In its statement to the ASX, Austal said the data breach had been limited to Australia and had not affected its US operations.

The ACSC and Australian Federal Police are still investigating the breach and extortion attempt.
